Guia do usuário FSx do Amazon File Gateway

AWS Storage Gateway

Versão da API 2021-03-31

AWS Storage Gateway: Guia do usuário FSx do Amazon File Gateway

Table of Contents

O Amazon FSx File Gateway não está mais disponível para novos clientes. Os clientes existentes do FSx File Gateway podem continuar usando o serviço normalmente. Para recursos semelhantes ao FSx File Gateway, visite esta postagem do blog.

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

O que é o Gateway de Arquivos do Amazon FSx

O Gateway de Arquivos do Amazon FSx (Gateway de Arquivos do FSx) é um novo tipo de Gateway de Arquivos que fornece baixa latência e acesso eficiente aos compartilhamentos de arquivos do FSx para Windows File Server na nuvem das instalações on-premises. Ao manter o armazenamento de arquivos on-premises devido a requisitos de latência ou largura de banda, você poderá usar o Gateway de Arquivos do FSx para acesso contínuo a compartilhamentos de arquivos do Windows totalmente gerenciados, altamente confiáveis e praticamente ilimitados fornecidos na Nuvem AWS pelo FSx para Windows File Server.

Benefícios do uso do Gateway de Arquivos do Amazon FSx

O Gateway de Arquivos do FSx oferece os seguintes benefícios:

- Ajuda a eliminar servidores de arquivos on-premises e consolida todos os seus dados na AWS para aproveitar a escala e a economia do armazenamento em nuvem.
- Fornece opções que você pode usar para todas as suas workloads de arquivos, incluindo aquelas que exigem acesso on-premises aos dados na nuvem.
- As aplicações que precisam permanecer on-premises agora podem experimentar a mesma baixa latência e alta performance que eles têm na AWS, sem sobrecarregar suas redes nem afetar as latências das aplicações mais exigentes.

Como funciona o Gateway de Arquivos do Amazon FSx

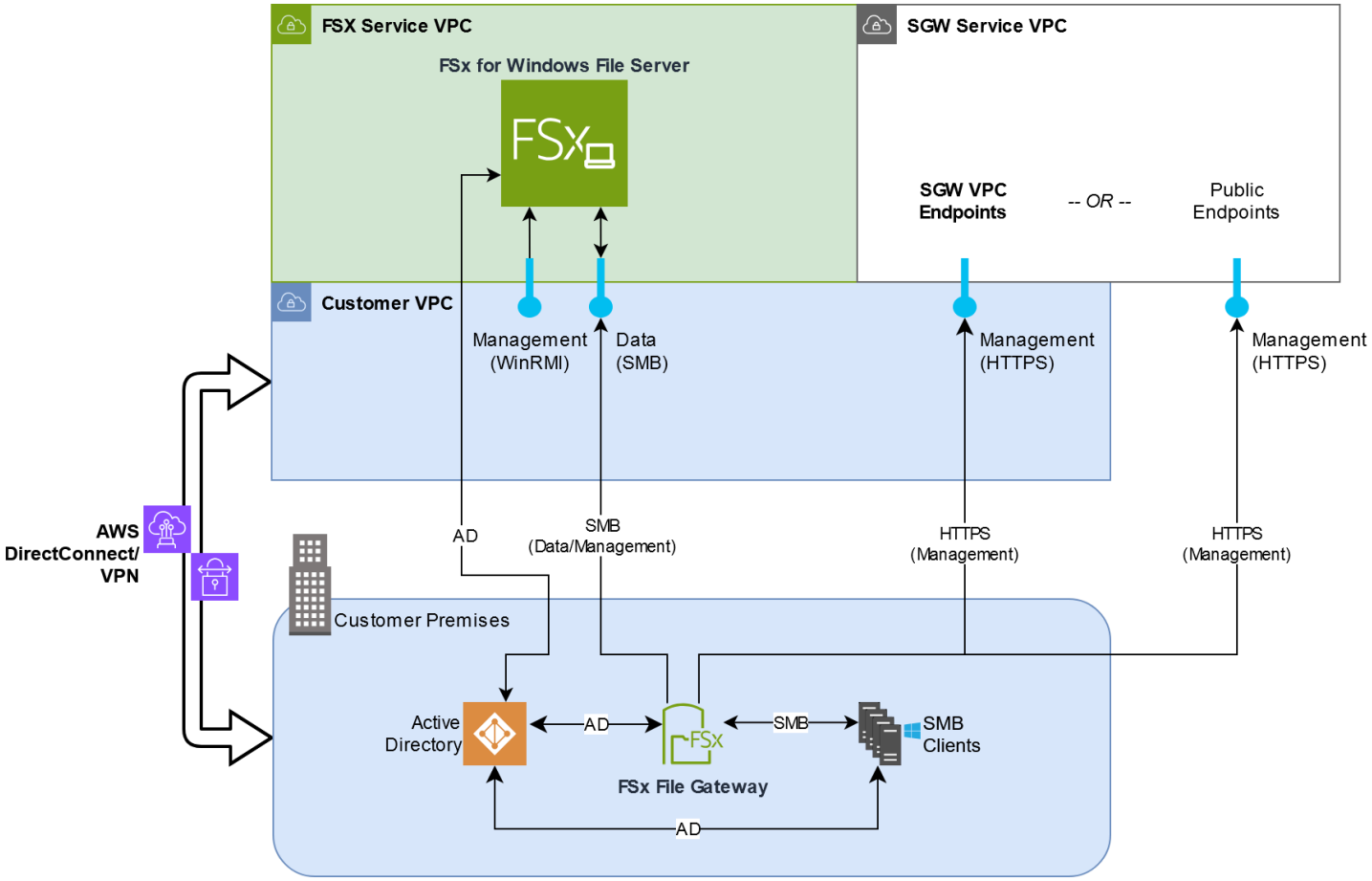
Para usar o Gateway de Arquivos do Amazon FSx (Gateway de Arquivos do FSx), você deve ter pelo menos um sistema de arquivos do Amazon FSx para Windows File Server. Você também deve ter acesso on-premises ao FSx para Windows File Server, seja por meio de uma VPN ou por meio de uma conexão com o Direct Connect. Para acessar mais informações sobre como usar os sistemas de arquivos do Amazon FSx, consulte O que é o Amazon FSx para Windows File Server?

Você implanta o gateway no ambiente on-premises como uma máquina virtual (VM) em execução no VMware ESXi, no Microsoft Hyper-V ou na máquina virtual baseada em kernel (KVM) do Linux ou como um dispositivo de hardware que você compra do revendedor de sua preferência. Você também pode implantar a VM do Storage Gateway na VMware Cloud na AWS ou como uma AMI no Amazon EC2. Depois de implantar o dispositivo, você ativa o Gateway de Arquivos do FSx por meio do console ou do Storage Gateway ou da API do Storage Gateway.

Depois que o Gateway de Arquivos do Amazon FSx for ativado e puder acessar o FSx para 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 vai usar o console do Storage Gateway para conectar o gateway ao FSx para Windows File Server existente. O FSx para Windows File Server disponibiliza todos os compartilhamentos no servidor como compartilhamentos em seu Gateway de Arquivos do Amazon FSx. Depois, você pode usar um cliente para procurar e se conectar aos compartilhamentos de arquivos no Gateway de Arquivos do FSx correspondentes ao Gateway de Arquivos do 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 para Windows File Server. O Gateway de Arquivos do FSx associa compartilhamentos de arquivos locais e seu conteúdo a compartilhamentos de arquivos armazenados remotamente no FSx para Windows File Server. Há uma correspondência 1:1 entre os arquivos remotos e visíveis localmente e seus compartilhamentos.

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



Observe o seguinte no diagrama:

- Direct Connect ou uma VPN é necessária para permitir que o Gateway de Arquivos do FSx acesse o compartilhamento de arquivos do Amazon FSx usando SMB e para permitir que o FSx para Windows File Server ingresse no seu domínio on-premises do Active Directory.
- A Amazon Virtual Private Cloud (Amazon VPC) é necessária para se conectar ao serviço FSx para Windows File Server VPC e ao serviço Storage Gateway VPC usando endpoints privados. O Gateway de Arquivos do FSx também pode se conectar aos endpoints públicos.

Você pode usar o Gateway de Arquivos do Amazon FSx em todas as regiões da AWS onde o FSx para Windows File Server está disponível.

Começando com AWS Storage Gateway

Esta seção fornece instruções para começar a usar AWS. Você precisa de uma AWS conta antes de começar a usar AWS Storage Gateway. Você pode usar uma conta da AWS existente ou se cadastrar em uma nova conta. Você também precisa de um usuário do IAM em sua AWS conta que pertença a um grupo com as permissões administrativas necessárias para realizar tarefas do Storage Gateway. Usuários com os privilégios apropriados podem acessar o console do Storage Gateway e a API do Storage Gateway para realizar tarefas de implantação, configuração e manutenção do gateway. Se você for um usuário iniciante, recomendamos que revise as seções AWS Regiões suportadas e os requisitos de configuração do File Gateway antes de começar a trabalhar com o Storage Gateway.

Esta seção contém os seguintes tópicos, que fornecem informações adicionais sobre a inicialização do AWS Storage Gateway:

Tópicos

- Cadastre-se na Amazon Web Services- Saiba como se inscrever AWS e criar uma AWS conta.
- Criar outro usuário do IAM com privilégios de administrador: saiba como criar um usuário do IAM com privilégios administrativos para sua conta da AWS .
- Acessando AWS Storage Gateway- Saiba como acessar AWS Storage Gateway por meio do console do Storage Gateway ou programaticamente usando o. AWS SDKs
- Regiões da AWS que suportam Storage Gateway- Saiba quais AWS regiões você pode usar para armazenar seus dados ao ativar seu gateway no Storage Gateway.

Cadastre-se na Amazon Web Services

Um Conta da AWS é um requisito fundamental para acessar AWS os serviços. Seu Conta da AWS é o contêiner básico para todos os AWS recursos que você cria como AWS usuário. Seu também Conta da AWS é o limite básico de segurança para seus AWS recursos. Eventuais recursos que você cria em sua conta estão disponíveis somente para usuários que tenham credenciais para essa mesma conta. Antes de começar a usar AWS Storage Gateway, você precisa se inscrever em um Conta da AWS.

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

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

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

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

Recomendamos ainda exigir que seus usuários usem credenciais temporárias ao acessar a AWS. Para fornecer credenciais temporárias, você pode usar a federação e um provedor de identidade, como o AWS IAM Identity Center. Se sua empresa já usa um provedor de identidade, você pode usá-lo com federação para simplificar a forma como você fornece acesso aos recursos em sua AWS conta.

Criar outro usuário do IAM com privilégios de administrador

Depois de criar sua AWS conta, use as etapas a seguir para criar um usuário AWS Identity and Access Management (IAM) para você e, em seguida, adicioná-lo a um grupo que tenha permissões administrativas. Para obter mais informações sobre como usar o AWS Identity and Access Management serviço para controlar o acesso aos recursos do Storage Gateway, consulteGerenciamento de identidade e acesso para AWS Storage Gateway.

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade do IAM (Recomendado)	Usar credenciais de curto prazo para acessar a AWS. Isso está de acordo com as práticas recomendadas de segurança. Para obter informações sobre as práticas recomendadas, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.	Seguindo as instruções em Conceitos básicos no Guia do usuário do Centro de Identidade do AWS IAM .	Configure o acesso programático configurando o AWS CLI para uso Centro de Identidade do AWS IAM no Guia do AWS Command Line Interface usuário.
No IAM (Não recomendado)	Usar credenciais de longo prazo para acessar a AWS.	Seguindo as instruções em Criar um acesso de emergência para um usuário do IAM no Guia do usuário do IAM.	Configurar o acesso programático, com base em Gerenciar chaves de acesso para usuários do IAM no Guia do usuário do IAM.

> **Warning**
>
> Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses

usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

Acessando AWS Storage Gateway

Você pode usar o console do AWS Storage Gateway para realizar várias tarefas de configuração e manutenção do gateway, incluindo ativar ou remover dispositivos de hardware do Storage Gateway da sua implantação, criar, gerenciar e excluir os diferentes tipos de gateway, criar, anexar, gerenciar e desanexar sistemas de arquivos e monitorar a integridade e o status de vários elementos do serviço Storage Gateway. Para simplificar e facilitar o uso, este guia se concentra na execução de tarefas usando a interface web do console do Storage Gateway. Você pode acessar o console do Storage Gateway por meio do navegador da web em: https://console.aws.amazon.com/storagegateway/home/.

Se preferir uma abordagem programática, você pode usar a AWS Storage Gateway Application Programming Interface (API) ou a Command Line Interface (CLI) para configurar e gerenciar os recursos em sua implantação do Storage Gateway. Para obter informações sobre ações, tipos de dados e sintaxe necessária para a API do Storage Gateway, consulte a Referência de API do Storage Gateway. Para obter mais informações sobre a CLI do Storage Gateway, consulte a Referência de comandos da AWS CLI.

Você também pode usar o AWS SDKs para desenvolver aplicativos que interajam com o Storage Gateway. O AWS SDKs for Java, .NET e PHP envolve a API subjacente do Storage Gateway para simplificar suas tarefas de programação. Para obter informações sobre como baixar bibliotecas de SDKs, consulte o Centro do desenvolvedor da AWS.

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

Regiões da AWS que suportam Storage Gateway

An Região da AWS é um local físico no mundo com AWS várias zonas de disponibilidade. As zonas de disponibilidade consistem em um ou mais AWS data centers discretos, cada um com energia, rede e conectividade redundantes, alojados em instalações separadas. Isso significa que cada uma Região da AWS está fisicamente isolada e independente das outras regiões. As regiões fornecem tolerância a falhas, estabilidade e resiliência e também podem reduzir a latência. Os recursos que você cria em uma região não existem em nenhuma outra região, a menos que você use explicitamente um recurso de replicação oferecido por um AWS serviço. Por exemplo, o Amazon S3

e o Amazon EC2 oferecem suporte à replicação entre Regiões. Alguns serviços, como AWS Identity and Access Management, não têm recursos regionais. Você pode lançar AWS recursos em locais que atendam às suas necessidades comerciais. Por exemplo, você pode querer lançar instâncias do Amazon EC2 para hospedar seus AWS Storage Gateway dispositivos Região da AWS na Europa para ficar mais perto de seus usuários europeus ou para atender aos requisitos legais. Você Conta da AWS determina quais das regiões suportadas por um serviço específico estão disponíveis para você usar.

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

- Amazon FSx File Gateway — Para AWS regiões suportadas e uma lista de endpoints de AWS serviço que você pode usar com o Amazon FSx File Gateway, consulte os endpoints e cotas FSx do Amazon File Gateway no. Referência geral da AWS
- Storage Gateway — Para AWS regiões compatíveis e uma lista de endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte AWS Storage Gateway endpoints e cotas no. Referência geral da AWS
- Dispositivo de Hardware do Storage Gateway: para regiões aceitas que podem ser usadas com o dispositivo de hardware, consulte Regiões do Dispositivo de Hardware do AWS Storage Gateway no Referência geral da AWS.

Requisitos de configuração do Gateway de Arquivos

A menos que especificado de outra forma, os requisitos a seguir são comuns a todos os tipos de Gatewayl de Arquivos no AWS Storage Gateway. A configuração deve atender aos requisitos nesta seção. Revise os requisitos que se aplicam à configuração do gateway antes de implantá-lo.

Tópicos

Pré-requisitos

Antes de configurar seu Amazon FSx File Gateway (FSx File Gateway) , você deve atender aos seguintes pré-requisitos:

- Crie e configure um sistema de arquivos FSx para Windows File Server. Para obter instruções, consulte Etapa 1: Crie seu sistema de arquivos no Guia do usuário do Amazon FSx para Windows File Server.
- Configure o Microsoft Active Directory (AD) e crie uma conta de serviço do Active Directory com as permissões necessárias. Para acessar mais informações, consulte Requisitos de permissão da conta de serviço do Active Directory.
- Verifique se há largura de banda de rede suficiente entre o gateway e a AWS. É necessário um mínimo de 100 Mbps para baixar, ativar e atualizar o gateway com êxito.
- Configure a conexão que você deseja usar para tráfego de rede entre AWS e o ambiente local em que você está implantando seu gateway. Você pode se conectar usando a Internet pública, rede privada, VPN ou Direct Connect. Se você quiser que seu gateway se comunique AWS por meio de uma conexão privada com uma Amazon Virtual Private Cloud, configure a Amazon VPC antes de configurar seu gateway.

- Garanta que seu gateway possa resolver o nome do seu controlador de domínio Active Directory. Você pode usar o DHCP em seu 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 a configuração de armazenamento para o gateway, bem como a quantidade mínima de espaço em disco para alocar ao armazenamento necessário.

Requisitos de hardware para instalações locais VMs

Ao implantar seu gateway on-premises, garanta que o hardware subjacente no qual está implantando a VM do gateway possa oferecer os seguintes recursos mínimos:

- Quatro processadores virtuais atribuídos à VM
- 16 GiB de 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 o gateway funcione. No entanto, para a família de instâncias otimizadas para computação, o tamanho deve ser pelo menos **`2xlarge`**.

> **Note**
>
> A AMI do Storage Gateway é compatível somente com instâncias baseadas em x86 que usam processadores Intel ou AMD. Instâncias baseadas em ARM que usam processadores Graviton não são compatíveis.

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

Recomendado para tipos de Gateway de Arquivos

- Família de instâncias de uso geral: tipos de instância m5, m6 ou m7. Escolha o tamanho da instância xlarge ou superior para atender aos requisitos de RAM e processador do Storage Gateway.
- Família de instâncias otimizadas para computação: tipos de instância c5, c6 ou c7. Escolha o tamanho da instância 2xlarge ou superior para atender aos requisitos de RAM e processador do Storage Gateway.
- Família de instâncias otimizadas para memória: tipos de instância r5, r6 ou r7. Escolha o tamanho da instância xlarge ou superior para atender aos requisitos de RAM e processador do Storage Gateway.
- Família de instâncias otimizadas para armazenamento: tipos de instância i3, i4 ou i7. Escolha o tamanho da instância xlarge ou superior para atender aos requisitos de RAM e processador do Storage Gateway.

> **Note**
>
> Quando você inicia seu gateway no Amazon EC2 e o tipo de instância selecionado aceita o armazenamento temporário, os discos são listados automaticamente. Para acessar mais informações sobre o armazenamento de instâncias do Amazon EC2, consulte Armazenamento de instâncias no Guia do usuário do Amazon EC2.

Requisitos de armazenamento

Além de 80 GiB de 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**
>
> É possível configurar uma ou mais unidades locais para seu cache, até a capacidade máxima.

Ao adicionar cache a um gateway existente, é importante criar discos no host (instância do hipervisor ou do Amazon EC2). Não altere o tamanho de discos existentes caso os discos tenham sido alocados anteriormente como 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 da rede variam com base na quantidade de dados carregados e baixados pelo gateway. É necessário um mínimo de 100 Mbps para baixar, ativar e atualizar o gateway com êxito. Os padrões de transferência de dados determinarão a largura de banda necessária para suportar a workload.

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, é possível implantar o gateway no Amazon EC2 ou usar outros tipos de implantação (incluindo on-premises) com políticas de segurança de rede que restrinjam os intervalos de endereço IP da AWS . Nesses casos, seu gateway pode ter problemas de conectividade do serviço quando os valores do intervalo de AWS IP são alterados. Os valores do intervalo de endereços AWS IP que você precisa usar estão no subconjunto de serviços da Amazon para a AWS região em que você ativa seu gateway. Para obter os valores atuais de intervalo de IPs, consulte Intervalos de endereços IP da AWS na Referência geral da AWS.

Tópicos

Requisitos de porta

FSx O File Gateway exige que portas específicas passem pela segurança de sua rede para uma implantação e operação bem-sucedidas. Algumas portas são necessárias para todos os gateways, enquanto outras são necessárias somente para configurações específicas, como ao se conectar a endpoints da VPC.

Para o FSx File Gateway, você deve usar o Microsoft Active Directory para permitir que os usuários do domínio acessem um compartilhamento de arquivos SMB (Server Message Block). É possível associar seu Gateway de Arquivos a qualquer domínio Microsoft Windows válido (solucionado por DNS).

Você também pode usar o Directory Service para criar um AWS Managed Microsoft ADna Amazon Web Services Cloud. Para a maioria das AWS Managed Microsoft AD implantações, você precisa configurar o serviço Dynamic Host Configuration Protocol (DHCP) para sua VPC. Para acessar informações sobre a criação de um conjunto de opções de DHCP, consulte Criar um conjunto de opções de DHCP no Guia de administração do AWS Directory Service .

A tabela a seguir lista as portas necessárias e descreve os requisitos condicionais na coluna Notas.

Requisitos de porta para o FSx File Gateway

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Navegadc da web	Seu navegado da web	VM do Storage Gateway	TCP HTTP	80	✓	✓	✓	Usado por sistemas locais para recuperar a chave de ativação do Storage Gateway. A porta

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
								80 só é usada durante a ativação de um dispositivo do Storage Gateway. Uma VM do Storage Gateway não exige que a porta 80 seja publicamente acessível. O nível necessário de acesso à porta 80 depende da configuração da rede.

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
								Se você ativar o gateway pelo Console de Gerenciamento do Storage Gateway, o host pelo qual se conecta ao console deverá ter acesso à porta 80 do gateway.
Navegador da web	VM do Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓	AWS Console de gerenciamento (todas as outras operações)

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
DNS	VM do Storage Gateway	Servidor Domain Name Service (DNS – Serviço do nome de domínio)	TCP e UDP DNS	53	✓	✓	✓	Usado para comunicação entre a VM do Storage Gateway e o servidor DNS para resolução de nome IP.

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
NTP	VM do Storage Gateway	Servidor de Network Time Protocol (NTP)	TCP e UDP NTP	123	✓	✓	✓	Usado por sistemas on-premises para sincronizar a hora da VM com a hora do host. Uma VM do Storage Gateway está configurada para usar os seguintes servidores NTP: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
								• 3.amazon.pool.ntp.org Note Não é necessário para gateways hospedados no Amazon EC2.

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Storage Gateway	VM do Storage Gateway	Suporte Ponto final	TCP SSH	22	✓	✓	✓	Permite Suporte acessar seu gateway para ajudá-lo a solucionar problemas de gateway. Você não precisa dessa porta aberta para a operação normal do gateway, mas ela é necessária para a solução de problemas. Para ver uma

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
								lista de endpoints, consulte os Endpoints do Suporte.
Storage Gateway	VM do Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓	Controle de gerenciamento
Amazon CloudFront	VM do Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓	Para ativação
VPC	VM do Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓*	Controle de gerenciamento *Obrigatório somente ao usar endpoints da VPC

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
VPC	VM do Storage Gateway	AWS	TCP HTTPS	1026		✓	✓*	Endpoint do ambiente de gerenciamento *Obrigatório somente ao usar endpoints da VPC
VPC	VM do Storage Gateway	AWS	TCP HTTPS	1027		✓	✓*	Ambiente de gerenciamento Anon (para ativação) *Obrigatório somente ao usar endpoints da VPC

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
VPC	VM do Storage Gateway	AWS	TCP HTTPS	1028		✓	✓*	Endpoint de proxy *Obrigatório somente ao usar endpoints da VPC
VPC	VM do Storage Gateway	AWS	TCP HTTPS	1031		✓	✓*	Plano de dados *Obrigatório somente ao usar endpoints da VPC

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
VPC	VM do Storage Gateway	AWS	TCP HTTPS	2222		✓	✓*	Canal de suporte SSH para VPCe *Exigido somente para abrir o canal de suporte ao usar endpoints da VPC.
VPC	VM do Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓*	Controle de gerenciamento *Obrigatório somente ao usar endpoints da VPC

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Cliente de compartilhamento de arquivo	Cliente SMB	VM do Storage Gateway	TCP ou UDP SMBv3	445	✓	✓	✓	Serviço de sessão de transferência de dados de compartilhamento de arquivos. Substitui as portas 137 a 139 do Microsoft Windows NT e versões posteriores.
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	NetBIOS UDP	137	✓	✓	✓	Serviço de nome
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	NetBIOS UDP	138	✓	✓	✓	Serviço de datagrama

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	TCP e UDP LDAP	389	✓	✓	✓	Conexão do cliente do Directory System Agent (DSA)
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	TCP e UDP Kerberos	88	✓	✓	✓	Kerberos
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	Mapeador de Environment/Endpontos de computação distribuída TCP (DCE/EMAP)	135	✓	✓	✓	RPC

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
FSx Conexão com a Amazon	VM do Storage Gateway	FSx para Windows File Server	TCP ou UDP SMBv3	445	✓	✓	✓	Serviço de sessão de transferência de dados de compartilhamento de arquivos.

Requisitos de rede e firewall para o Storage Gateway Hardware Appliance

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

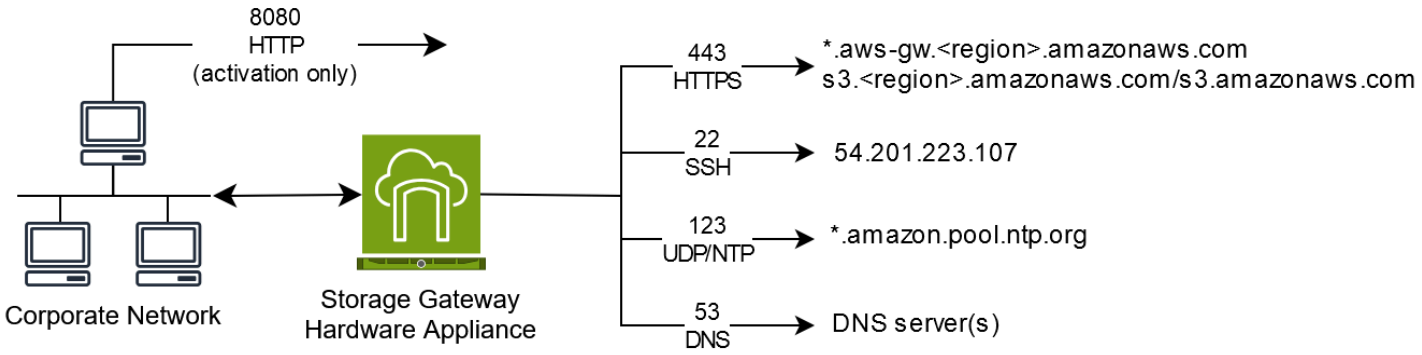
- Acesso à internet: em uma rede sempre disponível de conexão com a Internet por meio de uma interface de rede no servidor.
- DNS services: serviços DNS para comunicação entre o dispositivo de hardware e o servidor DNS.
- Sincronização de horário: um serviço Amazon NTP de horário configurado automaticamente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

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.

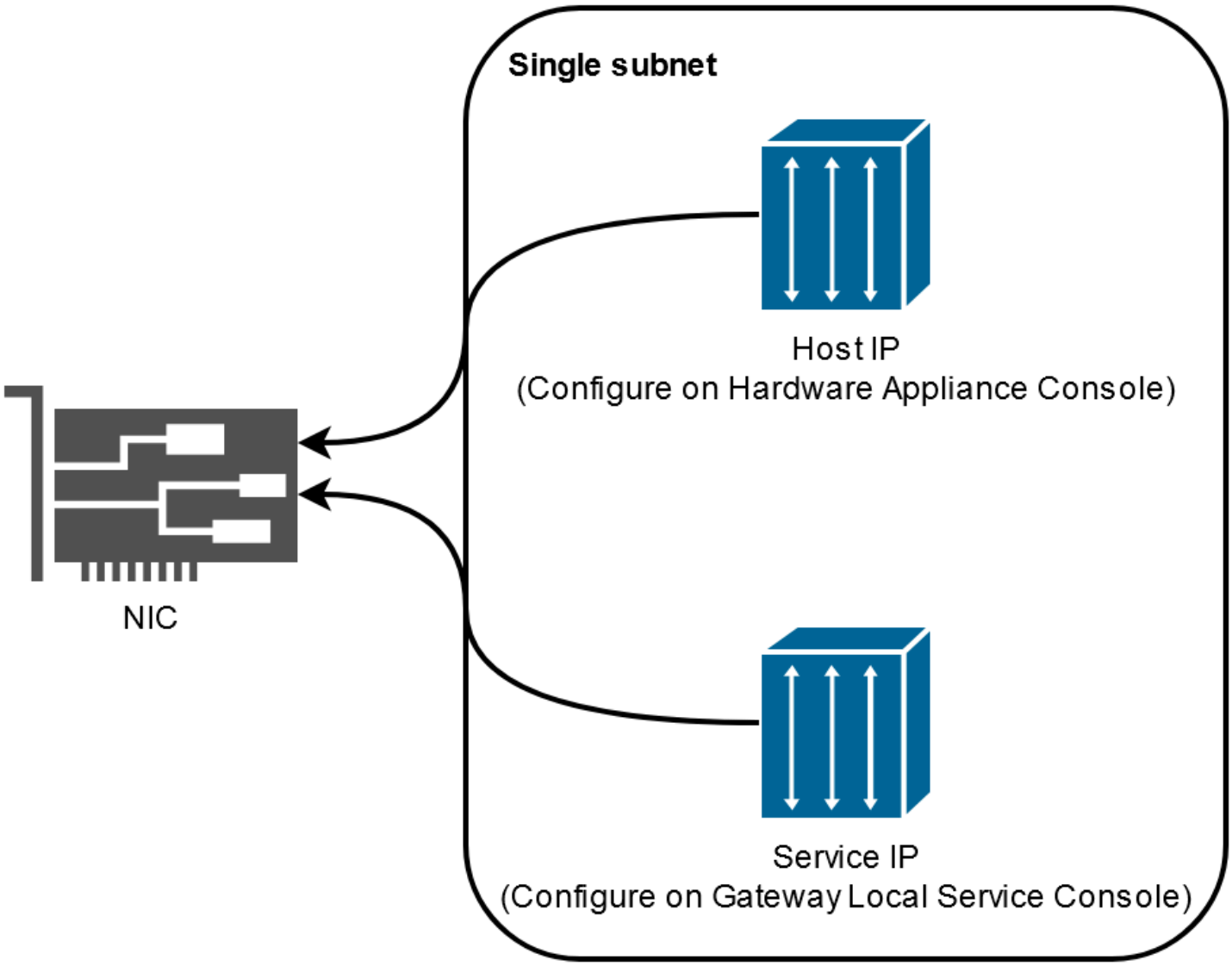
Protocolo	Porta	Direction	Fonte	Destino	Usage
SSH	22	Saída	Equipamento de hardware	`54.201.223.107`	Canal de suporte
DNS	53	Saída	Equipamento de hardware	Servidores DNS	Resolução de nome
UDP/NTP	123	Saída	Equipamento de hardware	`*.amazon.pool.ntp.org`	Sincronização de horário
HTTPS	443	Saída	Equipamento 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 Como configurar os parâmetros de rede do dispositivo de hardware.

> **Note**
>
> Para obter uma ilustração mostrando a parte traseira do servidor com suas portas, consulteInstalação física do dispositivo de hardware.

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 acessar mais informações sobre como ativar e configurar um dispositivo de hardware, consulte Usando o dispositivo de hardware AWS Storage Gateway.

Permitindo AWS Storage Gateway acesso por meio de firewalls e roteadores

Seu gateway requer acesso aos seguintes endpoints de serviço do Storage Gateway para se comunicar com AWS. Durante a configuração do gateway, selecione o tipo de endpoint para o gateway com base no ambiente de rede. Se usar um firewall ou roteador para filtrar ou limitar o tráfego de rede, você deverá configurar o firewall e o roteador para permitir a comunicação externa com a AWS nesses endpoints de serviço.

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

> **Important**
>
> *region*Substitua os exemplos de endpoint a seguir pela Região da AWS string correta para seu gateway, comous-west-2.
> *amzn-s3-demo-bucket*Substitua pelo nome real do bucket do Amazon S3 em sua implantação. Você também pode usar um asterisco (*) no lugar de *amzn-s3-demo-bucket* para criar uma entrada curinga em suas regras de firewall, o que permitirá listar o endpoint do serviço para todos os nomes de buckets.
> Se seus gateways estiverem implantados Regiões da AWS nos Estados Unidos da América ou Canadá e precisarem de conexões de endpoint compatíveis com o Padrão Federal de Processamento de Informações (FIPS), substitua por. *s3* s3-fips

Tipos de endpoint

Endpoints padrão

Esses endpoints oferecem suporte ao IPv4 tráfego entre seu dispositivo de gateway e. AWS

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

```
bucket-name.s3.region.amazonaws.com:443
```

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

```
anon-cp.storagegateway.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) (da `us-west-2`).

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

Além dos endpoints de serviço do Storage Gateway e do Amazon S3, o Storage Gateway VMs também exige acesso à rede aos seguintes servidores NTP:

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

Para obter mais informações sobre endpoints compatíveis Regiões da AWS e de serviço, consulte Storage Gateway no Referência geral da AWS.

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

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

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

  Se você precisar permitir que as instâncias conectem-se ao gateway de fora do respectivo grupo de segurança, é recomendável permitir conexões somente na porta 80 (para ativação).
- Se você deseja ativar seu gateway em um host do EC2 fora do grupo de segurança do gateway, permita conexões de entrada na porta 80 do endereço IP desse host. Se não conseguir determinar a ativação de endereço IP do host, poderá abrir a porta 80, ativar seu gateway e fechar o acesso na porta 80 assim que a ativação for concluída.

- Permita o acesso à porta 22 somente se você estiver usando Suporte para fins de solução de problemas. Para obter mais informações, consulte Você quer ajudar Suporte a solucionar problemas do seu gateway Amazon EC2.

Hipervisores compatíveis e requisitos de host

Você pode executar o Storage Gateway localmente como um dispositivo de máquina virtual (VM) ou um dispositivo de hardware físico, ou como uma instância do AWS Amazon EC2.

> **Note**
>
> O modo de inicialização UEFI com inicialização segura desativada (loader_secure=no) é necessário para o File Gateway 2.x, o Volume Gateway 3.x e o Tape Gateway 3.x. Um arquivo xml é fornecido com cada download do qcow como uma configuração rápida.

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

- VMware ESXi Hypervisor (versão 7.0 ou 8.0) — Para essa configuração, você também precisa de um cliente VMware vSphere para se conectar ao host.
- Hipervisor Microsoft Hyper-V (2019, 2022, or 2025): para essa configuração, você precisa de um Microsoft Hyper-V Manager em um computador cliente Microsoft Windows para se conectar ao host.
- Máquina virtual baseada em kernel (KVM) do Linux: uma tecnologia de virtualização gratuita e de código aberto. O KVM está incluído em todas as versões do Linux versão 2.6.20 e mais recentes. O Storage Gateway foi testado e compatível com as CentOS/RHEL distribuições 7.7, RHEL 8.6, 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. Consulte o aws-storage-gateway arquivo.xml fornecido para ver as configurações de inicialização sugeridas. O modo de inicialização UEFI com inicialização segura desativada (loader_secure=no) é necessário para o File Gateway 2.x, o Volume Gateway 3.x e o Tape Gateway 3.x.
- Nutanix AHV (Acropolis Hypervisor) a partir da versão 10.0.1.1 — Uma plataforma de virtualização baseada em KVM que é integrada à solução de infraestrutura hiperconvergente (HCI) da Nutanix.

- Instância do EC2: o Storage Gateway fornece uma imagem de máquina da Amazon (AMI) que contém a imagem da VM do gateway. Para obter informações sobre como implantar um gateway no Amazon EC2, consulte Implante um host padrão do Amazon EC2 para FSx o File Gateway.
- Dispositivo de Hardware do Storage Gateway: o Storage Gateway fornece um dispositivo de hardware físico como uma opção de implantação on-premises para locais com uma infraestrutura de máquina virtual limitada.

> **Note**
>
> O Storage Gateway não oferece suporte à recuperação de um gateway de uma VM criada por meio de um snapshot ou clonada de outra VM do gateway ou de uma AMI do Amazon EC2. Se a sua VM de gateway não funciona corretamente, ative um novo gateway e recupere os seus dados de outro. Para obter mais informações, consulte Como se recuperar de um caso de encerramento inesperado da máquina virtual.
> O Storage Gateway não oferece suporte à memória dinâmica nem à expansão da memória virtual.

Clientes SMB aceitos pelo Gateway de Arquivos

Os Gateways de Arquivos oferecem suporte aos seguintes clientes do Service Message Block (SMB):

- Microsoft Windows Server 2008 R2 e posterior
- Versões de área de trabalho do Windows: 10, 8 e 7.
- Windows Terminal Server em execução no Windows Server 2008 e versões posteriores

> **Note**
>
> A criptografia Server Message Block requer clientes que aceitem dialetos SMB v3.x.

Operações de sistema de arquivos aceitas pelo 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 na Amazon de forma FSx assíncrona por meio de transferências otimizadas. As leituras são primeiro atendidas pelo cache local. Se os dados não estiverem disponíveis, eles serão obtidos na Amazon FSx como um cache de leitura contínua.

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

Gerenciar discos locais para seu gateway

O gateway da máquina virtual (VM) usa os discos locais que você aloca no local para buffer e armazenamento. Um Gateway de Arquivos criado em uma instância do Amazon EC2 usará volumes do Amazon EBS como discos locais. Você decide o número e o tamanho dos discos que deseja alocar para o gateway. O gateway usa armazenamento em cache alocado por você para conceder acesso de baixa latência aos dados recém-acessados. O armazenamento em cache atua como o armazenamento durável local para dados que estão pendentes de upload para o . Gateways de Arquivos exigem pelo menos um disco de 150 GiB para usar como cache. Após a configuração inicial e a implantação do seu gateway, você pode adicionar mais discos para armazenamento em cache à medida que as demandas da workload aumentam. Esta seção contém os tópicos a seguir, que descrevem conceitos e procedimentos relacionados ao gerenciamento de discos locais.

Tópicos

- Como determinar o volume de armazenamento do disco local: saiba como determinar o número e o tamanho dos discos de cache local a serem alocados para seu Gateway de Arquivos.
- Configurar armazenamento em cache adicional: saiba como aumentar a capacidade de armazenamento em cache do seu Gateway de Arquivos à medida que as necessidades da sua aplicação mudam.
- Usar o armazenamento temporário com gateways do EC2: saiba como evitar a perda de dados ao usar armazenamento em disco efêmero com o Gateway de Arquivos.

Como determinar o volume de armazenamento do disco local

Ao implantar um gateway de arquivos do , considere a quantidade de disco de cache a ser alocada. O File Gateway usa um algoritmo usado menos recentemente para remover automaticamente os dados do cache. O cache em um File Gateway é compartilhado entre todos os compartilhamentos de arquivos nesse gateway. Se você tiver vários compartilhamentos ativos, é importante observar que a utilização intensa de um compartilhamento pode afetar a quantidade de recursos de cache aos quais outro compartilhamento tem acesso, possivelmente afetando a performance.

Ao determinar a quantidade de disco de cache necessária para uma determinada carga de trabalho, é importante observar que você sempre pode adicionar disco de cache ao seu gateway (até as cotas atuais no), mas não pode diminuir o cache de um determinado gateway. Você pode realizar uma análise básica no conjunto de dados para determinar a quantidade certa de disco de cache, mas não há como determinar exatamente quantos dados estão “ativos” e precisam ser armazenados localmente, versus “frios”, e podem ser colocados em camadas na nuvem. As cargas de trabalho mudam com o tempo, e o File Gateway oferece flexibilidade e elasticidade relacionadas à quantidade de recursos que podem ser consumidos. A quantidade de cache sempre pode ser aumentada, portanto, começar aos poucos e aumentar conforme necessário costuma ser a abordagem mais econômica.

Você pode usar uma aproximação inicial de 150 GiB para provisionar discos para o armazenamento em cache durante a configuração do gateway. Em seguida, você pode usar as métricas CloudWatch operacionais da Amazon para monitorar o uso do armazenamento em cache e provisionar mais armazenamento conforme necessário usando o console. Para obter informações sobre como usar métricas e configurar de alarmes, consulte Performance e otimização.

> **Note**
>
> Os recursos de armazenamento físico subjacentes são representados como um armazenamento de dados em 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 outro armazenamento de dados distinto.
>
> Se você tiver mais de um armazenamento de dados, é altamente recomendável escolher um para o armazenamento de dados e outro para o armazenamento em cache. O armazenamento de dados que conta apenas com um disco físico subjacente pode apresentar baixa performance em algumas situações, quando é usado para respaldar o

armazenamento em cache. Isso também é verdade se o backup for uma configuração RAID de menor desempenho, como. RAID1

Configurar armazenamento em cache adicional

À medida que as necessidades da sua aplicação mudarem, você poderá aumentar a capacidade de armazenamento em cache do gateway. É possível adicionar a capacidade de armazenamento ao seu gateway sem interromper a funcionalidade ou causar tempo de inatividade. Ao adicionar mais armazenamento, você o faz com a VM do gateway ativada.

> **Important**
>
> Ao adicionar cache a um gateway existente, você deve criar discos no hipervisor do host do gateway ou na instância do Amazon EC2. Não remova nem altere o tamanho dos discos existentes que já foram alocados como cache.

Como configurar um armazenamento em cache adicional para o gateway

1. Provisione um ou mais discos novos no gateway, no host, no hipervisor ou na instância do Amazon EC2. Para obter informações sobre como provisionar um disco em um hipervisor, consulte o manual do usuário do hipervisor. Para obter informações sobre o provisionamento de volumes do Amazon EBS para uma instância do Amazon EC2, consulte Volumes do Amazon EBS no Manual do usuário para instâncias do Linux do Amazon Elastic Computer Cloud. Nas etapas a seguir, você vai configurar esse disco como armazenamento em cache.
2. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
3. No painel de navegação, selecione Gateways da .
4. Procure seu gateway e selecione-o na lista.
5. No menu Ações, selecione Configurar armazenamento em cache.
6. Na seção Configurar armazenamento em cache, identifique os discos que você provisionou. Se você não vir os discos, selecione o ícone de atualização para atualizar a lista. Para cada disco, escolha Cache no menu suspenso Alocado para.

> **Note**
>
> O cache é a única opção disponível para alocar discos em um Gateway de Arquivos.

7. Escolha Salvar alterações para salvar as definições de configuração.

Usar o armazenamento temporário com gateways do EC2

Não recomendamos o uso de discos temporários para armazenamento em cache em gateways de arquivos. FSx

Os discos temporários fornecem armazenamento ao nível do bloco temporário para instâncias do Amazon EC2. Quando você inicia seu gateway com uma imagem de máquina da Amazon do Amazon EC2 e o tipo de instância selecionado oferece suporte ao armazenamento temporário, os discos temporários são listados automaticamente. Você pode selecionar um dos discos para armazenar os dados de cache do seu gateway. Para acessar mais informações, consulte Armazenamento de instância do Amazon EC2 no Guia do usuário do Amazon EC2.

> **Important**
>
> Se você estiver usando o armazenamento temporário e interromper e iniciar o gateway do Amazon EC2, o gateway ficará permanentemente off-line. Isso acontece porque o disco de armazenamento físico é substituído. Não há uma solução alternativa para esse problema. A única solução é excluir o gateway e ativar um novo em uma nova instância do EC2.

Usando o dispositivo de hardware AWS Storage Gateway

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

O AWS Storage Gateway Hardware Appliance é um dispositivo de hardware físico com o software Storage Gateway pré-instalado em uma configuração de servidor validada. Você pode gerenciar os dispositivos de hardware em sua implantação na página de visão geral do equipamento de hardware no AWS Storage Gateway console.

Cada dispositivo de hardware é um servidor 1U de alto desempenho que pode ser implantado em seu datacenter ou on-premises dentro do seu firewall corporativo. Ao ativar e comprar o dispositivo de hardware, o processo de ativação associa o dispositivo de hardware à sua Conta da AWS. Após a ativação, seu dispositivo de hardware será exibido no console na página Visão geral do dispositivo de hardware. Você pode configurar o dispositivo de hardware como um tipo S3 File Gateway, File Gateway, FSx Tape Gateway ou Volume Gateway. O procedimento que você usa para implantar esses tipos de gateway em um dispositivo de hardware é o mesmo que em uma plataforma virtual.

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

Nas seções a seguir, você encontrará instruções sobre como instalar, montar em rack, alimentar, configurar, ativar, iniciar, usar e excluir um dispositivo de hardware AWS Storage Gateway.

Tópicos

- Ativando seu dispositivo AWS de hardware Storage Gateway
- Como criar um gateway no dispositivo de hardware
- Como configurar um endereço IP de gateway no dispositivo de hardware
- Como remover o software de gateway do dispositivo de hardware
- Excluindo seu dispositivo de hardware AWS Storage Gateway

Configurando seu dispositivo de hardware AWS Storage Gateway

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Depois de receber seu dispositivo de hardware Storage Gateway, você usa o console local do dispositivo de hardware para configurar a rede para fornecer uma conexão sempre ativa e ativar seu dispositivo. AWS A ativação associa seu equipamento à AWS conta usada durante o processo de ativação. Depois que o equipamento for ativado, você poderá iniciar um S3 File Gateway, um File Gateway, FSx um Tape Gateway ou um Volume Gateway a partir do console do Storage Gateway.

Para instalar e configurar o dispositivo de hardware

1. Monte o dispositivo em rack e conecte-o à energia e à rede. Para obter mais informações, consulte Instalação física do dispositivo de hardware.
2. Defina os endereços do Protocolo de Internet versão 4 (IPv4) para o dispositivo de hardware (o host). Para obter mais informações, consulte Como configurar os parâmetros de rede do dispositivo de hardware.
3. Ative o dispositivo de hardware no console Página de visão geral do dispositivo de hardware na AWS região de sua escolha. Para obter mais informações, consulte Ativando seu dispositivo AWS de hardware Storage Gateway.
4. Crie um gateway no dispositivo de hardware. Para obter mais informações, consulte Como criar um gateway.

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

Aumento do armazenamento em cache utilizável

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

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

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

Opções da placa da interface de rede

Dependendo do modelo do aparelho que você solicitou, ele pode vir com uma placa de rede 10G-Base-T de RJ45 cobre ou 10G DA/SFP+.

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

Instalação física do dispositivo de hardware

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

O dispositivo tem um formato de 1U e cabe em um rack padrão de 19 polegadas compatível com a Comissão Eletrotécnica Internacional (IEC).

Pré-requisitos

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

- Cabos de alimentação: 1 (necessário); 2 (recomendado).
- Cabeamento de rede compatível (dependendo de qual placa de interface de rede, NIC, está incluída no dispositivo de hardware). O módulo óptico Twinax Copper DAC, SFP+ (compatível com Intel) ou transceptor de cobre SFP para Base-T.
- Teclado e monitor, ou uma solução de switch de teclado, vídeo e mouse (KVM).

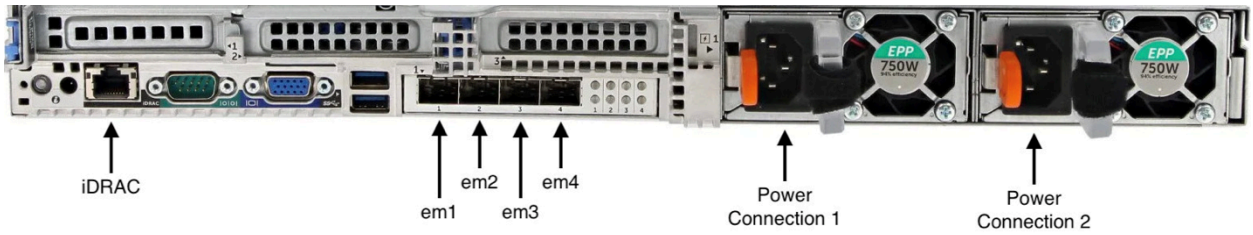
> **Note**
>
> Antes de executar o procedimento a seguir, verifique se você atende a todos os requisitos para o Storage Gateway Hardware Appliance como descrito em Requisitos de rede e firewall para o Storage Gateway Hardware Appliance.

Para instalar fisicamente o dispositivo de hardware

1. Retire o dispositivo de hardware de gateway de armazenamento do contêiner e siga as instruções contidas na caixa para montar o servidor no rack.

   A imagem a seguir mostra a parte traseira do dispositivo de hardware com portas para conexão de alimentação, Ethernet, monitor, teclado USB e iDRAC.

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



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

2. Conecte um cabo de alimentação para cada uma das duas fontes. É possível conectar a apenas uma fonte de alimentação, mas recomendamos ligações com ambas as fontes para redundância.
3. Conecte um cabo Ethernet à porta `em1` para garantir conexão permanente à Internet. A porta `em1` é a primeira das quatro portas de rede física na parte traseira, da esquerda para a direita.

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

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

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

Próxima etapa

Como acessar o console do dispositivo de hardware

Como acessar o console do dispositivo de hardware

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de

2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Quando você liga o dispositivo de hardware, o console do dispositivo de hardware aparece no monitor. O console do dispositivo de hardware apresenta uma interface de usuário específica AWS que você pode usar para definir uma senha de administrador, configurar os parâmetros iniciais da rede e abrir um canal de suporte para AWS.

Para trabalhar com o console do dispositivo de 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.

Na primeira vez que o console do equipamento de hardware aparece, a página de boas-vindas é exibida e você é solicitado a definir uma senha para a conta do usuário administrador antes de poder acessar o console.

Para definir uma senha de administrador

- No prompt Defina sua senha de login, faça o seguinte:

  a. Para Set Password (Definir senha), digite uma e, em seguida, pressione `Down arrow`.

  b. Para Confirm (Confirmar), digite novamente e, em seguida, escolha Save Password (Salvar senha).

Depois de definir sua senha, a Página inicial do console de hardware é exibida. A página inicial exibe informações de rede para as interfaces de rede em1, em2, em3 e em4 e tem as seguintes opções de menu:

- Configurar redes
- Abrir console de serviço
- Alterar senha
- logout
- Abrir console de suporte

Próxima etapa

Como configurar os parâmetros de rede do dispositivo de hardware

Como configurar os parâmetros de rede do dispositivo de hardware

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Depois que o dispositivo de hardware for inicializado e você definir sua senha de usuário administrador no console de hardware, conforme descrito em Como acessar o console do dispositivo de hardware, use o procedimento a seguir para configurar os parâmetros de rede aos quais seu dispositivo de hardware possa se conectar à AWS.

Para definir o endereço de rede

1. Na Página inicial, escolha Configurar rede e pressione `Enter`. A página Configurar rede é exibida. A página Configurar rede mostra informações de IP e DNS para cada uma das quatro interfaces de rede no dispositivo de hardware e inclui opções de menu para configurar endereços DHCP ou estáticos para cada uma.
2. Para a interface em1, siga um destes procedimentos:

   - Escolha DHCP e pressione `Enter` para usar o IPv4 endereço atribuído pelo servidor DHCP (Dynamic Host Configuration Protocol) à porta de rede física.

     Anote este endereço para uso posterior na etapa de ativação.
   - Escolha Estático e pressione `Enter` para configurar um IPv4 endereço estático.

     Insira um endereço IP, máscara de sub-rede, gateway e endereço de servidor DNS válidos para a interface de rede em1.

     Ao finalizar, escolha Salvar e pressione `Enter` para salvar a configuração.

> **Note**
>
> Você pode usar esse procedimento para configurar outras interfaces de rede além da em1. Se você configurar outras interfaces, elas deverão fornecer a mesma conexão sempre ativa com os AWS endpoints listados nos requisitos.
> Não é possível usar o Network Bonding e o LACP (Link Aggregation Control Protocol) no dispositivo de hardware e no Storage Gateway.
> Não recomendamos configurar várias interfaces de rede na mesma sub-rede, pois isso às vezes pode causar problemas de roteamento.

Para encerrar a sessão do console de hardware

1. Escolha Voltar e pressione `Enter` para retornar à Página inicial.
2. Escolha Sair e pressione `Enter` para retornar à página de boas-vindas.

Próxima etapa

Ativando seu dispositivo AWS de hardware Storage Gateway

Ativando seu dispositivo AWS de hardware Storage Gateway

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Depois de configurar seu endereço IP, você insere esse endereço IP na página Hardware do AWS Storage Gateway console para ativar seu dispositivo de hardware. O processo de ativação registra o dispositivo em sua conta da AWS .

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

Para ativar seu dispositivo de hardware AWS Storage Gateway

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

   > **Note**
   >
   > Para somente ativar, o seguinte deve acontecer:
   >
   > - Seu navegador deve estar na mesma rede que o seu dispositivo de hardware.
   > - O firewall deve permitir acesso HTTP na porta 8080 no dispositivo para o tráfego de entrada.

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

   Consulte mais informações sobre como configurar o endereço IP em Como configurar parâmetros de rede.
5. Em Nome, insira um nome para o dispositivo de hardware. Os nomes podem ter até 255 caracteres e não podem conter barras.
6. Em Fuso horário do dispositivo de hardware, insira o fuso horário local com base no qual a maior parte da workload do gateway será gerada e, depois, escolha Próximo.

   O fuso horário controla quando ocorrem atualizações de hardware, com o horário 2h00 usado como horário programado padrão para fazer atualizações. Idealmente, se o fuso horário estiver definido corretamente, as atualizações ocorrerão fora da janela local de dias úteis por padrão.
7. Revise os parâmetros de ativação na seção Detalhes do dispositivo de hardware. Você pode escolher Anterior para voltar e fazer alterações, se necessário. Caso contrário, escolha Ativar para finalizar a ativação.

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

Nesse momento, o dispositivo está associado à sua conta. A próxima etapa é configurar e iniciar um S3 File Gateway, FSx File Gateway, Tape Gateway ou Volume Gateway no novo equipamento.

Próxima etapa

Como criar um gateway no dispositivo de hardware

Como criar um gateway no dispositivo de hardware

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Você pode criar um gateway de arquivos, gateway de FSx arquivos, gateway de fita ou gateway de volume S3 em qualquer dispositivo de hardware do AWS Storage Gateway em sua implantação.

Para criar um gateway no dispositivo de hardware

1. Faça login Console de gerenciamento da AWS e abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Siga os procedimentos descritos em Como criar seu gateway para instalar, conectar e configurar o tipo de gateway escolhido.

Ao terminar de criar seu gateway no console do Storage Gateway, o software Storage Gateway começa a ser instalado automaticamente no dispositivo de hardware. Se você usa o Protocolo de Configuração Dinâmica de Host (DHCP), pode levar de cinco a dez minutos para que um gateway seja exibido como on-line no console. Para atribuir um endereço IP estático ao gateway instalado, consulte Configuring an IP address for the gateway.

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

Próxima etapa

Como configurar um endereço IP de gateway no dispositivo de hardware

Como configurar um endereço IP de gateway no dispositivo de hardware

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Antes de ativar seu dispositivo de hardware, você atribuiu um endereço IP à interface de rede física. Agora que ativou o equipamento e iniciou o Storage Gateway nele, você precisa atribuir outro endereço IP à máquina virtual do Storage Gateway que é executada no dispositivo de hardware. Para atribuir um endereço IP estático a um gateway instalado no seu dispositivo de hardware, configure o endereço IP do console local do gateway para esse gateway. Seus aplicativos (como o cliente NFS ou SMB) se conectam a esse endereço IP. É possível acessar o console local de gateway pelo console do dispositivo de hardware utilizando a opção Abrir console de serviço.

Para configurar o endereço IP dispositivo para trabalhar com aplicativos

1. No console de hardware, escolha Abrir console de serviço e pressione `Enter` para abrir a tela de login do console local do gateway.
2. A página de login do console AWS Storage Gateway local solicita que você faça login para alterar sua configuração de rede e outras configurações.

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

   > **Note**
   >
   > É recomendável alterar a senha padrão digitando o número correspondente para o console do Gateway no menu principal Ativação do AWS equipamento: Configuração e, em seguida, executando o `passwd` comando. Para obter informações sobre como

executar o comando, consulte Como executar comandos do Storage Gateway no console local. Você também pode definir a senha no console do Storage Gateway. Para obter mais informações, consulte Definir a senha do console local no console do Storage Gateway.

3. A página Ativação de dispositivo da AWS - Configuração inclui as seguintes opções:

   - Configuração de proxy HTTP/SOCKS
   - Configuração de rede
   - Testar a conectividade de rede
   - Exibir uma verificação de recursos do sistema
   - Gerenciamento de tempo do sistema
   - Informações da licença
   - Prompt de comando

   > **Note**
   >
   > Algumas opções aparecem somente para tipos específicos de gateway ou plataformas de host.

   Digite o número correspondente para navegar até a página Configuração de rede.

4. Siga um destes procedimentos para configurar o endereço IP do gateway:

   - Para usar o endereço IP atribuído pelo servidor Protocolo de Configuração Dinâmica de Host (DHCP), digite o número correspondente para Configurar DHCP e, em seguida, insira as informações de configuração DHCP válidas na página a seguir.
   - Para atribuir um endereço IP estático, digite o número correspondente para Configurar IP estático e, em seguida, insira o endereço IP válido e as informações de DNS na página a seguir.

   > **Note**
   >
   > O 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.

Depois de ativar e configurar seu dispositivo de hardware, ele é exibido no console. Agora é possível continuar o procedimento de instalação e configuração do seu gateway no console do Storage Gateway. Para receber instruções, consulte Configure seu Amazon FSx File Gateway.

Como remover o software de gateway do dispositivo de hardware

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Se você não precisar mais de um Storage Gateway específico implantado em um dispositivo de hardware, poderá remover o software do gateway do dispositivo de hardware. Depois de remover o software do gateway, você pode optar por implantar um novo gateway em seu lugar ou excluir o próprio dispositivo de hardware do console do Storage Gateway. Para remover um software de gateway de seu dispositivo de hardware, use o procedimento a seguir.

Para remover um gateway a partir de um dispositivo de hardware

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Hardware no painel de navegação no lado esquerdo da página do console e, em seguida, escolha o nome do dispositivo de hardware do qual você deseja remover o software do gateway.
3. No menu suspenso Ações, escolha Remover gateway.

Uma caixa de diálogo de confirmação é exibida.

4. Verifique se você deseja remover o software de gateway do dispositivo de hardware especificado, digite a palavra `remove` na caixa de confirmação.
5. Escolha Remover para remover permanentemente o software do gateway.

> **Note**
>
> Depois de remover o software do gateway, você não poderá desfazer a ação. Para determinados tipos de gateway, você pode perder dados na exclusão, especialmente os dados em cache. Para mais informações sobre como deletar um gateway, consulte Como excluir o gateway e remover recursos associados.

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

Excluindo seu dispositivo de hardware AWS Storage Gateway

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

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

> **Note**
>
> Para mover seu equipamento para uma AWS conta diferente ou Região da AWS, você deve primeiro excluí-lo usando o procedimento a seguir e, em seguida, abrir o canal de suporte do gateway e entrar em contato Suporte para realizar uma reinicialização suave. Para obter

mais informações, consulte Ativando o Suporte acesso para ajudar a solucionar problemas do gateway hospedado no local.

Para excluir do dispositivo de hardware

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

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

Como criar um gateway

Os tópicos de visão geral desta página fornecem uma sinopse geral de como funciona o processo de criação do Storage Gateway. Para obter step-by-step procedimentos para criar um tipo específico de gateway usando o console do Storage Gateway, consulte os tópicos a seguir:

- Criar e ativar um Gateway de Arquivos para o Amazon S3
- Crie e ative um Amazon FSx File Gateway
- Criar e ativar um Gateway de Fitas
- Criar e ativar um novo Gateway de Volumes

> **Important**
>
> O Amazon FSx File Gateway não está mais disponível para novos clientes. Os clientes existentes do FSx File Gateway podem continuar usando o serviço normalmente. Para recursos semelhantes ao FSx File Gateway, visite esta postagem do blog.

Visão geral: ativação do gateway

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

Configurar um gateway

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

Conecte-se a AWS

A próxima etapa é conectar seu gateway com a AWS. Para fazer isso, primeiro você escolhe o tipo de endpoint de serviço que deseja usar para comunicações entre o dispositivo virtual do gateway

e AWS os serviços na nuvem. Este endpoint pode ser acessado pela Internet pública ou somente de dentro da sua Amazon VPC, onde você tem controle total sobre a configuração de segurança da rede. O endereço IP do gateway ou sua chave de ativação é especificado, que pode ser obtido ao se conectar ao console local no dispositivo de gateway.

Analisar e ativar

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

Visão geral: configuração do gateway

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

Visão geral: recursos de armazenamento

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

Crie um sistema de arquivos Amazon FSx para Windows File Server

Para criar um Amazon FSx File Gateway em AWS Storage Gateway, a primeira etapa é criar um sistema de arquivos Amazon FSx para Windows File Server. Se você já criou um sistema de FSx arquivos da Amazon, vá para a próxima etapa,Crie e ative um Amazon FSx File Gateway.

Note

As seguintes limitações se aplicam ao gravar em um sistema de FSx arquivos da Amazon a partir de um gateway de FSx arquivos:

- Seu sistema de FSx arquivos da Amazon e seu gateway de FSx arquivos devem pertencer à mesma AWS conta e estar localizados na mesma AWS região.
- Cada gateway pode aceitar cinco sistemas de arquivos anexados. Quando você está anexando um sistema de arquivos, o console do Storage Gateway notifica se o gateway selecionado está no limite da capacidade. Nesse caso, você deve escolher um gateway diferente ou desanexar um sistema de arquivos para poder anexar outro.
- FSx O File Gateway oferece suporte a cotas de armazenamento flexível (emitindo avisos quando os usuários ultrapassam seus limites de dados), mas não oferece suporte a cotas rígidas (impondo limites de dados negando o acesso de gravação). As cotas flexíveis são suportadas para todos os usuários, exceto o usuário FSx administrador da Amazon. Para obter mais informações sobre a configuração de cotas de armazenamento, consulte Cotas de armazenamento no Guia do usuário do Amazon FSx para Windows File Server.
- Não recomendamos o uso do Microsoft Distributed File System (DFS) para redirecionar os usuários para o sistema de arquivos da Amazon por meio FSx do FSx File Gateway. Em vez disso, configure o DFS para redirecionar diretamente para o sistema de FSx arquivos da Amazon Nuvem AWS conforme descrito em Agrupando vários sistemas de arquivos com namespaces do DFS no Guia do usuário do FSx Amazon para Windows File Server.
- Algumas operações de FSx arquivo no File Gateway, como renomeações de pastas de nível superior ou alterações de permissão, podem resultar em várias operações de arquivo que causam uma alta I/O carga no sistema de arquivos do Windows File Server. FSx Se seu sistema de arquivos não tiver recursos de desempenho suficientes para sua carga de trabalho, o sistema de arquivos poderá excluir cópias de sombra porque prioriza a disponibilidade da cópia contínua em I/O relação à retenção histórica de cópias paralelas.

  No FSx console da Amazon, verifique a página de monitoramento e desempenho para ver se seu sistema de arquivos está subprovisionado. Se estiver, você poderá mudar para o armazenamento de SSD, aumentar a capacidade de throughput ou aumentar o IOPS da SSD para lidar com sua workload.

Para criar um sistema de arquivos FSx para Windows File Server

1. Abra o Console de gerenciamento da AWS at https://console.aws.amazon.com/fsx/home/ e escolha a região na qual você deseja criar seu gateway.
2. Siga as instruções em Introdução à Amazon FSx no Guia do usuário do Amazon FSx para Windows File Server.

Crie e ative um Amazon FSx File Gateway

Nesta seção, é possível encontrar instruções sobre como criar, implantar e ativar um Gateway de Arquivos no AWS Storage Gateway.

Tópicos

- Configurar um Amazon FSx File Gateway
- Conecte seu Amazon FSx File Gateway a AWS
- Revise as configurações e ative seu Amazon FSx File Gateway
- Configure seu Amazon FSx File Gateway

Configurar um Amazon FSx File Gateway

Para configurar um novo gateway FSx de arquivos

1. Abra o Console de gerenciamento da AWS em https://console.aws.amazon.com/storagegateway/casa/ e escolha Região da AWS onde você deseja criar seu gateway.
2. Escolha Criar gateway para abrir a página Configurar gateway.
3. Na seção Configurações de gateway, faça o seguinte:

    a. Em Gateway name (Nome do gateway), insira um nome para o seu gateway. Depois de criar um gateway, você pode procurar esse nome para encontrar seu gateway nas páginas de lista no console do AWS Storage Gateway .

    b. Em Fuso horário do gateway, escolha o fuso horário local da parte do mundo em que você deseja implantar seu gateway.
4. Na seção Opções de gateway, em Tipo de gateway, escolha Amazon FSx File Gateway.
5. Na seção Opções de plataforma, faça o seguinte:

a. Em Plataforma host, escolha a plataforma na qual você deseja implantar seu gateway. Depois, siga as instruções específicas da plataforma exibidas na página do console do Storage Gateway para configurar a plataforma host. Você pode escolher entre as seguintes opções:

   - VMware ESXi— Baixe, implante e configure a máquina virtual do gateway usando VMware ESXi.
   - Microsoft Hyper-V: baixe, implante e configure a máquina virtual de gateway usando o Microsoft Hyper-V.
   - Linux KVM: baixe, implante e configure a máquina virtual de gateway usando a máquina virtual baseada em kernel (KVM). Consulte o aws-storage-gateway arquivo.xml fornecido para ver as configurações de inicialização sugeridas. O modo de inicialização UEFI com inicialização segura desativada (loader_secure=no) é necessário para o File Gateway 2.x, o Volume Gateway 3.x e o Tape Gateway 3.x.
   - Amazon EC2: configure e inicie uma instância do Amazon EC2 para hospedar seu gateway.
   - Dispositivo de hardware — Solicite um dispositivo de hardware físico dedicado AWS para hospedar seu gateway.

b. Em Confirmar configuração do gateway, marque a caixa de seleção para confirmar que você executou as etapas de implantação da plataforma host escolhida. Esta etapa não se aplica à plataforma host do dispositivo de hardware.

6. Agora que seu gateway está configurado, você deve escolher como deseja se conectar e se comunicar com ele AWS. Escolha Próximo para continuar.

Conecte seu Amazon FSx File Gateway a AWS

Para conectar um novo gateway FSx de arquivos ao AWS

1. Se você ainda não tiver feito isso, conclua o procedimento descrito em Configurar um Amazon FSx File Gateway. Ao terminar, escolha Avançar para abrir a AWS página Connect to no AWS Storage Gateway console.
2. Na seção Opções de endpoint, para Endpoint de serviço, escolha o tipo de endpoint com o qual seu gateway usará para se comunicar. AWS Você pode escolher entre as seguintes opções:

- Acessível ao público — Seu gateway se AWS comunica pela Internet pública. Se você selecionar essa opção, use a caixa de seleção Endpoint habilitado para FIPS para especificar se a conexão deve estar em conformidade com os padrões FIPS (Padrões Federais de Processamento de Informações).

  > **Note**
  >
  > Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint compatível com FIPS. Para obter mais informações, consulte Federal Information Processing Standard (FIPS – Norma federal de processamento de informações) 140-2.
  >
  > O endpoint de serviço de FIPS está disponível somente em algumas regiões da AWS . Para obter mais informações, consulte endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.

- VPC hospedado — Seu gateway se comunica AWS por meio de uma conexão privada com sua nuvem privada virtual (VPC), permitindo que você controle suas configurações de rede. Se você selecionar essa opção, deverá especificar um endpoint da VPC existente escolhendo seu ID de endpoint da VPC na lista suspensa. É possível também fornecer o endereço IP ou o nome do Sistema de Nomes de Domínio (DNS) do endpoint da VPC.

3. Na seção Opções de conexão do gateway, em Opções de conexão, escolha como identificar seu gateway na AWS. Você pode escolher entre as seguintes opções:

   - Endereço IP: forneça o endereço IP do seu gateway no campo correspondente. Este endereço IP deve ser público ou acessível de dentro da sua rede atual e você deve ser capaz de se conectar com ele do seu navegador da web.

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

   - Chave de ativação: forneça a chave de ativação do seu gateway no campo correspondente. É possível gerar uma chave de ativação usando o console local do gateway. Se o endereço IP do seu gateway não estiver disponível, escolha essa opção.

4. Agora que você escolheu como deseja que seu gateway se conecte AWS, você deve ativar o gateway. Escolha Próximo para continuar.

Revise as configurações e ative seu Amazon FSx File Gateway

Para ativar um novo gateway FSx de arquivos

1. Conclua os procedimentos descritos nos seguintes tópicos, caso ainda não o tenha feito isso:

   - Configurar um Amazon FSx File Gateway
   - Conecte seu Amazon FSx File Gateway a AWS

   Ao terminar, escolha Avançar para abrir a página Revisar e ativar no console do AWS Storage Gateway .
2. Revise os detalhes iniciais do gateway para cada seção na página.
3. Se uma seção contiver erros, escolha Editar para retornar à página de configurações correspondente e fazer as alterações.

   > **Important**
   >
   > Não é possível modificar as opções do gateway ou as configurações de conexão após a ativação do gateway.

4. Agora que ativou seu gateway, você precisa realizar a primeira configuração para alocar os discos de armazenamento local e configurar o registro em log. Escolha Próximo para continuar.

Configure seu Amazon FSx File Gateway

Para realizar a primeira configuração em um novo gateway de FSx arquivos

1. Conclua os procedimentos descritos nos seguintes tópicos, caso ainda não o tenha feito isso:

   - Configurar um Amazon FSx File Gateway
   - Conecte seu Amazon FSx File Gateway a AWS
   - Revise as configurações e ative seu Amazon FSx File Gateway

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

2. Na seção Configurar armazenamento, use as listas suspensas para alocar pelo menos um disco local com capacidade de pelo menos 150 gibibytes (GiB) para o cache. Os discos locais listados nesta seção correspondem ao armazenamento físico que você provisionou em sua plataforma host.
3. Na seção Grupo de CloudWatch registros, escolha como configurar o Amazon CloudWatch Logs para monitorar a integridade do seu gateway. Você pode escolher entre as seguintes opções:

   - Criar um novo grupo de logs: configure um novo grupo de logs para monitorar seu gateway.
   - Usar um grupo de logs existente: escolha um grupo de logs existente na lista suspensa correspondente.
   - Desative o registro — Não use o Amazon CloudWatch Logs para monitorar seu gateway.

   > **Note**
   >
   > Para receber os logs de integridade do Storage Gateway, as permissões a seguir devem estar presentes na política de recursos do grupo de logs. *highlighted section*Substitua o pelas informações específicas do grupo de registros ResourceArn para sua implantação.
   >
   > ```
   > "Sid": "AWSLogDeliveryWrite20150319",
   >       "Effect": "Allow",
   >       "Principal": {
   >         "Service": [
   >           "delivery.logs.amazonaws.com"
   >         ]
   >       },
   >       "Action": [
   >         "logs:CreateLogStream",
   >         "logs:PutLogEvents"
   >       ],
   >       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
   > ```
   >
   > O elemento “Recurso” é necessário somente se você quiser que as permissões sejam aplicadas explicitamente a um grupo de logs individual.

4. Na seção de CloudWatch alarmes, escolha como configurar os CloudWatch alarmes da Amazon para notificá-lo quando as métricas do seu gateway se desviam dos limites definidos. Você pode escolher entre as seguintes opções:

   - Crie os alarmes recomendados pelo Storage Gateway — Crie todos os CloudWatch alarmes recomendados automaticamente quando o gateway for criado. Para obter mais informações sobre os alarmes recomendados, consulte Entendendo os CloudWatch alarmes.

     > **Note**
     >
     > Esse recurso requer permissões CloudWatch de política que não são concedidas automaticamente como parte da política de acesso total pré-configurada do Storage Gateway. Certifique-se de que sua política de segurança conceda as seguintes permissões antes de tentar criar CloudWatch alarmes recomendados:
     >
     > - `cloudwatch:PutMetricAlarm`: criar alarmes
     > - `cloudwatch:DisableAlarmActions`: desativar as ações de alarme
     > - `cloudwatch:EnableAlarmActions`: ativar as ações de alarme
     > - `cloudwatch:DeleteAlarms`: excluir alarmes

   - Crie um alarme personalizado — Configure um novo CloudWatch alarme para ser notificado sobre as métricas do seu gateway. Escolha Criar alarme para definir métricas e especificar ações de alarme no CloudWatch console da Amazon. Para obter instruções, consulte Como usar CloudWatch alarmes da Amazon no Guia do CloudWatch usuário da Amazon.
   - Sem alarme — Não use CloudWatch alarmes para ser notificado sobre as métricas do seu gateway.

5. (Opcional) Na seção Tags, escolha Adicionar nova tag e, depois, insira um par de chave-valor com distinção entre maiúsculas e minúsculas para ajudar você a pesquisar e filtrar seu gateway nas páginas de listagem no console do AWS Storage Gateway . Repita esta etapa para adicionar quantas tags precisar.

6. (Opcional) Na seção Verificar configuração de VMware alta disponibilidade, se seu gateway estiver implantado em um VMware host que faz parte de um cluster de VMware alta disponibilidade (HA), escolha Verificar VMware HA para testar se a configuração de HA está funcionando corretamente.

> **Note**
>
> Esta seção aparece somente para gateways que estão sendo executados na plataforma VMware host.
> Essa etapa não é necessária para concluir o processo de configuração do gateway. É possível testar a configuração de HA do gateway a qualquer momento. A verificação leva alguns minutos e reinicia a máquina virtual (VM) do Storage Gateway.

7. Escolha Configurar para concluir a criação do gateway.

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

Agora que criou o gateway, você deve anexar um sistema de arquivos a ser usado por ele. Para obter instruções, consulte Anexar um sistema de arquivos Amazon FSx para Windows File Server.

Se você não tiver um sistema de FSx arquivos Amazon existente para anexar, deverá criar um. Para obter instruções, consulte Introdução à Amazon FSx.

Ativar um gateway em uma nuvem privada virtual

É possível criar uma conexão privada entre o dispositivo do gateway on-premises e a infraestrutura de armazenamento baseada em nuvem. Você pode usar essa conexão para ativar seu gateway e configurá-lo para transferir dados para serviços AWS de armazenamento sem se comunicar pela Internet pública. Usando o serviço Amazon VPC, você pode lançar AWS recursos, incluindo endpoints de interface de rede privada, em uma nuvem privada virtual (VPC) personalizada. Uma VPC dá controle para que você controle as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Para obter mais informações VPCs, consulte O que é Amazon VPC? no Guia do usuário da Amazon VPC.

Para ativar seu gateway em uma VPC, use o console da Amazon VPC para , criar um endpoint da VPC para o Storage Gateway e acessar o ID do endpoint da VPC e, depois, especificá-lo quando você criar e ativar o gateway. Para obter mais informações, consulte seu Amazon FSx File Gateway a. AWS

Para configurar seu gateway de FSx arquivos para transferir dados por meio da VPC, você deve estabelecer uma VPN ou um AWS DirectConnect link entre a VPC do Amazon FSx para Windows File Server e a rede em que seu gateway está implantado.

> **Note**
>
> O gateway deve ser ativado na mesma região em que você criou o endpoint da VPC para o Storage Gateway.

Como criar um endpoint da VPC para o Storage Gateway

Siga estas instruções para criar um VPC endpoint. Se você já tem um endpoint da VPC para o Storage Gateway, pode usá-lo.

Para criar um endpoint da VPC para o Storage Gateway

1. Faça login no Console de gerenciamento da AWS e abra o console da Amazon VPC em. https://console.aws.amazon.com/vpc/
2. No painel de navegação, selecione Endpoints e Criar endpoint.
3. Na página Criar Endpoint, selecione Serviços da AWS para Categoria de serviço.
4. Em 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 Habilitar nome de DNS não está selecionado.
7. Para Security group (Grupo de segurança), escolha o grupo de segurança que você deseja usar para a VPC. Você pode aceitar o grupo de segurança padrão. Verifique se todas as portas TCP a seguir são permitidas no seu grupo de segurança:
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Escolha Criar endpoint. O estado inicial do endpoint é pending (pendente). Quando o endpoint for criado, anote o ID do VPC endpoint que você acabou de criar.
9. Quando o endpoint for criado, escolha Endpoints e, depois, o novo VPC endpoint.

10. Na guia Detalhes do endpoint do gateway de armazenamento selecionado, em Nomes DNS, use o primeiro nome DNS que não especifique uma zona de disponibilidade. O nome DNS deve ser semelhante ao seguinte exemplo: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Agora que você tem um endpoint da VPC, poderá criar e ativar seu gateway. Para obter mais informações, consulte Criar e ativar um Amazon FSx File Gateway.

Para acessar informações sobre como recuperar uma chave de ativação, consulte Recuperar uma chave de ativação para seu gateway.

Definir as configurações de acesso do domínio do Microsoft Active Directory

Nesta etapa, você define as configurações de acesso para unir seu Amazon FSx File Gateway a um domínio do Microsoft Active Directory.

Como definir as configurações do Active Directory

1. No console do Storage Gateway, escolha sistemas de FSx arquivos no menu de navegação.
2. Escolha Anexar sistema de FSx arquivos.
3. Na página Confirmar gateway, escolha o gateway que você deseja associar ao seu domínio Active Directory no menu suspenso.

   Se você não tiver um gateway, crie um. Garanta que seu gateway possa resolver o nome do seu controlador de domínio Active Directory. Para mais informações, consulte Pré-requisitos.
4. Insira valores para as configurações do Active Directory:

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

   - Em Nome do domínio, insira o nome do domínio do Active Directory que você deseja usar.
   - Em Nome do domínio, insira o nome do usuário do Active Directory que você deseja usar para inserir o gateway no domínio. Esse usuário deve ter as permissões necessárias. Para acessar mais informações, consulte Requisitos de permissão da conta de serviço do Active Directory.
   - Em Senha do domínio, digite a senha do usuário.
   - Em Unidade organizacional - opcional, você pode especificar uma unidade organizacional à qual o Active Directory pertence.

     > **Note**
     >
     > Se você deixar esse campo em branco, a associação a um domínio criará uma conta de computador do Active Directory no contêiner de computadores padrão

(que não é uma UO), usando o ID do gateway como nome da conta (por exemplo, SGW-1234ADE). Não é possível personalizar o nome dessa conta.
Se o ambiente do Active Directory exigir que você prepare contas para facilitar o processo de ingresso no domínio, será necessário criar essa conta com antecedência.
Se seu ambiente do Active Directory tiver uma UO designada para novos objetos de computador, você deverá especificar essa UO ao ingressar no domínio.

- Insira um valor para Controladores de domínio: opcional.

5. Escolha Avançar para abrir a página Anexar sistema de FSx arquivos.

Próxima etapa

Anexe um sistema de arquivos Amazon FSx para Windows File Server

Anexe um sistema de arquivos Amazon FSx para Windows File Server

Você deve ter um sistema de arquivos FSx para Windows File Server antes de poder anexá-lo a um gateway de FSx arquivos. Se você não tiver um sistema de arquivos, crie um. Para obter instruções, consulte Etapa 1: Crie seu sistema de arquivos no Guia do usuário do Amazon FSx para Windows File Server.

A próxima etapa é conectar um sistema de FSx arquivos da Amazon ao gateway. Quando você anexa um sistema de FSx arquivos da Amazon, todos os compartilhamentos de arquivos no sistema de arquivos são disponibilizados para o Amazon FSx File Gateway (FSx File Gateway) para você montar.

> **Note**
>
> As seguintes limitações se aplicam ao gravar em um sistema de FSx arquivos da Amazon a partir do Amazon FSx File Gateway:
>
> - Seu sistema de FSx arquivos da Amazon e seu gateway de FSx arquivos devem pertencer ao mesmo Conta da AWS e estar localizados no mesmo Região da AWS.
> - Cada gateway pode comportar até cinco sistemas de arquivos anexados. Quando você está anexando um sistema de arquivos, o console do Storage Gateway notifica se o gateway selecionado está no limite da capacidade. Nesse caso, você deve escolher um gateway diferente ou desanexar um sistema de arquivos para poder anexar outro.
> - FSx O File Gateway oferece suporte a cotas de armazenamento flexível (que avisam quando os usuários ultrapassam seus limites de dados), mas não oferece suporte a cotas rígidas (que impõem limites de dados ao negar o acesso de gravação). As cotas flexíveis são suportadas para todos os usuários, exceto o usuário FSx administrador da Amazon. Para obter mais informações sobre a configuração de cotas de armazenamento, consulte Cotas de armazenamento no Guia FSx do usuário da Amazon.
> - Não recomendamos o uso do Microsoft Distributed File System (DFS) para redirecionar os usuários para o sistema de arquivos da Amazon por meio FSx do FSx File Gateway. Em vez disso, configure o DFS para redirecionar diretamente para o sistema de FSx arquivos da Amazon Nuvem AWS conforme descrito em Agrupando vários sistemas de arquivos com namespaces do DFS no Guia do usuário do FSx Amazon para Windows File Server.

Para anexar um sistema de FSx arquivos da Amazon

1. No console do Storage Gateway, na página Sistemas de FSx arquivos > Anexar sistema de FSx arquivos, preencha os seguintes campos na seção de configurações do sistema de FSx arquivos:

   - Em nome do sistema de FSx arquivos, escolha o sistema de arquivos que você deseja anexar na lista suspensa.
   - Em Endereço IP do Endpoint Local, insira o endereço IP do gateway que os clientes usarão para procurar compartilhamentos de arquivos no sistema de FSx arquivos.

   > **Note**
   >
   > - Você deve especificar um endereço IP para cada sistema de arquivos anexado ao gateway.
   > - Para os EC2 gateways da Amazon, você pode especificar o endereço IP privado da EC2 instância, a menos que ela já esteja sendo usada por um sistema de arquivos diferente. Nesse caso, você deve adicionar um novo endereço privado ao gateway e reiniciá-lo. Para obter mais informações, consulte Vários endereços IP no Guia do EC2 usuário da Amazon.
   > - Para gateways on-premises, você pode especificar o endereço IP da interface de rede primária (estática ou DHCP), a menos que ele já esteja sendo usado por um sistema de arquivos diferente. Nesse caso, você deve fornecer um endereço IP diferente da mesma sub-rede da interface primária, que será disponibilizado como um IP virtual. Não use um endereço IP atribuído a nenhuma interface de rede que não seja a primária.

2. Na seção Configurações da conta de serviço, forneça as credenciais de login da conta de serviço associadas ao sistema de arquivos da Amazon FSx .

   > **Note**
   >
   > Essa conta de serviço deve ter privilégios de Operadores de Backup do serviço Active Directory associado aos seus sistemas de FSx arquivos da Amazon ou ter permissões equivalentes.

> **Important**
>
> Para garantir permissões suficientes a arquivos, pastas e metadados de arquivos, recomendamos tornar a conta de serviço um membro do grupo de administradores do sistema de arquivos.
> Se você estiver usando o AWS Directory Service Microsoft Active Directory com o Amazon FSx for Windows File Server, a conta de serviço deverá ser membro do grupo FSx Administradores AWS Delegados.
> Se você estiver usando um Active Directory autogerenciado com o Amazon FSx para Windows File Server, recomendamos que a conta de serviço seja membro do grupo personalizado de administradores de sistemas de arquivos delegados que você especificou para administração do sistema de arquivos ao criar seu sistema de arquivos Amazon FSx .
> Se você optou por não criar um grupo personalizado de administradores de sistemas de arquivos delegados ao criar o sistema de FSx arquivos da Amazon, o grupo padrão é Administradores de domínio. Embora você possa transformar a conta de serviço em um membro desse grupo, o procedimento não é indicado como prática recomendada.
> Para obter mais informações, consulte Delegar privilégios à sua conta de FSx serviço da Amazon no Guia do usuário do Amazon FSx para Windows File Server.

3. Na seção Registros de auditoria, escolha Grupos de registros existentes e escolha o registro que você deseja usar para monitorar o acesso ao seu sistema de FSx arquivos da Amazon. Você pode criar outro. Para não monitorar o sistema, selecione Desabilitar registro em log.
4. Em Configuração da atualização automatizada do cache, se quiser que seu cache seja atualizado automaticamente, selecione Definir intervalo de atualização e especifique um intervalo entre 5 minutos e 30 dias.
5. (Opcional) Na seção Tags, escolha Adicionar nova tag para adicionar uma ou mais chaves e um valor para marcar suas definições.
6. Escolha Next (Avançar) e analise as configurações. Para alterar suas configurações, você pode selecionar Editar em cada seção.
7. Quando terminar, escolha Concluir.

Próxima etapa

Monte e use seu compartilhamento de FSx arquivos da Amazon

Monte e use seu compartilhamento de FSx arquivos da Amazon

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

Tópicos

Montar o compartilhamento de arquivos SMB no cliente

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

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

- O comando `net use`: não é preservado em reinicializações do sistema, a menos que você use a opção `/persistent:(yes:no)`.
- Utilitário de linha de comandos `CmdKey`: cria uma conexão persistente com um compartilhamento de arquivos SMB montado que permanece após uma reinicialização.
- Uma unidade de rede associada no Explorador de Arquivos: configura o compartilhamento de arquivos montado no login de reconexão e para exigir que você insira suas credenciais de rede.
- PowerShell script — 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, confira 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 oferece suporte ao bloqueio SMB ou aos atributos estendidos do 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 do prompt de comando.
2. Abra o menu de contexto (clique com o botão direito do mouse) de Prompt de comando e escolha Executar como administrador.
3. Digite o comando:

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

> **Note**
>
> Ao montar os compartilhamentos de arquivos, é provável que você precise montar novamente o compartilhamento de arquivos ao reinicializar seu cliente.

Para montar um compartilhamento de arquivos SMB usando Windows File Explorer

1. Pressione a tecla Windows e digite **File Explorer** na caixa Pesquisa do Windows ou pressione **Win+E**.
2. No painel de navegação, escolha Este PC. Depois, na guia Computador, escolha Associar unidade de rede.
3. Na caixa de diálogo Associar unidade de rede, escolha uma letra de unidade em Unidade.

4. Para Pasta, digite ***[File Gateway IP]**[SMB File Share Name]*** ou selecione Procurar para escolher seu compartilhamento de arquivos SMB na caixa de diálogo.
5. (Opcional) Selecione Reconectar ao entrar se quiser que seu ponto de montagem persista após reinicializações.
6. (Opcional) Selecione 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.
7. Escolha Finalizar para concluir o ponto de montagem.

Teste seu gateway FSx de arquivos

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

Para fazer upload de arquivos do seu cliente Windows para a 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 sistema de arquivos.
2. Copie arquivos ou um diretório para a unidade.

> **Note**
>
> Os Gateways de Arquivos não oferecem suporte à criação de links físicos ou simbólicos em um compartilhamento de arquivos.

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 Gateway), incluindo anexar e desanexar sistemas de FSx arquivos da Amazon e definir as configurações do Microsoft Active Directory.

Tópicos

Noções básicas sobre o status do gateway

Cada gateway na implantação do AWS Storage Gateway tem um status associado que informa rapidamente qual é a integridade do gateway. Na maior parte do tempo, o status indica que o gateway está funcionando normalmente e que nenhuma ação é necessária de sua parte. Em alguns casos, o status indica um problema com que pode ou não exigir uma ação de sua parte.

Você pode ver o status de cada gateway em sua implantação na página Gateways do console do Storage Gateway. O status do gateway aparece na coluna Status ao lado do nome do gateway. O status do gateway que está funcionando normalmente é `RUNNING`.

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

Status	Significado
`RUNNING`	O gateway está configurado corretamente e disponível para uso.
`OFFLINE`	Seu gateway pode estar sendo exibido como `OFFLINE` por um ou mais dos seguintes motivos:

Status	Significado
	• O gateway não consegue alcançar os endpoints do serviço Storage Gateway. • O gateway teve um desligamento inesperado. • Um gateway tem um disco de cache associado que foi desconectado, modificado ou falhou.

Noções básicas de status do sistema de arquivos

Você pode visualizar rapidamente a integridade de um sistema de arquivos observando seu status. Se o status indicar que o sistema de arquivos está funcionando normalmente, nenhuma ação será necessária de sua parte. Se o status indicar que há um problema, você poderá investigar para determinar se uma ação pode ser necessária.

Você pode visualizar o status de um sistema de arquivos no console do Storage Gateway, na coluna Status. Um sistema de arquivos que está funcionando corretamente mostra o status DISPONÍVEL. Esse deve ser o status na maioria das vezes.

A tabela a seguir descreve os status de compartilhamentos de arquivos, o que eles significam e se uma ação pode ser necessária.

Status	Significado
DISPONÍVEL	O sistema de arquivos está configurado corretamente e disponível para uso. Esse é o status padrão de um sistema de arquivos que está funcionando corretamente.
CRIANDO	O sistema de arquivos ainda não foi totalmente criado e não está pronto para uso. O status CREATING é transitório. Nenhuma ação é necessári a. Se o sistema de arquivos ficar preso nesse status, provavelmente é porque a VM do gateway perdeu a AWS conexão com.
ATUALIZANDO	A configuração do sistema de arquivos está sendo atualizada no momento. O status ATUALIZANDO é transitório. Nenhuma ação é necessária. Se um sistema de arquivos ficar preso nesse status, provavelmente é porque a VM do gateway perdeu a AWS conexão com.

Status	Significado
EXCLUINDO	O compartilhamento de arquivos está sendo excluído. O sistema de arquivos não é excluído até que todos os dados sejam enviados para AWS o. O status DELETING é transitório e nenhuma ação é necessária.
FORCE_DELETING	O sistema de arquivos está sendo excluído à força. O sistema de arquivos é excluído imediatamente e os dados não são enviados para AWS. O status FORCE_DELETING é transitório e nenhuma ação é necessária.
ERRO	O sistema de arquivos encontra-se em um estado corrompido. É necessário realizar uma ação. Algumas causas possíveis são problemas com credenciais ou privilégios de acesso, problemas de conectividade ou espaço de armazenamento insuficiente no sistema de arquivos. Quando o problema que provocou esse estado corrompido é resolvido, o sistema de arquivos volta para o estado AVAILABLE.

Editar informações básicas para um gateway FSx de arquivos

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

Para editar informações básicas de um gateway existente

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Gateways e escolha o gateway para o qual você deseja editar as informações básicas.
3. No menu suspenso Ações, escolha Editar informações do gateway.
4. Em Gateway name (Nome do gateway), insira um nome para o seu gateway. É possível pesquisar esse nome para encontrar o gateway nas páginas de listagem no console do Storage Gateway.

> **Note**
>
> Os nomes de gateway devem ter entre 2 e 255 caracteres e não podem incluir uma barra (\ ou /).

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

5. Em Fuso horário do gateway, escolha o fuso horário local da parte do mundo em que você deseja implantar seu gateway.
6. Em Escolha como configurar o grupo de registros, 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.
   - Usar um grupo de logs existente: escolha um grupo de logs existente na lista suspensa correspondente.
   - Desative o registro — Não use o Amazon CloudWatch Logs para monitorar seu gateway.
7. Quando terminar de modificar as definições que pretende alterar, escolha Salvar alterações.

Configurar um nível de segurança para o gateway

Você pode configurar o nível de segurança SMB para seu gateway de FSx arquivos para especificar se o gateway deve exigir assinatura SMB (Server Message Block) ou criptografia SMB.

Para configurar os níveis segurança

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Gateways e selecione o gateway para o qual deseja editar as configurações de SMB.
3. No menu suspenso Ações, escolha Editar configurações do SMB e selecione Configurações de segurança do SMB.
4. Em Security level (Nível de segurança), escolha uma das seguintes opções:

> **Note**
>
> Para obter informações sobre como definir essa configuração usando a AWS API, consulte SMBSecurityEstratégia de atualização na Referência da AWS Storage Gateway API.
>
> Um nível de segurança mais alto pode afetar a performance do gateway.

- Criptografia obrigatória — Se você escolher essa opção, o FSx File Gateway só permitirá conexões de SMBv3 clientes que usam algoritmos de criptografia AES de 256 bits. Algoritmos de 128 bits não são permitidos. Essa opção é altamente recomendada para ambientes que trabalham com dados sensíveis. Ela funciona com clientes SMB no Microsoft Windows 8, no Windows Server 2012 ou posterior.
- Impor criptografia — Se você escolher essa opção, o FSx File Gateway só permitirá conexões de SMBv3 clientes que tenham a criptografia ativada. Tanto algoritmos de 256 bits quanto de 128 bits são permitidos. Essa opção é altamente recomendada para ambientes que trabalham com dados sensíveis. Ela funciona com clientes SMB no Microsoft Windows 8, no Windows Server 2012 ou posterior.
- Impor assinatura — Se você escolher essa opção, o FSx File Gateway só permitirá conexões de SMBv2 ou SMBv3 clientes que tenham a assinatura ativada. Essa opção funciona com clientes SMB no Microsoft Windows Vista, no Windows Server 2008 ou posterior.

> **Note**
>
> O nível de segurança padrão para o FSx File Gateway é Enforce encryption.

5. Escolha Salvar.

Editando configurações do Active Directory para n FSx File Gateway

Para usar seu Microsoft Active Directory corporativo ou AWS Managed Microsoft AD para acesso autenticado pelo usuário ao seu sistema de FSx arquivos da Amazon, edite as configurações de SMB para seu gateway e forneça suas credenciais de domínio do Active Directory. Isso permite que seu gateway ingresse no domínio de seu Active Directory e permite que os membros do domínio acessem o sistema de arquivos.

> **Note**
>
> Usando Directory Service, você pode criar um serviço de domínio do Active Directory hospedado no Nuvem AWS.

Para usar AWS Managed Microsoft AD com um gateway do Amazon EC2, você deve criar a instância do Amazon EC2 na mesma VPC do, adicionar o grupo de segurança AWS Managed Microsoft AD_WorkspaceMembers à instância do Amazon EC2 e ingressar no domínio AD usando as credenciais de administrador do. AWS Managed Microsoft AD
Para obter mais informações sobre AWS Managed Microsoft AD, consulte o Guia de AWS Directory Service administração.
Para acessar mais informações sobre o Amazon EC2, consulte a Documentação do Amazon Elastic Compute Cloud.

Como ativar a autenticação do Active Directory

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Gateways e selecione o gateway para o qual deseja editar as configurações de SMB.
3. No menu suspenso Ações, escolha Editar configurações do SMB e selecione Configurações do Active Directory.
4. Em Nome do domínio, insira o nome do domínio do Active Directory ao qual deseja associar o gateway.

> **Note**
>
> Active Directory status (Status do Active Directory) mostra Detached (Desanexado) quando um gateway nunca ingressou em um domínio.
> Sua conta de serviço do Active Directory deve ter as permissões necessárias. Para obter mais informações, consulte Requisitos de permissão da conta de serviço do Active Directory.
> A associação a um domínio criará uma conta de computador do Active Directory no contêiner de computadores padrão (que não é uma UO) usando o ID do gateway como nome da conta (por exemplo, SGW-1234ADE). Não é possível personalizar o nome dessa conta.
> Se o ambiente do Active Directory exigir que você prepare contas para facilitar o processo de ingresso no domínio, será necessário criar essa conta com antecedência.
> Se seu ambiente do Active Directory tiver uma UO designada para novos objetos de computador, você deverá especificar essa UO ao ingressar no domínio.
> Se seu gateway não conseguir ingressar em um diretório do Active Directory, tente se unir ao endereço IP do diretório usando a operação de JoinDomainAPI.

5. Em Usuário do domínio e Senha do domínio, insira as credenciais da conta de serviço do Active Directory que o gateway usará para ingressar no domínio.
6. (Opcional) Em Unidade organizacional (UO), insira a UO designada que seu Active Directory usa para novos objetos de computador.
7. (Opcional) Para controlador (es) de domínio (DC), insira o nome de um ou mais DCs por meio dos quais seu gateway se conectará ao Active Directory. Você pode inserir vários DCs como uma lista separada por vírgulas. Você pode deixar esse campo em branco para permitir que o DNS selecione automaticamente um DC.
8. Escolha Salvar alterações.

Editando configurações para um sistema de FSx arquivos da Amazon

Depois de criar um sistema de arquivos Amazon FSx para Windows File Server, você pode editar as configurações dos CloudWatch registros, da atualização automática do cache e das credenciais da conta de FSx serviço da Amazon.

Para editar as configurações do sistema FSx de arquivos da Amazon

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, escolha Sistema de arquivos e selecione o sistema de arquivos cujas configurações você deseja editar.
3. Em Ações, escolha Editar configurações do sistema de arquivos.
4. Na seção de configurações do sistema de arquivos, verifique o gateway, a FSx localização da Amazon e as informações de endereço IP.

   > **Note**
   >
   > Não é possível editar o endereço IP de um sistema de arquivos depois que ele é anexado a um gateway. Para alterar o endereço IP, você deve desanexar e reanexar o sistema de arquivos.

5. Na seção Registros de auditoria, escolha uma opção para usar grupos de CloudWatch registros para monitorar o acesso aos sistemas de FSx arquivos da Amazon. Você pode usar um grupo existente.

6. Em Configurações de atualização automática de cache, escolha uma opção. Se você escolher Definir intervalo de recuperação, defina o tempo em dias, horas e minutos para atualizar o cache do sistema de arquivos usando a vida útil (TTL).

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

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

7. Na seção Configurações da conta de serviço: opcional, insira um nome de usuário e uma senha. Essas credenciais são para um usuário que tem a função de Administrador de Backup do serviço Active Directory associado aos seus sistemas de FSx arquivos da Amazon.
8. Escolha Salvar alterações.

Separando um sistema de FSx arquivos da Amazon

Desanexar um sistema de arquivos não exclui seus dados no FSx Windows File Server. Os dados gravados nesses sistemas de arquivos antes de você separá-los ainda serão carregados no seu servidor FSx de arquivos do Windows.

Para separar um sistema de FSx arquivos da Amazon

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha sistemas de FSx arquivos e, em seguida, selecione um ou mais sistemas de arquivos para desanexar.
3. Para Ações, escolha Desanexar sistema de arquivos. Uma caixa de diálogo de confirmação é exibida.
4. Verifique se você deseja desanexar os sistemas de arquivos especificados, depois, digite a palavra desanexar na caixa de confirmação e escolha Desanexar.

Como monitorar o Storage Gateway

Os tópicos desta seção descrevem como monitorar um gateway usando a Amazon CloudWatch, incluindo o monitoramento do armazenamento em cache e outros recursos associados ao gateway. O console do Storage Gateway é usado para visualizar métricas e alarmes do gateway. Por exemplo, você pode ver o número de bytes usados em operações de leitura e gravação, o tempo gasto em operações de leitura e gravação e o tempo gasto para recuperar dados da AWS nuvem. Com essas métricas, você pode acompanhar a integridade de seu gateway e definir alarmes para notificá-lo quando uma ou mais métricas afastarem-se de um limite definido.

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

Tópicos

- Entendendo os CloudWatch alarmes- Aprenda informações básicas sobre CloudWatch alarmes, incluindo estados de alarme e configurações recomendadas.
- Crie CloudWatch alarmes recomendados- Saiba como você pode configurar de forma rápida e automática todos os CloudWatch alarmes recomendados como parte do processo inicial de configuração do File Gateway.
- Crie um CloudWatch alarme personalizado- Saiba como você pode criar um CloudWatch alarme personalizado para monitorar uma métrica específica usando critérios de avaliação específicos para acionar estados de alarme e enviar notificações.
- Monitorando seu gateway de de FSx arquivos- Aprenda a visualizar CloudWatch registros e registros de auditoria e encontrar informações sobre as métricas específicas do gateway e do sistema de arquivos de compartilhamento de arquivos que são relatadas pelo seu gateway.

Entendendo os CloudWatch alarmes

CloudWatch os alarmes monitoram informações sobre seu gateway com base em métricas e expressões. Você pode adicionar CloudWatch alarmes ao seu gateway e visualizar seus status

no console do Storage Gateway. Para obter mais informações sobre as métricas usadas para monitorar o , consulte do gateway e Compreendendo as métricas de do sistema de arquivos. Para cada alarme, você especifica as condições que ativarão o estado ALARM. Os indicadores de status do alarme no console do Storage Gateway ficam vermelhos quando estão no estado ALARM, facilitando o monitoramento proativo do status. É possível configurar alarmes para invocar ações automaticamente com base em mudanças sustentadas no estado. Para obter mais informações sobre CloudWatch alarmes, consulte Usando CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.

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

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

- Espera alta de E/S: `IoWaitpercent` >= 20 para 3 pontos de dados em 15 minutos
- Percentual de cache sujo: `CachePercentDirty` > 80 para 4 pontos de dados em 20 minutos
- Falha no upload de arquivos: `FilesFailingUpload` >= 1 para 1 ponto de dados em 5 minutos.
- Erro no sistema de arquivos: `FileSystem-ERROR` >= 1 para 1 ponto de dados em 5 minutos.
- Notificações de integridade: `HealthNotifications` >= 1 para 1 ponto de dados em 5 minutos. Ao configurar esse alarme, defina Tratamento de dados ausentes como notBreaching.

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

Para gateways em plataformas de VMware host que fazem parte de um cluster de VMware alta disponibilidade, também recomendamos este CloudWatch alarme adicional:

- Notificações de disponibilidade: `AvailabilityNotifications` >= 1 para 1 ponto de dados em 5 minutos. Ao configurar esse alarme, defina Tratamento de dados ausentes como notBreaching.

A tabela a seguir descreve os estados CloudWatch de alarme.

Estado	Description
OK	A métrica ou a expressão está dentro do limite definido.
Alarme	A métrica ou a expressão está fora do limite definido.
Dados insuficientes	O alarme acabou de ser acionado, a métrica não está disponível ou não há dados suficient es para a métrica determinar o estado do alarme.
Nenhum	Nenhum alarme foi criado para o gateway. Para criar um alarme, consulte Crie um CloudWatch alarme personalizado para seu gateway.
Indisponível	O estado do alarme é desconhecido. Escolha Indisponível para visualizar informações de erro na guia Monitoramento.

Criação de CloudWatch alarmes recomendados para seu gateway

Ao criar um novo gateway usando o console do Storage Gateway, você pode optar por criar todos os CloudWatch alarmes recomendados automaticamente como parte do processo de configuração inicial. Para obter mais informações, consulte . Se você quiser adicionar ou atualizar CloudWatch os alarmes recomendados para um gateway existente depois de já ter concluído a primeira configuração, use o procedimento a seguir.

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

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

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

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

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

Crie um CloudWatch alarme personalizado para seu gateway

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

Para criar um CloudWatch alarme no console do Storage Gateway

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa/.
2. No painel de navegação, escolha Gateways e o gateway para o qual você deseja criar um alarme.
3. Na página de detalhes do gateway, selecione a guia Monitoramento.
4. Em Alarmes, escolha Criar alarme para abrir o CloudWatch console.

5. Use o CloudWatch console para criar o tipo de alarme que você deseja. É possível criar os seguintes tipos de alarmes:

   - Alarme de limite estático: um alarme baseado em um limite definido para uma métrica escolhida. O alarme entra no estado ALARM quando a métrica atinge o limite de um número especificado de períodos de avaliação.

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

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

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

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

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

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

     Para criar um alarme composto, consulte Criação de um alarme composto no Guia CloudWatch do usuário da Amazon.

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

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

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

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

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

Para obter informações sobre como editar ou excluir um alarme, consulte Editando ou excluindo um CloudWatch alarme.

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

Monitorando seu gateway de de FSx arquivos

Você pode monitorar o File Gateway e os recursos associados AWS Storage Gateway usando CloudWatch métricas e registros de auditoria da Amazon. Você também pode usar CloudWatch Eventos para ser notificado quando suas operações de arquivo forem concluídas.

Tópicos

- Obtendo registros de integridade do File Gateway com grupos CloudWatch de registros
- Usando CloudWatch métricas da Amazon
- Noções básicas de métricas de gateway
- Noções básicas de métricas de sistema
- Compreendendo os registros de auditoria do File Gateway

Obtendo registros de integridade do File Gateway com grupos CloudWatch de registros

Você pode usar o Amazon CloudWatch Logs para obter informações sobre a integridade do seu e recursos relacionados. É possível usar os logs para monitorar o gateway em busca de erros encontrados. Além disso, você pode usar filtros de CloudWatch assinatura da Amazon para automatizar o processamento das informações de log em tempo real. Para obter mais informações, consulte Processamento em tempo real de dados de log com assinaturas no Guia CloudWatch do usuário da Amazon.

Por exemplo, você pode configurar um grupo de CloudWatch registros para monitorar seu gateway e ser notificado quando o FSx File Gateway falhar ao fazer upload de arquivos para um sistema de FSx arquivos da Amazon. É possível configurar o grupo quando estiver ativando o gateway ou depois que ele estiver ativado e em execução. Para obter informações sobre como configurar um grupo de logs do CloudWatch ao ativar um gateway, consulte Configure seu Amazon FSx File Gateway. Para obter informações gerais sobre grupos de CloudWatch registros, consulte Como trabalhar com grupos de registros e fluxos de registros no Guia do CloudWatch usuário da Amazon.

Para obter informações sobre como solucionar os erros que podem ser relatados pelo , consulte. Solução de problemas: problemas no Gateway de Arquivos

Configurando um grupo de CloudWatch registros após a ativação do gateway

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

Para configurar um grupo de CloudWatch registros para trabalhar com seu

1. Faça login Console de gerenciamento da AWS e abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, escolha Gateways e, em seguida, escolha o gateway para o qual você deseja configurar o grupo de CloudWatch registros.
3. Em Ações, selecione Editar informações do gateway.
4. Em Escolher como configurar o grupo de logs, escolha uma das seguintes opções:

   - Crie um novo grupo de registros para criar um novo grupo de CloudWatch registros.
   - Use um grupo de registros existente para usar um grupo de CloudWatch registros que já existe.

Escolha um grupo de logs na Lista de grupos de logs existentes.

- Desative o registro se você não quiser monitorar seu gateway usando grupos de CloudWatch registros.

5. Escolha Salvar alterações.
6. Para obter os logs de integridade do gateway, faça o seguinte:

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

Usando CloudWatch métricas da Amazon

Você pode obter dados de monitoramento para o File Gateway usando a API Console de gerenciamento da AWS ou a CloudWatch API. O console exibe uma série de gráficos com base nos dados brutos da CloudWatch API. A CloudWatch API também pode ser usada por meio de uma das ferramentas AWS SDKsde CloudWatch API da Amazon. Dependendo das necessidades, você pode preferir usar os gráficos exibidos no console ou recuperados da API.

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

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

A tabela a seguir resume que tipo de dados de métrica do Storage Gateway estão disponíveis.

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

- Visualizando métricas disponíveis
- Obter estatísticas para uma métrica
- Criar alarmes do CloudWatch

Noções básicas de métricas de gateway

A tabela a seguir descreve as métricas que abrangem os gateways de FSx arquivos. Cada gateway tem um conjunto de métricas associadas a ele. Algumas métricas específicas do gateway têm o mesmo nome de determinadas métricas. file-system-specific Essas métricas representam medições do mesmo tipo, mas são dimensionadas para o gateway, não para o sistema de arquivos.

Sempre especifique 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 indicar o `Gateway Name` para o gateway cujos dados de métrica deseja visualizar. Para obter mais informações, consulte Usando CloudWatch métricas da Amazon.

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

A tabela a seguir descreve as métricas que você pode usar para obter informações sobre o s.

Métrica	Description
`AvailabilityNotifications`	Essa métrica relata o número de notificações de integridade relacionadas à disponibilidade que foram geradas pelo gateway no período do relatório. Unidades: contagem
`CacheDirectorySize`	Essa métrica monitora o tamanho das pastas no cache do gateway. O tamanho da pasta é definido pelo número de arquivos e subpastas em seu primeiro nível. Isso não é contado de forma recursiva nas subpastas. Use essa métrica com a estatística `Average` para medir o tamanho médio de uma pasta no cache do gateway. Use essa métrica com a estatística `Max` para medir o tamanho máximo de uma pasta no cache do gateway. Unidades: contagem
`CacheFileSize`	Essa métrica monitora o tamanho dos arquivos no cache do gateway. Use essa métrica com a estatística `Average` para medir o tamanho médio de um arquivo no cache do gateway. Use essa métrica com a estatística `Max` para medir o tamanho máximo de um arquivo no cache do gateway.

Métrica	Description
	Unidades: bytes
`CacheFree`	Essa métrica relata o número de bytes disponíveis no cache do gateway. Unidades: bytes
`CacheHitPercent`	Porcentagem de operações de leitura da aplicação do gateway que são feitas pelo cache. A amostra é capturada no final do período do relatório. Quando não há operações de leitura da aplicação do gateway, essa métrica relata 100%. Unidades: percentual
`CachePercentDirty`	A porcentagem geral do cache do gateway que não persistiu. AWS 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 relata o número de bytes utilizado s no cache do gateway. Unidades: bytes

Métrica	Description
`CloudBytesDownloaded`	O número total de bytes dos quais o gateway foi baixado AWS durante o 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
`CloudBytesUploaded`	O número total de bytes para os quais o gateway foi carregado AWS durante o período do relatório. Use essa métrica com a `Sum` estatística para medir a taxa de transferência e com a `Samples` estatística para medir as input/output operações por segundo (IOPS). Unidades: bytes
`FilesFailingUpload`	Essa métrica monitora o número de arquivos cujo upload não está sendo feito para a AWS. Esses arquivos vão gerar notificações de integridade que contêm mais informações sobre o problema. Use essa métrica com a estatística `Sum` para mostrar o número de arquivos cujo upload não está sendo feito para a AWS no momento. Unidades: contagem
`FileShares`	Essa métrica relata o número de compartil hamentos de arquivos no gateway. Unidades: contagem

Métrica	Description
`FileSystem-ERROR`	Essa métrica fornece o número de associações do sistema de arquivos nesses gateways que estão no estado ERROR. Se essa métrica relata que alguma associaçã o do sistema de arquivos está no estado ERROR, é provável que haja um problema com o gateway que possa causar interrupções no seu fluxo de trabalho. É recomendável criar um alarme para quando essa métrica informa um valor diferente de zero. Unidades: contagem
`HealthNotifications`	Essa métrica relata o número de notificações de integridade que foram geradas pelo gateway no período do relatório. Unidades: contagem
`IndexEvictions`	Essa métrica informa o número de arquivos cujos metadados foram removidos do índice de metadados de arquivos armazenado em cache para liberar espaço para novas entradas. O gateway mantém esse índice de metadados, que é preenchido a partir da AWS nuvem sob demanda. Unidades: contagem
`IndexFetches`	Essa métrica informa o número de arquivos para os quais os metadados foram recuperad os. O gateway mantém um índice em cache dos metadados do arquivo, que é preenchido a partir da AWS nuvem sob demanda. Unidades: contagem

Métrica	Description
`IoWaitPercent`	Essa métrica informa a porcentagem de tempo que a CPU está aguardando uma resposta do disco local. Unidades: percentual
`MemTotalBytes`	Essa métrica relata a quantidade total de memória no gateway. Unidades: bytes
`MemUsedBytes`	Essa métrica relata a quantidade de memória usada no gateway. Unidades: bytes
`RootDiskFreeBytes`	Essa métrica relata o número de bytes disponíveis no disco raiz do gateway. Se essa métrica indicar que menos de 20 GB estão livres, você deverá aumentar o tamanho do disco raiz. Para isso, você pode aumentar o tamanho do disco raiz existente na VM. Quando a VM é reinicializada, o gateway reconhece o tamanho aumentado no disco raiz. Unidades: bytes

Métrica	Description
SmbV2Sessions	Essa métrica relata o número de SMBv2 sessões que estão ativas no gateway. Essa métrica é emitida uma vez para cada sistema de arquivos associado ao gateway. Use a estatística SUM para calcular o número total de SMBv2 sessões ativas em todos os sistemas de arquivos. Unidades: contagem
SmbV3Sessions	Essa métrica relata o número de SMBv3 sessões que estão ativas no gateway. Essa métrica é emitida uma vez para cada sistema de arquivos associado ao gateway. Use a estatística SUM para calcular o número total de SMBv3 sessões ativas em todos os sistemas de arquivos. Unidades: contagem
TotalCacheSize	Essa métrica relata o tamanho total do cache. Unidades: bytes
UserCpuPercent	Essa métrica relata a porcentagem de tempo gasto no processamento do gateway. Unidades: percentual

Noções básicas de métricas de sistema

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

Sempre especifique se deseja trabalhar com uma métrica de gateway ou de sistema de arquivos, antes de trabalhar com métricas. Especificamente, ao trabalhar com métricas de sistema de arquivos, é necessário especificar o `File system ID`, que identifica o sistema de arquivos cujas métricas você tem interesse em visualizar. Para obter mais informações, consulte Usando CloudWatch métricas da Amazon.

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

A tabela a seguir descreve as métricas do Storage Gateway que podem ser usadas para acessar informações sobre os compartilhamentos de arquivos.

Métrica	Description
`CacheHitPercent`	Porcentagem de operações de leitura da aplicação 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 da aplicação do compartilhamento de arquivos, essa métrica relata 100%. Unidades: percentual
`CachePercentDirty`	A contribuição do compartilhamento de arquivos para o percentual geral do cache do gateway não mantido na AWS. A amostra é capturada no final do período do relatório. Use essa métrica com a estatística `Sum`. Preferencialmente, essa métrica deve permanecer baixa.

Métrica	Description
	Note Use a métrica `CachePercentDirty` do gateway para visualizar o percentual geral do cache do gateway que não é mantido na AWS. Unidades: percentual
`CachePercentUsed`	A porcentagem do cache de dados usado em todo o gateway. A amostra é capturada no final do período do relatório. Essa métrica específica do compartilhamento de arquivos relata o mesmo valor que a métrica específica do gateway correspondente. Unidades: percentual
`CloudBytesUploaded`	O número total de bytes para os quais o gateway foi carregado AWS durante o período do relatório. Use essa métrica com a estatística `Sum` para medir a taxa de transferência e com a estatística `Samples` para medir IOPS. Unidades: bytes

Métrica	Description
`CloudBytesDownloaded`	O número total de bytes dos quais o gateway foi baixado AWS durante o período do relatório. Use essa métrica com a `Sum` estatística para medir a taxa de transferência e com a `Samples` estatística para medir as input/output operações por segundo (IOPS). Unidades: bytes
`FilesFailingUpload`	Essa métrica monitora o número de arquivos cujo upload não está sendo feito para a AWS. Esses arquivos vão gerar notificações de integridade que contêm mais informações sobre o problema. Use essa métrica com a estatística `Sum` para mostrar o número de arquivos cujo upload não está sendo feito para a AWS no momento. Unidades: contagem
`ReadBytes`	O número total de bytes lidos das aplicações on-premises 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

Métrica	Description
`WriteBytes`	O número total de bytes gravados nos aplicativos locais no período do relatório. Use essa métrica com a estatística `Sum` para medir a taxa de transferência e com a estatística `Samples` para medir IOPS. Unidades: bytes

Compreendendo os registros de auditoria do File Gateway

Os logs de auditoria FSx do Amazon FSx File Gateway (File Gateway) fornecem detalhes sobre o acesso do usuário aos arquivos e pastas dentro de uma associação de sistema 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 compatibilidade com as ferramentas de processamento de log existentes para eventos de segurança do Windows.

Operações

A tabela a seguir descreve as operações de acesso ao File Gateway File Gateway.

Nome da 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.
Delete	Exclua um arquivo ou uma pasta.
Atributos de gravação	Atualize os metadados do arquivo ou da pasta (proprietárioACLs, grupo, permissões).

Atributos.

A tabela a seguir descreve os atributos de acesso ao FSx arquivo de log de auditoria do 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.
`SubjectUserName`	O nome de usuário do cliente do Active Directory.
`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.

Atributo	Definição
`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 em log (as falhas são registradas em log, 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 em log por operação

A tabela a seguir descreve os atributos do 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

	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)
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						
versic	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						
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

	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)
`fileSi nBytes`				X						

Manter seu gateway

Manter seu Amazon FSx File Gateway envolve fazer manutenção geral para otimizar o desempenho do seu gateway. Essas tarefas são comuns a todos os tipos de gateway.

Esta seção contém os seguintes tópicos, que descrevem conceitos e procedimentos relacionados à manutenção do Amazon FSx File Gateway Amazon Gateway:

Tópicos

- Como gerenciar atualizações de gateway: saiba como ativar ou desativar as atualizações de manutenção e modificar o cronograma da janela de manutenção do Gateway de Arquivos.
- Como executar tarefas de manutenção usando o console local: saiba como realizar tarefas de manutenção usando o console local do gateway.
- Encerrar a VM do gateway: saiba o que fazer se precisar desligar ou reinicializar sua máquina virtual do gateway para manutenção, como ao aplicar um patch ao hipervisor.
- Substituindo seu File Gateway por uma nova instância— Saiba como substituir o File Gateway por uma nova instância quando quiser melhorar o desempenho ou responder a uma notificação para migrar o gateway.
- Como excluir o gateway e remover recursos associados— Saiba como excluir seu gateway usando o AWS Storage Gateway console e limpar os recursos associados para evitar a cobrança pelo uso contínuo.

Como gerenciar atualizações de gateway

O Storage Gateway consiste em um componente de serviços de nuvem gerenciados e um componente de dispositivo de gateway que você implanta localmente ou em uma instância do Amazon EC2 na nuvem. AWS Ambos os componentes recebem atualizações regulares. Os tópicos desta seção descrevem o ritmo dessas atualizações, como elas são aplicadas e como definir as configurações de atualização nos gateways em sua implantação.

> **Important**
>
> Trate o dispositivo do Storage Gateway como uma máquina virtual gerenciada e não tente acessar nem modificar a instalação ou o conteúdo do dispositivo. A tentativa de instalar ou

atualizar qualquer pacote de software usando métodos diferentes do mecanismo normal de atualização do AWS gateway (por exemplo, ferramentas SSM ou hipervisor) pode causar mau funcionamento do gateway.
O Storage Gateway aplica patches de forma automática e regular ao dispositivo a fim de manter a segurança e a estabilidade. Os dispositivos do Storage Gateway usam o Amazon Linux como sistema operacional básico. Você pode conferir o status dos problemas detectados de vulnerabilidades e exposições comuns (CVE) no Amazon Linux Security Center. Os patches CVE são aplicados automaticamente em até 30 dias após serem lançados, conforme mostrado no Amazon Linux Security Center. Os patches são instalados durante o cronograma de manutenção do gateway, desde que o gateway esteja on-line.
O Storage Gateway não oferece suporte à atualização manual de um gateway do Amazon EC2 usando diretivas cloud-init. Se você usar esse método para atualizar um gateway, poderá encontrar problemas de interoperabilidade que impedirão você de ativar ou usar o dispositivo de gateway.

Frequência de atualização e comportamento esperado

AWS atualiza o componente de serviços em nuvem conforme necessário, sem causar interrupções nos gateways implantados. Seus dispositivos de gateway implantados recebem os seguintes tipos de atualização:

- Manutenção: as atualizações regulares que podem incluir atualizações do sistema operacional e do software, correções para lidar com estabilidade, performance e segurança, bem como acesso a novos recursos.
- Urgente: atualizações críticas que incluem as correções necessárias de problemas que afetam imediatamente a segurança, a performance ou a durabilidade do seu gateway. As atualizações urgentes podem ser lançadas a qualquer momento, fora da cadência normal das atualizações mensais de manutenção e recursos.

Todas as atualizações são cumulativas e atualizam os gateways para a versão atual quando aplicadas. Para acessar informações sobre as alterações específicas incluídas em cada atualização, consulte .

Todas as atualizações do dispositivo de gateway podem causar uma breve interrupção do serviço. O host da VM do gateway não precisa ser reinicializado durante as atualizações, mas o gateway ficará indisponível por um curto período enquanto o dispositivo do gateway for atualizado e reiniciado.

Ao implantar e ativar o gateway, um cronograma de janela de manutenção padrão é definido. Você pode modificar o cronograma da janela de manutenção a qualquer momento. Você também pode desativar as atualizações de manutenção, mas recomendamos deixá-las ativadas.

> **Note**
>
> Atualizações urgentes serão aplicadas de acordo com o cronograma da janela de manutenção, mesmo que as atualizações de manutenção regulares estejam desativadas.

Antes que qualquer atualização seja aplicada ao seu gateway, AWS notifica você com uma mensagem no console do Storage Gateway e no seu AWS Health Dashboard. Para obter mais informações, consulte AWS Health Dashboard. Para modificar o endereço de e-mail para o qual as notificações de atualização de software são enviadas, consulte Atualizar os contatos alternativos da sua AWSAWS conta no Guia de referência de gerenciamento de contas.

Quando há atualizações disponíveis, a guia do gateway Detalhes exibe uma mensagem de manutenção. Você pode ver a data e a hora em que a última atualização bem-sucedida foi aplicada na guia Detalhes.

Ativar ou desativar as atualizações de manutenção

Quando as atualizações de manutenção são ativadas, o gateway aplica automaticamente essas atualizações de acordo com a programação da janela de manutenção configurada. Para obter mais informações, consulte Modify the gateway maintenance window schedule.

Se as atualizações de manutenção estiverem desativadas, o gateway não aplicará essas atualizações automaticamente, mas você sempre poderá aplicá-las manualmente usando o console, a API ou a CLI do Storage Gateway. Às vezes, atualizações urgentes serão aplicadas durante a janela de manutenção configurada, independentemente dessa configuração.

> **Note**
>
> O procedimento a seguir descreve como ativar ou desativar as atualizações do gateway usando o console do Storage Gateway. Para alterar essa configuração programaticamente usando a API, consulte UpdateMaintenanceStartTimena Referência da API do Storage Gateway.

Para ativar ou desativar as atualizações de manutenção usando o console do Storage Gateway:

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, escolha Gateways e o gateway para o qual você deseja configurar atualizações de manutenção.
3. Escolha Ações e, em seguida, selecione Editar configurações de manutenção.
4. Em Atualizações de manutenção, selecione Ativado ou Desativado.
5. Quando concluir, escolha Salvar alterações.

Você pode verificar a configuração atualizada na guia Detalhes do gateway selecionado no console do Storage Gateway.

Modificar o cronograma da janela de manutenção do gateway

Se as atualizações de manutenção estiverem ativadas, seu gateway aplicará automaticamente essas atualizações de acordo com o cronograma da janela de manutenção. Às vezes, atualizações urgentes serão aplicadas durante a janela de manutenção configurada, independentemente da configuração das atualizações de manutenção.

> **Note**
>
> O procedimento a seguir descreve como modificar a programação da janela de manutenção usando o console do Storage Gateway. Para alterar essa configuração programaticamente usando a API, consulte UpdateMaintenanceStartTimena Referência da API do Storage Gateway.

Para modificar a programação da janela de manutenção usando o console do Storage Gateway:

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, escolha Gateways e o gateway para o qual você deseja configurar atualizações de manutenção.
3. Escolha Ações e, em seguida, selecione Editar configurações de manutenção.
4. Em Hora de início da janela de manutenção, faça o seguinte:

    a. Em Programação, escolha Semanal ou Mensal para definir a cadência da janela de manutenção.

b. Se você escolher Semanal, modifique os valores para Dia da semana e Hora para definir o ponto específico durante cada semana em que a janela de manutenção será iniciada.

   Se você escolher Mensal, modifique os valores para Dia do mês e Hora para definir o ponto específico durante cada mês em que a janela de manutenção será iniciada.

   > **Note**
   >
   > O valor máximo que pode ser definido para o dia do mês é 28. Não é possível definir o cronograma de manutenção para começar nos dias 29 a 31.
   > Se você receber um erro ao definir essa configuração, isso pode significar que o software do gateway está desatualizado. Considere primeiro atualizar seu gateway manualmente e, em seguida, tentar configurar o cronograma da janela de manutenção novamente.

5. Quando concluir, escolha Salvar alterações.

Você pode verificar as configurações atualizadas na guia Detalhes do gateway selecionado no console do Storage Gateway.

Aplicar uma atualização manualmente

Se uma atualização de software estiver disponível para seu gateway, você poderá aplicá-la manualmente seguindo o procedimento abaixo. Esse processo de atualização manual ignora o cronograma da janela de manutenção e aplica a atualização imediatamente, mesmo que as atualizações de manutenção estejam desativadas.

> **Note**
>
> O procedimento a seguir descreve como aplicar uma atualização usando o console do Storage Gateway. Para realizar essa ação de forma programática usando a API, consulte UpdateGatewaySoftwareNowa Referência da API do Storage Gateway.

Para aplicar uma atualização de software de gateway usando o console do Storage Gateway:

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.

2. No painel de navegação, escolha Gateways e, em seguida, o gateway que você deseja gerenciar.

   Se uma atualização estiver disponível, o console exibirá um banner de notificação azul na guia Detalhes do gateway, que inclui uma opção para aplicar a atualização.
3. Escolha Aplicar atualização agora para atualizar imediatamente o gateway.

> **Note**
>
> Essa operação causa uma interrupção temporária na funcionalidade do gateway durante a instalação da atualização. Durante esse período, o status do gateway aparece como OFFLINE no console do Storage Gateway. Após a conclusão da instalação da atualização, o gateway retoma a operação normal e o status muda para RUNNING.

Você pode verificar se o software do gateway foi atualizado para a versão mais recente verificando a guia Detalhes do gateway selecionado no console do Storage Gateway.

Como executar tarefas de manutenção usando o console local

Esta seção contém os tópicos a seguir, que fornecem informações sobre como realizar tarefas de manutenção usando o console local do dispositivo de gateway. Para realizar essas tarefas, acesse o console local por meio da máquina virtual on-premises ou da instância do Amazon EC2 que hospeda seu dispositivo de gateway. A maioria das tarefas é comum nas diferentes plataformas de hospedagem, mas há também algumas diferenças.

Tópicos

- Acessar o console local do gateway- Aprenda a fazer login no console local de um gateway local hospedado em uma máquina virtual baseada em kernel Linux (KVM) VMware ESXi ou na plataforma Microsoft Hyper-V Manager.
- Realizar tarefas no console local da máquina virtual: aprenda a usar o console local para realizar tarefas básicas e avançadas de configuração para um gateway on-premises, como configurar um proxy HTTP, visualizar o status dos recursos do sistema ou executar comandos do terminal.
- Realizar tarefas no console local do gateway do Amazon EC2: aprenda a fazer login no console local para realizar tarefas básicas e avançadas de configuração para um gateway do Amazon EC2, como configurar um proxy HTTP, visualizar o status dos recursos do sistema ou executar comandos do terminal.

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, você pode encontrar informações sobre como acessar o console local da VM usando a Máquina Virtual Baseada em Kernel Linux (KVM) VMware ESXi e o Microsoft Hyper-V Manager.

Tópicos

Acessar o console local do gateway com o Linux KVM

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

Como acessar o console local do gateway com a KVM

1. Use o comando a seguir para listar os VMs que estão atualmente disponíveis no KVM.

   ```
   # virsh list
   ```

   O comando retorna uma lista VMs com informações de ID, nome e estado para cada um. Observe o `Id` da VM para a qual deseja executar o console local do gateway.

2. Use o comando a seguir para acessar o console local.

   ```
   # virsh console Id
   ```

   *`Id`*Substitua pelo ID da VM que você anotou na etapa anterior.

   O console local do gateway do AWS equipamento solicita que você faça login para alterar sua configuração de rede e outras configurações.

3. Insira seu nome de usuário e senha para fazer login no console local do gateway. Para acessar mais informações, consulte Fazer login no console local do Gateway de Arquivos.

Depois de fazer login, o menu Ativação de dispositivo da AWS - Configuração é exibido. Você pode selecionar as opções do menu para realizar tarefas de configuração do gateway. Para obter mais informações, consulte Performing tasks on the virtual machine local console.

Acessando o console local do Gateway com VMware ESXi

Para acessar o console local do seu gateway com VMware ESXi

1. No cliente VMware vSphere, selecione sua VM de gateway.
2. Verifique se a VM do gateway está ativada.

> **Note**
>
> Se a VM do gateway estiver ativada, um ícone de seta verde aparecerá com o ícone da VM no painel do navegador da VM no lado esquerdo da janela do aplicativo. Se a VM do gateway não estiver ativada, você poderá ativá-la escolhendo o ícone verde Ligar no menu da Barra de ferramentas na parte superior da janela do aplicativo.

3. Escolha a guia Console no painel de informações principal no lado direito da janela do aplicativo.

   Depois de alguns instantes, o console local do gateway do AWS Appliance solicita que você faça login para alterar sua configuração de rede e outras configurações.

> **Note**
>
> Para liberar o cursor da janela do console, pressione Ctrl+Alt.

4. Insira seu nome de usuário e senha para fazer login no console local do gateway. Para acessar mais informações, consulte Fazer login no console local do Gateway de Arquivos.

   Depois de fazer login, o menu Ativação de dispositivo da AWS - Configuração é exibido. Você pode selecionar as opções do menu para realizar tarefas de configuração do gateway. Para obter mais informações, consulte Performing tasks on the virtual machine local console.

Acessar o console local do gateway com o Microsoft Hyper-V

Para acessar o console local do gateway (Microsoft Hyper-V)

1. Selecione sua VM do dispositivo de gateway no painel Máquinas Virtuais no lado esquerdo da janela do aplicativo Microsoft Hyper-V Manager.
2. Verifique se o gateway está ativado.

   > **Note**
   >
   > Se a VM do gateway estiver ativada, `Running` será exibido na coluna Estado da VM no painel Máquinas virtuais no lado esquerdo da janela da aplicação. Se a VM do gateway não estiver ativada, você pode ativá-la escolhendo Iniciar no painel Ações no lado direito da janela do aplicativo.

3. Escolha Conectar no painel Ações.

   A janela Virtual Machine Connection é exibida. Se uma janela de autenticação for exibida, digite as credenciais fornecidas pelo administrador do hipervisor.

   Depois de alguns instantes, o console local do gateway do AWS Appliance solicita que você faça login para alterar sua configuração de rede e outras configurações.
4. Insira seu nome de usuário e senha para fazer login no console local do gateway. Para acessar mais informações, consulte Fazer login no console local do Gateway de Arquivos.

   Depois de fazer login, o menu Ativação de dispositivo da AWS - Configuração é exibido. Você pode selecionar as opções do menu para realizar tarefas de configuração do gateway. Para obter mais informações, consulte Performing tasks on the virtual machine local console.

Realizar tarefas no console local da máquina virtual

Em relação a um Gateway de Arquivos implantado na infraestrutura on-premises, você pode realizar as tarefas de manutenção a seguir utilizando o console local do host da VM. Essas tarefas são comuns aos VMware hipervisores Microsoft Hyper-V e Linux Kernel-based Virtual Machine (KVM).

Tópicos

- Fazer login no console local do Gateway de Arquivos: saiba como fazer login no console local, onde é possível definir configurações de rede do gateway e alterar a senha padrão.

- Como configurar um proxy de HTTP- Saiba como configurar o Storage Gateway para rotear todo o tráfego de AWS endpoints por meio de um servidor proxy.
- Definir configurações de rede do gateway: saiba mais sobre como configurar o gateway para usar DHCP ou um endereço IP estático.
- Como testar a conectividade de rede do gateway: saiba como usar console local do gateway para testar a conectividade de rede.
- Como visualizar o status de recursos de sistema do gateway: saiba como conferir os núcleos de CPU virtual, o tamanho do volume raiz e a RAM do gateway.
- Configurar um servidor de NTP para seu gateway: saiba como visualizar e editar as configurações do servidor de NTP e sincronizar o horário de seu gateway com o host do hipervisor.
- Como executar comandos do Storage Gateway no console local- Aprenda a executar comandos do console local para realizar tarefas como salvar tabelas de roteamento, conectar-se a Suporte e muito mais.

Fazer login no console local do Gateway de Arquivos

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 da VM, vai usar as credenciais temporárias para fazer login. Estas credenciais temporárias concedem acesso aos menus onde é possível definir configurações de rede do gateway e alterar a senha no console local. O nome de usuário inicial é `admin` e a senha temporária é `password`. Você deverá alterar a senha no primeiro login.

Como alterar a senha temporária

1. No menu principal Ativação do dispositivo da AWS : configuração, insira o número correspondente para Console do Gateway.
2. Execute o comando `passwd`. Para obter informações sobre como executar o comando, consulte Como executar comandos do Storage Gateway no console local.

Definir a senha do console local no console do Storage Gateway

Você também pode gerenciar a senha do console local por meio do console baseado na Web do Storage Gateway. Qualquer atualização de senha bem-sucedida feita com o console baseado na Web substituirá a senha usada pelo console local da VM do gateway, incluindo a senha temporária, caso você nunca tenha feito login localmente. Se o gateway não estiver acessível atualmente pela rede, o processo de atualização da senha falhará.

Para definir a senha do console local no console do Storage Gateway

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, selecione Gateways e escolha o gateway para o qual você deseja definir uma nova senha.
3. Em Actions (Ações), escolha Set Local Console Password (Definir senha do console local).
4. Na caixa de diálogo Set Local Console Password (Definir senha do console local), digite uma nova senha, confirme a senha e escolha Save (Salvar).

   A nova senha substitui a senha atual. O serviço Storage Gateway não salva, armazena nem registra em log a senha, mas a transmite com segurança por um canal criptografado para a VM, onde ela é armazenada com segurança.

   > **Note**
   >
   > A senha pode conter qualquer caractere do teclado e ter de 1 a 512 caracteres de extensão.

Como configurar um proxy de HTTP

Os Gateways de Arquivos aceitam a configuração de um proxy HTTP.

> **Note**
>
> Os Gateways de Arquivos aceitam somente a configuração de um proxy HTTP.

Se seu gateway precisar usar um servidor de proxy para se comunicar com a internet, será preciso definir as configurações de proxy HTTP para esse gateway. Para fazer isso, especifique um endereço IP e um número de porta para o host que executa o proxy. Depois de fazer isso, o Storage Gateway roteia todo o tráfego AWS do endpoint por meio do seu servidor proxy. As comunicações entre o gateway e os endpoints são criptografadas, mesmo quando se usa o proxy HTTP. Para obter informações sobre os requisitos de rede para seu gateway, consulte Requisitos de rede e firewall.

Como configurar um proxy HTTP para um Gateway de Arquivos

1. Faça login no console local do seu gateway:

- Para obter mais informações sobre como fazer login no console VMware ESXi local, consulteAcessando o console local do Gateway com VMware ESXi.
- Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte Acessar o console local do gateway com o Microsoft Hyper-V.
- Para obter mais informações sobre como fazer login no console local da Linux Kernel-based Virtual Machine (KVM), consulte Acessar o console local do gateway com o Linux KVM.

2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Configurar proxy HTTP.
3. No menu Configuração do proxy HTTP de ativação do equipamento da AWS , insira o número correspondente para a tarefa que você deseja realizar:

   - Configurar proxy de HTTP: você precisará fornecer um nome de host e a porta para concluir a configuração.
   - Visualizar a configuração atual do proxy HTTP: se nenhum proxy HTTP estiver configurado, a mensagem `HTTP Proxy not configured` será exibida. Se houver um proxy HTTP configurado, o nome do host e a porta do proxy serão exibidos.
   - Remover uma configuração de proxy de HTTP: a mensagem `HTTP Proxy Configuration Removed` será exibida.
4. Reinicie a VM para aplicar suas configurações de HTTP.

Definir 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 como fazer login no console VMware ESXi local, consulteAcessando o console local do Gateway com VMware ESXi.
   - Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte Acessar o console local do gateway com o Microsoft Hyper-V.

- Para obter mais informações sobre o registro em log no console local da KVM, consulte Acessar o console local do gateway com o Linux KVM.

2. No menu principal Ativação do dispositivo da AWS : configuração, insira o número correspondente para selecionar Conectividade de rede.
3. No menu Configuração de rede, realize uma das seguintes tarefas:

Para executar esta tarefa	Faça o seguinte
Obter informações sobre seu adaptador de rede	Insira o número correspondente para selecionar Descrever adaptador. 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 (endereço de IP) • Máscara de rede • Endereço IP do gateway • Status de DHCP habilitado Os nomes dos adaptadores listados aqui são usados ao configurar um endereço IP estático ou definir o adaptador padrão do seu gateway.
Configurar o roteamento DHCP	

Para executar esta tarefa	Faça o seguinte
	Insira o número correspondente para selecionar Configurar DHCP. Você é solicitado a configurar a interface de rede para usar o DHCP.

Para executar esta tarefa	Faça o seguinte
Configurar um endereço IP estático para gateway	Insira o número correspondente para seleciona r Configurar IP estático. Você é solicitado a digitar as seguintes informações para configurar um endereço IP estático: • Nome do adaptador de rede • IP address (endereço de IP) • Máscara de rede • Endereço de gateway padrão • Endereço Domain Name Service (DNS) • Endereço DNS secundário **Important** Se o gateway já tiver sido ativado, você deverá encerrá-lo e reiniciá-lo por meio do console do Storage Gateway para que as configurações sejam aplicadas. Para obter mais informações, consulte Encerrar a VM do gateway. Se seu gateway usar mais de uma interface de rede, você deverá definir todas as interface

Para executar esta tarefa	Faça o seguinte
	s ativas para usar DHCP ou endereços IP estáticos. 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 ativar a interface, nesse caso, você deve configurá-la para um 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.

Para executar esta tarefa	Faça o seguinte
Configure um nome de host para seu gateway	Insira o número correspondente para selecionar Configurar nome do host. Você será solicitado a escolher se o gateway usará um nome de host estático especificado por você ou adquirirá um automaticamente por meio do DCHP ou rDNS. Se você selecionar Estático, precisará fornecer um nome de host estático, como `testgateway.example.com` . Digite y para aplicar a configuração. **Note** Se você configurar um nome de host estático para o gateway, verifique se o nome de host fornecido está no domínio ao qual o gateway está associado. Você também deve criar um registro A no sistema DNS que aponta o endereço IP do gateway para o nome de host estático.
Visualizar a configuração de nome do host do gateway	Insira o número correspondente para selecionar Visualizar configuração do nome do host. O nome do host, o modo de aquisição, o domínio e a região do Active Directory do seu gateway são exibidos.

Para executar esta tarefa	Faça o seguinte
Redefinir todas as configurações de rede do gateway para DHCP	Insira o número correspondente para selecionar Redefinir tudo para DHCP. Todas as interfaces de rede são definidas para usar DHCP. **Important** Se o gateway já tiver sido ativado, você deverá encerrá-lo e reiniciá-lo por meio do console do Storage Gateway para que as configurações sejam aplicadas. Para obter mais informações, consulte Encerrar a VM do gateway.
Configurar o adaptador de rota padrão do gateway	Insira o número correspondente para selecionar Configurar adaptador padrão. Os adaptadores disponíveis para seu gateway são exibidos, e é solicitado que você escolha um dos adaptadores, por exemplo, **`eth0`**.
Editar a configuração de DNS do seu gateway	Insira o número correspondente para selecionar Editar configuração do DNS. Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos. O novo endereço IP será solicitado.

Para executar esta tarefa	Faça o seguinte
Visualizar a configuração de DNS do gateway	Insira o número correspondente para selecionar Visualizar configuração atual do DNS. Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos. **Note** Para algumas versões do VMware hipervisor, você pode editar a configuração do adaptador nesse menu.
Visualizar tabelas de roteamento	Insira o número correspondente para selecionar Visualizar rotas. A rota padrão de seu gateway é exibida.

Como testar a conectividade de rede do gateway

É possível pode usar o console local de seu gateway para testar a sua conexão com a Internet. Este teste pode ser útil quando estiver solucionando problemas de rede em seu gateway.

Como testar a conectividade de rede do gateway

1. Faça login no console local do seu gateway:

   - Para obter mais informações sobre como fazer login no console VMware ESXi local, consulteAcessando o console local do Gateway com VMware ESXi.
   - Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte Acessar o console local do gateway com o Microsoft Hyper-V.
   - Para obter mais informações sobre o registro em log no console local da KVM, consulte Acessar o console local do gateway com o Linux KVM.

2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Testar conectividade de rede.

   Se o gateway já tiver sido ativado, o teste de conectividade começará imediatamente. Para gateways que ainda não foram ativados, você deve especificar o tipo de endpoint e Região da AWS conforme descrito nas etapas a seguir.
3. Se o gateway ainda não estiver ativado, insira o número correspondente para selecionar o tipo de endpoint do gateway.
4. Se você selecionou o tipo de endpoint público, insira o número correspondente para selecionar o Região da AWS que você deseja testar. Para obter suporte Regiões da AWS e uma lista dos endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte AWS Storage Gateway endpoints e cotas no. Referência geral da AWS

Conforme o teste progride, cada endpoint exibe [PASSED] ou [FAILED], indicando o status da conexão da seguinte forma:

Mensagem	Description
[PASSED]	O Storage Gateway tem conectividade de rede.
[FAILED]	O Storage Gateway não tem conectividade de rede.

Como visualizar o status de recursos de sistema do gateway

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

Para visualizar o status de uma verificação de recursos do sistema

1. Faça login no console local do seu gateway:

   - Para obter mais informações sobre como fazer login no VMware ESXi console, consulteAcessando o console local do Gateway com VMware ESXi.
   - Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte Acessar o console local do gateway com o Microsoft Hyper-V.

- Para obter mais informações sobre o registro em log no console local da KVM, consulte Acessar o console local do gateway com o Linux KVM.

2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Visualizar verificação de recursos do sistema.

   Cada recurso exibe [OK], [AVISO] ou [FALHA], indicando o status do recurso da seguinte forma:

Mensagem	Description
[OK]	O recurso passou na verificação de recursos do sistema.
[WARNING]	O recurso não atende aos requisitos recomendados, mas seu gateway vai continuar funcionando. O Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.
[FAIL]	O recurso não atende aos requisitos mínimos. Talvez o gateway não funcione corretamente. O Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

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

Configurar um servidor de NTP 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 como fazer login no console VMware ESXi local, consulteAcessando o console local do Gateway com VMware ESXi.
- Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte Acessar o console local do gateway com o Microsoft Hyper-V.
- Para obter mais informações sobre o registro em log no console local da KVM, consulte Acessar o console local do gateway com o Linux KVM.

2. No menu principal Ativação do dispositivo da AWS : configuração, insira o número correspondente para selecionar Gerenciamento do horário do sistema.
3. No menu Gerenciamento de tempo do sistema, insira o número correspondente para realizar uma das tarefas a seguir.

Para executar esta tarefa	Faça o seguinte
Exibir e sincronizar o horário da sua VM com o horário do servidor NTP.	Insira o número correspondente para seleciona r Visualizar e sincronizar o tempo do sistema. O horário atual da sua VM é exibida. Seu Gateway de Arquivos 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 implantad o e em execução, em algumas situações o horário da VM do gateway pode apresentar desvios. Por exemplo, imagine que há alguma interrupção prolongada na rede e o host do hipervisor e o gateway não recebem 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 executar esta tarefa	Faça o seguinte
	Para um gateway implantado em VMware ESXi, definir a hora do host do hiperviso r e sincronizar a hora da VM com o host é suficiente para evitar o desvio de tempo. Para obter mais informações, consulte Sincronize o horário da VM com VMware o horário 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 Sincronizar o horário da VM com o horário do host Hyper-V ou Linux KVM. 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	Insira o número correspondente para seleciona r Editar configuração do NTP. Você é solicitado a fornecer um servidor NTP preferencial e um secundário.
Exibir a configuração do seu servidor NTP	Insira o número correspondente para seleciona r Visualizar configuração do DNS. A configuração do seu servidor NTP é exibida.

Como executar comandos do Storage Gateway no console local

O console local da VM no Storage Gateway ajuda a oferecer um ambiente seguro para a configuração e o diagnóstico de problemas em seu gateway. Usando os comandos do console local, você pode realizar tarefas de manutenção, como salvar tabelas de roteamento, conectar-se a Suporte, etc.

Para executar um comando de configuração ou diagnóstico

1. Faça login no console local do seu gateway:

   - Para obter mais informações sobre como fazer login no console VMware ESXi local, consulteAcessando o console local do Gateway com VMware ESXi.
   - Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte Acessar o console local do gateway com o Microsoft Hyper-V.
   - Para obter mais informações sobre o registro em log no console local da KVM, consulte Acessar o console local do gateway com o Linux KVM.

2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Console do gateway.
3. No prompt de comando do console do gateway, insira **h**.

   O console exibe o menu COMANDOS DISPONÍVEIS, que lista os comandos disponíveis:

Command	Função
dig	Colete a saída do dig para solucionar problemas de DNS.
exit	Retorne ao menu Configuração.
h	Exibir a lista de comandos disponível.
ifconfig	Visualize ou configure interfaces de rede. **Note** É recomendável definir as configura ções de rede ou IP usando o console do Storage Gateway ou a opção de menu do console local dedicado. Para receber instruções, consulte Definir as configurações de rede do gateway.

Command	Função
ip	Mostra/manipule roteamentos, dispositivos e túneis. **Note** É recomendável definir as configurações de rede ou IP usando o console do Storage Gateway ou a opção de menu do console local dedicado. Para receber instruções, consulte Definir as configurações de rede do gateway.
iptables	Ferramenta de administração para IPv4 filtragem de pacotes e NAT.
ncport	Teste a conectividade com uma porta TCP específica em uma rede.
nping	Colete a saída do nping para solucionar problemas de rede.
open-support-channel	Connect to AWS Support. Para obter instruções sobre como ativar o acesso ao AWS suporte, consulte Você quer que o AWS Suporte ajude a solucionar problemas do seu gateway EC2.
passwd	Atualize os tokens de autenticação.
save-iptables	Mantenha as tabelas IP.
save-routing-table	Salve a entrada da tabela de rotas recém-adicionada.
tcptraceroute	Colete a saída de traceroute no tráfego TCP para um destino.

Command	Função
sslcheck	Retorna a saída com o emissor do certificado **Note** O Storage Gateway usa a verificação do emissor do certificado e não oferece suporte à inspeção SSL. Se esse comando retornar um emissor diferente de aws-appliance@amazon.com, é provável que uma aplicação esteja executando uma inspeção de SSL. Nesse caso, recomendamos ignorar a inspeção de SSL do dispositivo do Storage Gateway.

4. No prompt de comando do console do gateway, digite o comando correspondente para a função que você deseja usar e siga as instruções.

Para saber mais sobre um comando, digite **`man`** + *`command name`* no prompt de comando.

Realizar tarefas no console local do gateway do Amazon EC2

Algumas tarefas de manutenção exigem que você faça login no console local ao executar um gateway implantado em uma instância do Amazon EC2. Esta seção descreve como fazer login no console local e realizar tarefas de manutenção.

Tópicos

- Fazer login no console local do gateway do Amazon EC2: saiba como se conectar e fazer login no console local do gateway da sua instância do Amazon EC2 usando um cliente Secure Shell (SSH).
- Encaminhar o gateway implantado no Amazon EC2 por meio de um proxy HTTP- Aprenda a configurar um proxy Socket Secure versão 5 (SOCKS5) entre AWS e um gateway implantado em uma instância do Amazon EC2.
- Como testar a conectividade de rede do gateway: saiba como usar o console local do gateway para testar a conectividade de rede entre o gateway e vários recursos de rede.

- Como visualizar o status de recursos de sistema do gateway: saiba mais sobre como usar o console local do gateway para conferir os núcleos de CPU virtuais do gateway, o tamanho do volume raiz e a RAM.
- Executar comandos do Storage Gateway no console local para um gateway do Amazon EC2: saiba como executar comandos do console para realizar tarefas, como salvar tabelas de rotas, entrar em contato com o Suporte e muito mais.
- Definir configurações de rede para seu gateway do Amazon EC2: saiba como usar o console local para visualizar e definir configurações de rede, como DNS e nome do host, para um gateway em uma instância do Amazon EC2.

Fazer login no console local do gateway do Amazon EC2

É possível fazer login no console local do gateway em uma instância do Amazon EC2 utilizando um cliente Secure Shell (SSH). Para acessar informações detalhadas, consulte Conectar-se à sua instância no Guia do usuário do Amazon EC2. Para se conectar dessa forma, você precisará do par de chaves SSH que você especificou ao executar sua instância. Para acessar informações sobre pares de chave do Amazon EC2, consulte Pares de chave do Amazon EC2 no Guia do usuário do Amazon EC2.

Para fazer login no console local do gateway

1. Conecte-se à instância do Amazon EC2 usando SSH e faça login como usuário administrador.
2. Depois de fazer login, será possível ver o menu principal Ativação do dispositivo da AWS : configuração, onde você pode realizar várias tarefas.

Para saber mais sobre esta tarefa	Consulte este tópico
Configurar um proxy HTTP para seu gateway	Encaminhar o gateway implantado no Amazon EC2 por meio de um proxy HTTP
Configurar configurações de rede para seu gateway	Definir configurações de rede para seu gateway do Amazon EC2
Testar a conectividade de rede	Como testar a conectividade de rede do gateway

Para saber mais sobre esta tarefa	Consulte este tópico
Exibir uma verificação de recursos do sistema	Como visualizar o status de recursos de sistema do gateway.
Executar comandos do console do Storage Gateway	Executar comandos do Storage Gateway no console local para um gateway do Amazon EC2

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

Para sair da sessão de configuração, insira **X**.

Encaminhar o gateway implantado no Amazon EC2 por meio de um proxy HTTP

O Storage Gateway suporta a configuração de um proxy Secure Socket versão 5 (SOCKS5) entre o gateway implantado no Amazon EC2 e na AWS.

Se seu gateway precisar usar um servidor de proxy para se comunicar com a internet, será preciso definir as configurações de proxy HTTP para esse gateway. Para fazer isso, especifique um endereço IP e um número de porta para o host que executa o proxy. Depois de fazer isso, o Storage Gateway roteia todo o tráfego AWS do endpoint por meio do seu servidor proxy. As comunicações entre o gateway e os endpoints são criptografadas, mesmo quando se usa o proxy HTTP.

Para rotear o tráfego de internet de seu gateway por meio de um servidor de proxy local

1. Faça login no console local do gateway. Para instruções, consulte Fazer login no console local do gateway do Amazon EC2.
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Configurar proxy HTTP.
3. No menu Configuração do proxy HTTP de ativação do equipamento da AWS , insira o número correspondente para a tarefa que você deseja realizar:

   - Configurar proxy de HTTP: você precisará fornecer um nome de host e a porta para concluir a configuração.
   - Visualizar a configuração atual do proxy HTTP: se nenhum proxy HTTP estiver configurado, a mensagem `HTTP Proxy not configured` será exibida. Se houver um proxy HTTP configurado, o nome do host e a porta do proxy serão exibidos.

- Remover uma configuração de proxy de HTTP: a mensagem `HTTP Proxy Configuration Removed` será exibida.

Como testar a conectividade de rede do gateway

É possível pode usar o console local de seu gateway para testar a sua conexão com a Internet. Este teste pode ser útil quando estiver solucionando problemas de rede em seu gateway.

Para testar a conectividade do gateway

1. Faça login no console local do gateway. Para instruções, consulte Fazer login no console local do gateway do Amazon EC2.
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Testar conectividade de rede.

   Se o gateway já tiver sido ativado, o teste de conectividade começará imediatamente. Para gateways que ainda não foram ativados, você deve especificar o tipo de endpoint e Região da AWS conforme descrito nas etapas a seguir.
3. Se o gateway ainda não estiver ativado, insira o número correspondente para selecionar o tipo de endpoint do gateway.
4. Se você selecionou o tipo de endpoint público, insira o número correspondente para selecionar o Região da AWS que você deseja testar. Para obter suporte Regiões da AWS e uma lista dos endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte AWS Storage Gateway endpoints e cotas no. Referência geral da AWS

Conforme o teste progride, cada endpoint exibe [PASSED] ou [FAILED], indicando o status da conexão da seguinte forma:

Mensagem	Description
[PASSED]	O Storage Gateway tem conectividade de rede.
[FAILED]	O Storage Gateway não tem conectividade de rede.

Como visualizar o status de recursos de sistema do gateway

Quando o seu Gateway de Arquivos é iniciado, ele confere os núcleos da CPU virtual, o tamanho do volume raiz e a RAM. Ele determina se esses recursos disponíveis do sistema são suficientes para seu gateway funcionar corretamente. Você pode visualizar os resultados da verificação de recursos do sistema usando o console local do gateway.

Para visualizar o status de uma verificação de recursos do sistema

1. Faça login no console local no Gateway de Arquivos do Amazon EC2. Para instruções, consulte Fazer login no console local do gateway do Amazon EC2.
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Visualizar verificação de recursos do sistema.

   O console local do gateway exibe [OK], [WARNING] ou [FAIL] para indicar o status do recurso da seguinte forma:

Mensagem	Description
[OK]	O recurso passou na verificação de recursos do sistema.
[WARNING]	O recurso não atende aos requisitos recomendados, mas seu gateway vai continuar funcionando. O console local do gateway exibe uma mensagem que descreve os resultados da verificação de recursos.
[FAIL]	O recurso não atende aos requisitos mínimos. Talvez o gateway não funcione corretame nte. O console local do gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

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

Executar comandos do Storage Gateway no console local para um gateway do Amazon EC2

O AWS Storage Gateway console ajuda a fornecer um ambiente seguro para configurar e diagnosticar problemas com seu gateway. Usando os comandos do console, você pode realizar tarefas de manutenção, como salvar tabelas de roteamento ou conectar-se a. Suporte

Para executar um comando de configuração ou diagnóstico

1. Faça login no console local do gateway. Para instruções, consulte Fazer login no console local do gateway do Amazon EC2.
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Console do gateway.
3. No prompt de comando do console do gateway, insira **h**.

   O console exibe o menu COMANDOS DISPONÍVEIS, que lista os comandos disponíveis:

Command	Função
dig	Colete a saída do dig para solucionar problemas de DNS.
exit	Retorne ao menu Configuração.
h	Exibir a lista de comandos disponível.
ifconfig	Visualize ou configure interfaces de rede. **Note** É recomendável definir as configura ções de rede ou IP usando o console do Storage Gateway ou a opção de menu do console local dedicado. Para receber instruções, consulte Definir as configurações de rede do gateway.

Command	Função
ip	Mostra/manipule roteamentos, dispositivos e túneis. **Note** É recomendável definir as configurações de rede ou IP usando o console do Storage Gateway ou a opção de menu do console local dedicado. Para receber instruções, consulte Definir as configurações de rede do gateway.
iptables	Ferramenta de administração para IPv4 filtragem de pacotes e NAT.
ncport	Teste a conectividade com uma porta TCP específica em uma rede.
nping	Colete a saída do nping para solucionar problemas de rede.
open-support-channel	Connect to AWS Support.
save-iptables	Mantenha as tabelas IP.
save-routing-table	Salve a entrada da tabela de rotas recém-adicionada.
tcptraceroute	Colete a saída de traceroute no tráfego TCP para um destino.

4. No prompt de comando do console do gateway, digite o comando correspondente para a função que você deseja usar e siga as instruções.

Para saber mais sobre um comando, digite **man** + *command name* no prompt de comando.

Definir configurações de rede para seu gateway do Amazon EC2

Você pode visualizar e definir as configurações de rede do seu Gateway de Arquivos do Amazon EC2 utilizando o console local do gateway.

Como definir suas configurações de rede

1. Faça login no console local no Gateway de Arquivos do Amazon EC2. Para instruções, consulte Fazer login no console local do gateway do Amazon EC2.
2. No menu principal Ativação do dispositivo da AWS : configuração, insira o número correspondente para selecionar Conectividade de rede.
3. No menu Ativação do dispositivo da AWS : configuração da rede, insira o número correspondente à tarefa que você deseja realizar:

   - Editar configuração de DNS: o console local do gateway exibe os adaptadores disponíveis para os servidores DNS primários e secundários. O console então solicitará que você forneça o novo endereço IP.
   - Visualizar configuração de DNS: o console local do gateway exibe os adaptadores disponíveis para os servidores DNS primários e secundários.
   - Configurar o nome do host: o console local do gateway solicita que você decida se o gateway usará um nome de host estático especificado por você ou se adquirirá um nome de host automaticamente por meio do DCHP ou rDNS.

     > **Note**
     >
     > Se você optar por configurar um nome de host estático para seu gateway, deverá criar um registro A em seu sistema DNS que aponte o endereço IP do gateway para seu nome de host estático.

   - Visualizar configuração do nome do host: o console local do gateway exibe o nome do host, o modo de aquisição, o domínio e a região do Active Directory para seu Gateway de Arquivos do Amazon EC2.

Encerrar a VM do gateway

Você pode precisar encerrar ou reiniciar a VM para manutenção; por exemplo, ao aplicar um patch ao hipervisor. É possível encerrar VMs do gateway on-premises utilizando a interface de hipervisor e instâncias do Amazon EC2 usando o console do Amazon EC2.

> **Important**
>
> Se você estiver usando o armazenamento temporário e interromper e iniciar o gateway do Amazon EC2, o gateway ficará permanentemente off-line. Isso acontece porque o disco de armazenamento físico é substituído. Não há uma solução alternativa para esse problema. A única solução é excluir o gateway e ativar um novo em uma nova instância do EC2.

Substituindo seu File Gateway por uma nova instância

Você pode substituir um File Gateway por uma nova instância à medida que suas necessidades de dados e desempenho aumentarem ou se você receber uma AWS notificação para migrar seu gateway. Talvez isso seja necessário caso deseje migrar o gateway para uma plataforma de hospedagem melhor, para instâncias mais recentes do Amazon EC2 ou para atualizar o hardware do servidor subjacente.

> **Important**
>
> Use essas instruções somente para migrar dispositivos de gateway que executam a versão 1.x. Você não pode usá-los para migrar dispositivos de gateway que executam versões inferiores.

> **Note**
>
> A migração só pode ser realizada entre gateways do mesmo tipo. Por exemplo, você não pode migrar configurações ou dados de um gateway de FSx arquivos para um gateway de arquivos S3.

Para substituir seu gateway FSx do File Gateway por uma nova instância com um disco de cache vazio e um novo ID de gateway:

1. Pare todos os aplicativos que estão gravando no gateway de arquivos existente do . Verifique se a métrica `CachePercentDirty` na guia Monitoramento é `0` antes de configurar as associações do sistema de arquivos no novo gateway.
2. Use o AWS Command Line Interface (AWS CLI) para coletar e salvar as informações de configuração sobre o e os sistemas de arquivos associados, fazendo o seguinte:

   a. Salve as informações de configuração do gateway para o .

   ```
   aws storagegateway describe-gateway-information --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   Este comando produz um bloco JSON que contém metadados sobre o gateway, como seu nome, interfaces de rede, fuso horário configurado e o estado (se o gateway está em execução).

   b. Salve as configurações do Server Message Block (SMB) do .

   ```
   aws storagegateway describe-smb-settings --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   Este comando produz um bloco JSON que contém o nome de domínio do Microsoft Active Directory no qual o gateway ingressou.

   c. Salve as informações de compartilhamento de arquivos para cada sistema de arquivos associado ao :

   Use o comando a seguir para cada sistema de arquivos associado.

   ```
   aws storagegateway describe-file-system-associations --file-system-
   association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-
   association/fsa-987A654B"
   ```

   Este comando produz um bloco JSON que contém metadados sobre o sistema de arquivos, como seu ARN de localização, destino do log de auditoria, atributos de atualização do cache, endereços IP configurados e tags.

3. Crie um novo File Gateway com as mesmas configurações do gateway antigo. Se necessário, consulte as informações que você salvou na Etapa 2.
4. Crie novas associações de sistema de arquivos para o novo gateway com as mesmas definições e configurações que os sistemas de arquivos configurados no gateway antigo. Se necessário, consulte as informações que você salvou na Etapa 2.
5. Confirme se o novo gateway está funcionando corretamente e, depois, reassocie/transfira os clientes dos sistemas de arquivos antigos para os novos da maneira mais adequada ao ambiente.
6. Confirme se o novo gateway está funcionando corretamente e, depois, exclua o gateway antigo do console do Storage Gateway.

> **Important**
>
> Antes de excluir um File Gateway, verifique se não há aplicativos gravando atualmente no cache desse gateway. Se excluir o gateway enquanto ele estiver em uso, poderá perder dados.

> **Warning**
>
> Não é possível recuperar um gateway excluído.

7. Exclua a VM do gateway antigo ou a instância do Amazon EC2.

Como excluir o gateway e remover recursos associados

Se você não pretende continuar usando seu gateway, pense na possibilidade de excluir o gateway e os recursos a ele associados. A remoção de recursos pode ajudá-lo a evitar cobranças por recursos que você não pretende continuar a usar e a reduzir sua fatura mensal.

Quando você exclui um gateway, ele não aparece mais no AWS Storage Gateway Management Console e suas conexões do sistema de de arquivos são fechadas. O procedimento para excluir um gateway é o mesmo para todos os tipos de gateway; no entanto, dependendo do tipo de gateway que você deseja excluir e do host no qual ele está implantado, siga as instruções específicas para remover recursos associados.

É possível excluir um gateway usando o console do Storage Gateway ou de forma programática. É possível encontrar informações a seguir sobre como excluir um gateway usando o console do Storage Gateway. Se você deseja excluir seu gateway de forma programática, consulte Referência de API do AWS Storage Gateway.

Como excluir um gateway usando o console do Storage Gateway

O procedimento para excluir um gateway é o mesmo para todos os tipos de gateway. No entanto, dependendo do tipo de gateway que você deseja excluir e do host no qual está implantado, talvez você precise executar outras tarefas para remover recursos associados ao gateway. A remoção desses recursos ajuda-o a evitar despesas com recursos que você não pretende usar.

> **Note**
>
> Para os gateways implantados em uma instância do Amazon EC2, a instância continua a existir até que você a exclua.
> Para gateways implantados em uma máquina virtual (VM), depois que você exclui seu gateway, a VM do gateway continua presente em seu ambiente de virtualização. Para remover a VM, use o cliente VMware vSphere, o Microsoft Hyper-V Manager ou o cliente Linux Kernel based Virtual Machine (KVM) para se conectar ao host e remover a VM. Observe que você não pode reutilizar a VM do gateway excluído para ativar um novo gateway.

Para excluir um gateway

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Gateways e selecione um ou mais gateways para excluir.
3. Em Actions (Ações), selecione Delete gateway (Excluir gateway). Uma caixa de diálogo de confirmação é exibida.

> **Warning**
>
> Antes de executar esta etapa, verifique se não há nenhuma aplicação gravando no momento nos volumes do gateway. Se excluir o gateway enquanto ele estiver em uso, poderá perder dados. Não é possível recuperar um gateway excluído.

4. Verifique se você deseja excluir os gateways especificados, digite a palavra excluir na caixa de confirmação e escolha Excluir.
5. (Opcional) Se você quiser fornecer feedback sobre o gateway excluído, preencha a caixa de diálogo de comentários e escolha Enviar. Caso contrário, selecione Interromper.

> **Important**
>
> Ao excluir um gateway, você deixa de pagar as despesas de software, mas recursos, como o bucket do Amazon S3 e instâncias do Amazon EC2 são mantidos. Você pode remover a instância do Amazon EC2 do gateway depois que o gateway de arquivos for removido.

Performance e otimização

Esta seção descreve orientações e práticas recomendadas para otimizar a performance do Gateway de Arquivos.

Tópicos

Orientação básica de desempenho para o

Nesta seção, você pode encontrar orientações para provisionar hardware para sua VM do FSx File Gateway. As configurações de instâncias que estão listados na tabela são exemplos e são fornecidas para referência.

Para obter melhor desempenho, o tamanho do disco de cache deve ser ajustado ao tamanho do conjunto de trabalho ativo. Usar vários discos locais para o cache aumenta o desempenho de gravação ao paralelizar acesso a dados e gera IOPS maior.

> **Note**
>
> Não recomendamos o uso do armazenamento temporário. Para obter informações sobre como usar o armazenamento temporário, consulte Usar o armazenamento temporário com gateways do EC2.
> O limite de tamanho sugerido para diretórios individuais nos sistemas de arquivos que você conecta ao Gateway de Arquivos é de 10 mil arquivos por diretório. Você pode usar o Gateway de Arquivos com diretórios com mais de 10 mil arquivos, mas a performance pode ser afetada.

Nas tabelas a seguir, as operações de leitura de ocorrência de cache são leituras dos dados dos arquivos que são feitas pelo cache. As operações de leitura perdida do cache são leituras dos dados do arquivo que são fornecidos FSx pelo Amazon para Windows File Server.

A tabela a seguir mostra um exemplo de configuração FSx do File Gateway.

FSx Desempenho do File Gateway em clientes Windows

Exemplo de configuração	Protocolo	Throughput de gravação (tamanhos de arquivos 1 GB)	Throughput de leitura de ocorrência de cache	Throughput de leitura de solicitações não atendidas pelo cache
Disco raiz: 80 GB, io1 SSD, 4.000 IOPs Discos de cache: 2 x 2 TiB NVME Desempenho mínimo da rede: 10 Gbps CPU: 32 vCPU | RAM: 244 GB	SMBv3 - 1 tópico	162 MiB/sec (1,4 Gbps)	403 MiB/sec (3,4 Gbps)	288 MiB/sec (2,4 Gbps)
	SMBv3 - 8 fios	511 MiB/sec (4,3 Gbps)	571 MiB/sec (4,8 Gbps)	567 MiB/sec (4,8 Gbps)

> **Note**
>
> Seu desempenho pode variar com base na configuração da plataforma de hospedagem e na largura de banda da rede. A performance do throughput de gravação diminui com o tamanho do arquivo, com o maior throughput possível para arquivos pequenos (menos de 32 MiB) sendo 16 arquivos por segundo.

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. O desempenho aprimorado do disco geralmente resulta em melhor taxa de transferência e mais input/output operações por segundo (IOPS). Para acessar informações sobre como adicionar discos, consulte Configurar armazenamento em cache adicional.

Para medir a taxa de transferência, use as métricas `ReadBytes` e `WriteBytes` com a estatística `Samples` 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**
>
> CloudWatch as métricas não estão disponíveis para todos os gateways. Para obter informações sobre métricas de gateway, consulte Monitorando seu gateway de de FSx 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 sobrecarregando a assinatura CPUs do servidor host.

Ao adicionar mais CPUs ao servidor host do gateway, você aumenta a capacidade de processamento do gateway. Isso permite que seu gateway lide, paralelamente, com o armazenamento de dados do seu aplicativo no armazenamento local e com o upload desses dados para o S3 para Windows File Server. CPUs Além disso, ajuda a garantir que seu gateway receba recursos de CPU suficientes quando o host for compartilhado com outros 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 em seu servidor host de gateway. Você pode usar 24 CPUs para melhorar significativamente o desempenho do seu gateway. Recomendamos a seguinte configuração de gateway para o servidor de host do gateway:

- 24 CPUs.
- 16 GiB de 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 de 16 TiB a 32 TiB
  - 48 GiB de RAM reservada para gateways com tamanho de cache de 32 TiB a 64 TiB
- Disco 1 anexado ao controlador paravirtual 1, para ser usado como cache do gateway da seguinte forma:
  - SSD usando um NVMe controlador.
- Adaptador de rede 1 configurado na rede 1 da VM:
  - Use a rede VM 1 e adicione VMXnet3 (10 Gbps) para ser usada para ingestão.
- Adaptador de rede 2 configurado na rede 2 da VM:
  - Use a rede VM 2 e adicione uma VMXnet3 (10 Gbps) a ser usada para se conectar. 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 de armazenamento físico subjacentes são representados como um 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. É possível usar as métricas `ReadBytes` e `WriteBytes` do gateway para medir o total de throughput de dados.

Para seu aplicativo, compare a taxa de transferência medidas com a taxa de transferência desejada. Se a taxa de transferência medida for inferior à taxa de transferência desejada, a ampliação da largura de banda entre o aplicativo e o gateway pode melhorar o desempenho se a rede for o gargalo. Da mesma forma, você pode aumentar a largura de banda entre a VM e os discos locais, se eles não estiverem diretamente vinculados.

Adicione recursos de CPU ao seu ambiente de aplicativos

Se seu aplicativo puder usar recursos adicionais de CPU, adicionar mais CPUs pode ajudar seu aplicativo a escalar sua I/O carga.

Algumas operações de FSx arquivo no File Gateway, como renomeações de pastas de nível superior ou alterações de permissão, podem resultar em várias operações de arquivo que levam a uma alta I/O carga no sistema de arquivos do Windows File Server. FSx Se o sistema de arquivos não tiver recursos de desempenho suficientes para sua carga de trabalho, o sistema de arquivos poderá excluir as cópias paralelas porque prioriza a disponibilidade de cópias paralelas contínuas em I/O relação à retenção histórica.

No FSx console da Amazon, verifique a página de monitoramento e desempenho para ver se seu sistema de arquivos está subprovisionado. Se estiver, você poderá mudar para o armazenamento de SSD, aumentar a capacidade de throughput ou aumentar o IOPS da SSD para lidar com sua workload.

Maximizar o throughput do Gateway de Arquivos do S3

As seções a seguir descrevem as práticas recomendadas para maximizar o throughput entre seus clientes NFS e SMB, o Gateway de Arquivos do S3 e o Amazon S3. A orientação fornecida em cada seção contribui de modo incremental para melhorar o throughput geral. Embora nenhuma dessas recomendações seja necessária e não sejam interdependentes, elas foram selecionadas e ordenadas de uma forma lógica Suporte usada para testar e ajustar as implementações do S3 File

Gateway. Ao implementar e testar essas sugestões, lembre-se de que cada implantação do Gateway de Arquivos do S3 é exclusiva, portanto, seus resultados podem variar.

O Gateway de Arquivos do S3 oferece uma interface de arquivo para armazenar e recuperar objetos do Amazon S3 utilizando protocolos de arquivo NFS ou SMB padrão do setor, com um mapeamento 1:1 nativo entre arquivo e objeto. Você implanta o S3 File Gateway como uma máquina virtual localmente em seu ambiente VMware Microsoft Hyper-V ou Linux KVM, ou na nuvem como AWS uma instância do Amazon EC2. O Gateway de Arquivos do S3 não foi projetado para atuar como um substituto completo do NAS empresarial. O Gateway de Arquivos do S3 emula um sistema de arquivos, mas não se trata de um. Usar o Amazon S3 como armazenamento de back-end durável cria uma sobrecarga adicional em cada I/O operação, portanto, avaliar o desempenho do S3 File Gateway em relação a um NAS ou servidor de arquivos existente não é uma comparação equivalente.

Implantar seu gateway no mesmo local que seus clientes

Recomendamos implantar seu dispositivo virtual do Gateway de Arquivos do S3 em um local físico com a menor latência de rede possível entre ele e seus clientes NFS ou SMB. Ao escolher um local para o gateway, pense no seguinte:

- A menor latência de rede para o gateway pode ajudar a melhorar a performance de clientes NFS ou SMB.
- O Gateway de Arquivos do S3 foi projetado para tolerar maior latência de rede entre o gateway e o Amazon S3 do que entre o gateway e os clientes.
- Para instâncias do Gateway de Arquivos do S3 implantadas no Amazon EC2, recomendamos manter o gateway e os clientes NFS ou SMB no mesmo grupo de posicionamento. Para acessar mais informações, consulte Grupos de posicionamento de instâncias do Amazon EC2 no Guia do usuário do Amazon Elastic Compute Cloud.

Reduzir os gargalos causados por discos lentos

Recomendamos monitorar a `IoWaitPercent` CloudWatch métrica para identificar gargalos de desempenho que podem resultar da lentidão dos discos de armazenamento no S3 File Gateway. Ao tentar otimizar os problemas de performance relacionados ao disco, pense no seguinte:

- `IoWaitPercent` informa a porcentagem de tempo que a CPU está aguardando uma resposta do disco de cache ou local.

- Quando `IoWaitPercent` é maior que 5–10%, isso geralmente indica um gargalo no gateway causado por discos com performance insuficiente. Essa métrica deve ser a mais próxima possível de 0%, o que significa que o gateway nunca está esperando no disco, o que ajuda a otimizar os recursos da CPU.
- Você pode verificar `IoWaitPercent` a guia Monitoramento do console do Storage Gateway ou configurar CloudWatch os alarmes recomendados para notificá-lo automaticamente se a métrica ultrapassar um limite específico. Para obter mais informações, consulte Criação de CloudWatch alarmes recomendados para seu gateway.
- Recomendamos usar um NVMe ou um SSD para minimizar os discos raiz e de cache do seu gateway. `IoWaitPercent`

Ajustar a alocação de recursos da máquina virtual para CPU, RAM e discos de cache

Ao tentar otimizar o throughput do Gateway de Arquivos do S3, é importante alocar recursos suficientes para a VM do gateway, incluindo CPU, RAM e discos de cache. Os requisitos mínimos de recursos virtuais de 4 CPUs, 16 GB de RAM e 150 GB de armazenamento em cache geralmente são adequados apenas para cargas de trabalho menores. Ao alocar recursos virtuais para workloads maiores, recomendamos o seguinte:

- Aumente o número alocado CPUs para entre 16 e 48, dependendo do uso típico da CPU gerado pelo seu S3 File Gateway. Você pode monitorar o uso da CPU usando a métrica `UserCpuPercent`. Para acessar mais informações, consulte Noções básicas das métricas de gateway.
- Aumente a RAM alocada para entre 32 e 64 GB.

> **Note**
>
> O Gateway de Arquivos do S3 não pode utilizar mais de 64 GB de RAM.

- Use NVMe nosso SSD para discos raiz e disco de cache e dimensione seus discos de cache para se alinharem ao conjunto máximo de dados de trabalho que você planeja gravar no gateway. Para obter mais informações, consulte as melhores práticas de dimensionamento de cache do S3 File Gateway no canal oficial da Amazon Web Services YouTube .
- Adicione pelo menos quatro discos de cache virtual ao gateway, em vez de usar um único disco grande. Vários discos virtuais podem melhorar a performance mesmo que compartilhem o mesmo

disco físico subjacente, mas as melhorias geralmente são maiores quando os discos virtuais estão localizados em discos físicos subjacentes diferentes.

Por exemplo, se quiser implantar 12 TB de cache, poderá utilizar uma das seguintes configurações:

- 4 discos de cache de 3 TB.
- 8 discos de cache de 1,5 TB.
- 12 discos de cache de 1 TB.

Além da performance, isso permite um gerenciamento mais eficiente da máquina virtual ao longo do tempo. Conforme sua workload muda, você pode aumentar de modo incremental o número de discos de cache e sua capacidade geral de cache, mantendo o tamanho original de cada disco virtual individual para preservar a integridade do gateway.

Para acessar mais informações, consulte Determinar o volume de armazenamento do disco local.

Ao implantar o Gateway de Arquivos do S3 como uma instância do Amazon EC2, pense no seguinte:

- O tipo de instância que você escolher pode afetar significativamente a performance do gateway. O Amazon EC2 oferece ampla flexibilidade para ajustar a alocação de recursos para sua instância do Gateway de Arquivos do S3.
- Para os tipos de instância do Amazon EC2 recomendados para o Gateway de Arquivos do S3, consulte Requisitos para tipos de instância do Amazon EC2.
- Você pode alterar o tipo de instância do Amazon EC2 que hospeda um Gateway de Arquivos do S3 ativo. Isso permite que você ajuste facilmente a geração de hardware e a alocação de recursos do Amazon EC2 para encontrar uma proporção ideal. price-to-performance Para alterar o tipo de instância, use o seguinte procedimento no console do Amazon EC2:
  1. Interrompe a instância do Amazon EC2.
  2. Altere o tipo de instância do Amazon EC2.
  3. Ligue a instância do Amazon EC2.

  > **Note**
  >
  > A interrupção de uma instância que hospeda um Gateway de Arquivos do S3 interromperá temporariamente o acesso ao compartilhamento de arquivos. Certifique-se de agendar uma janela de manutenção, se necessário.

- A price-to-performance proporção de uma instância do Amazon EC2 se refere à quantidade de poder computacional que você obtém pelo preço pago. Normalmente, as instâncias do Amazon EC2 de nova geração oferecem a price-to-performance melhor proporção, com hardware mais novo e desempenho aprimorado a um custo relativamente menor em comparação com as gerações anteriores. Fatores, como tipo de instância, região e padrões de uso, afetam essa proporção, por isso é importante selecionar a instância certa para sua workload específica a fim de otimizar a relação custo-benefício.

Ajustar o nível de segurança do SMB

O SMBv3 protocolo permite tanto a assinatura SMB quanto a criptografia SMB, que têm algumas desvantagens em desempenho e segurança. Para otimizar o throughput, você pode ajustar o nível de segurança SMB do gateway a fim de especificar quais desses recursos de segurança são aplicados às conexões do cliente. Para acessar mais informações, consulte Definir um nível de segurança para seu gateway.

Ao ajustar o nível de segurança SMB, pense no seguinte:

- O nível de segurança padrão para o Gateway de Arquivos do S3 é Aplicar criptografia. Essa configuração aplica criptografia e assinatura para conexões de clientes SMB com compartilhamentos de arquivos do gateway, o que significa que todo o tráfego do cliente para o gateway é criptografado. Essa configuração não afeta o tráfego do gateway para AWS, que é sempre criptografado.

  O gateway limita cada conexão de cliente criptografada a uma única vCPU. Por exemplo, se você tiver apenas 1 cliente criptografado, esse cliente estará limitado a apenas 1 vCPU, mesmo que 4 ou mais v CPUs estejam alocados para o gateway. Por esse motivo, o throughput de conexões criptografadas de um único cliente para o Gateway de Arquivos do S3 normalmente fica entre 40 e 60 MB/s.
- Se seus requisitos de segurança permitirem um procedimento mais relaxado, você poderá alterar o nível de segurança para Negociado pelo cliente, o que desabilitará a criptografia SMB e aplicará somente a assinatura SMB. Com essa configuração, as conexões do cliente com o gateway podem utilizar vários vCPUs, o que normalmente resulta em maior desempenho de taxa de transferência.

> **Note**
>
> Depois de alterar o nível de segurança SMB do seu Gateway de Arquivos do S3, você deve esperar que o status do compartilhamento de arquivos mude de Atualizando para Disponível no console do Storage Gateway e, depois, desconectar e reconectar seus clientes SMB para que a nova configuração entre em vigor.

Usar vários encadeamentos e clientes para paralelizar as operações de gravação

É difícil ter a máxima performance de throughput com um Gateway de Arquivos do S3 que usa somente um cliente NFS ou SMB para gravar um arquivo por vez, porque a gravação sequencial de um único cliente é uma operação de encadeamento único. Em vez disso, recomendamos usar vários encadeamentos de cada cliente NFS ou SMB para gravar vários arquivos em paralelo e usar vários clientes NFS ou SMB simultaneamente no seu Gateway de Arquivos do S3 a fim de maximizar o throughput do gateway.

O uso de vários encadeamentos pode melhorar significativamente a performance. No entanto, o uso de mais encadeamentos requer mais recursos do sistema, o que pode afetar negativamente a performance se o gateway não for dimensionado para atender ao aumento da carga. Em uma implantação típica, você pode esperar ter uma melhor performance de throughput à medida que adiciona mais encadeamentos e clientes, até atingir as limitações máximas de hardware e largura de banda para seu gateway. Recomendamos experimentar diferentes quantidades de encadeamentos para encontrar o equilíbrio ideal entre velocidade e uso de recursos do sistema para sua configuração específica de hardware e rede.

Pense nas seguintes informações sobre ferramentas comuns que podem ajudar você a testar a configuração do encadeamento e do cliente:

- Você pode testar a performance de gravação em vários encadeamentos utilizando ferramentas, como robocopy, para copiar um conjunto de arquivos em um compartilhamento de arquivos no seu gateway. Por padrão, o robocopy usa 8 encadeamentos ao copiar arquivos, mas você pode especificar até 128.

  Para usar vários encadeamentos com robocopy, adicione a opção `/MT:n` ao seu comando, em que n é o número de encadeamentos que você deseja usar. Por exemplo:

```
robocopy C:\source D:\destination /MT:64
```

Esse comando usará 64 encadeamentos para a operação de cópia.

> **Note**
>
> Não recomendamos usar o Windows Explorer para arrastar e soltar arquivos ao testar o throughput máximo, pois esse método é limitado a um único encadeamento e copia os arquivos sequencialmente.

Para acessar mais informações, consulte robocopy no site do Microsoft Learn.

- Você também pode realizar testes usando ferramentas comuns de benchmarking de armazenamento, como DISKSPD ou FIO. Essas ferramentas têm opções para ajustar o número de encadeamentos, a profundidade de E/S e outros parâmetros de acordo com seus requisitos específicos de workload.

  DiskSpd permite controlar o número de segmentos usando o `-t` parâmetro. Por exemplo:

  ```
  diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
  ```

  Este exemplo de comando faz o seguinte:

  - Cria um arquivo de teste de 10 GB (`-c1G`)
  - Funciona por 300 segundos (`-d300`)
  - Executa um I/O teste aleatório com 50% de leituras e 50% de gravações (`-r -w50`)
  - Usa 64 encadeamentos (`-t64`)
  - Define a profundidade da fila para 32 por encadeamento (`-o32`)
  - Usa tamanho de bloco de 1 MB (`-b1M`)
  - Desativa o armazenamento em cache de hardware e software (`-h -L`)

  Para acessar mais informações, consulte Usar o DISKSPD para testar a performance do armazenamento da workload no site do Microsoft Learn.

- O FIO usa o parâmetro `numjobs` para controlar o número de encadeamentos paralelos. Por exemplo:

```
fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
--size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
group_reporting
```

Este exemplo de comando faz o seguinte:

- Executa um I/O teste aleatório (`--rw=randrw`)
- Executa 70% de leituras e 30% de gravações (`--rwmixread=70`).
- Usa tamanho de bloco de 1 MB (`--bs=1M`).
- Define a I/O profundidade para 64 (`--iodepth=64`)
- Testa em um arquivo de 10 GB (`--size=10G`).
- É executado por 5 minutos (`--runtime=300`).
- Cria 64 trabalhos paralelos (encadeamentos) (`--numjobs=64`).
- Usa mecanismo assíncrono I/O () `--ioengine=libaio`
- Agrupa os resultados para facilitar a análise (`--group_reporting`).

Para acessar mais informações, consulte fio na página do manual do Linux.

-

Desativa a atualização automática do cache.

O recurso de atualização automática de cache permite que seu Gateway de Arquivos do S3 atualize seus metadados automaticamente, o que pode ajudar a capturar quaisquer alterações que usuários ou aplicações façam em seu conjunto de arquivos gravando diretamente no bucket do Amazon S3, em vez de por meio do gateway. Para acessar mais informações, consulte Atualizar o cache de objetos do bucket do Amazon S3.

Para otimizar o throughput do gateway, recomendamos desativar esse recurso em implantações em que todas as leituras e gravações no bucket do Amazon S3 serão realizadas por meio do Gateway de Arquivos do S3.

Ao configurar a atualização automatizada de cache, pense no seguinte:

- Se você precisar usar a atualização automática de cache porque os usuários ou aplicações em sua implantação ocasionalmente gravam diretamente no Amazon S3, recomendamos configurar o maior intervalo de tempo possível entre as atualizações, o que ainda seja prático para suas

necessidades comerciais. Um intervalo maior de atualização do cache ajuda a reduzir o número de operações de metadados que o gateway precisa realizar ao navegar em diretórios ou modificar arquivos.

Por exemplo: defina a atualização automática do cache como 24 horas, em vez de 5 minutos, se isso for tolerável para sua workload.

- O intervalo de tempo mínimo é 5 minutos. O intervalo máximo é de 30 dias.
- Se você optar por definir um intervalo de atualização de cache muito curto, recomendamos testar a experiência de navegação em diretórios para seus clientes NFS e SMB. O tempo necessário para atualizar o cache do gateway pode aumentar substancialmente, dependendo do número de arquivos e subdiretórios em seu bucket do Amazon S3.

Aumentar o número de encadeamentos de upload do Amazon S3

Por padrão, o Gateway de Arquivos do S3 abre oito encadeamentos para upload de dados do Amazon S3, o que oferece capacidade de upload suficiente para a maioria das implantações típicas. No entanto, é possível que um gateway receba dados de clientes NFS e SMB a uma taxa maior do que a que pode ser carregada para o Amazon S3 com a capacidade padrão de oito encadeamentos, o que pode fazer com que o cache local atinja seu limite de armazenamento.

Em circunstâncias específicas, Suporte pode aumentar a contagem do pool de threads de upload do Amazon S3 para seu gateway de 8 para 40, o que permite que mais dados sejam carregados paralelamente. Dependendo da largura de banda e de outros fatores específicos de sua implantação, isso pode aumentar significativamente a performance do upload e ajudar a reduzir a quantidade de armazenamento em cache necessária para oferecer suporte à sua workload.

Recomendamos usar a `CachePercentDirty` CloudWatch métrica para monitorar a quantidade de dados armazenados nos discos de cache do gateway local que ainda não foram enviados para o Amazon S3 e Suporte entrar em contato para ajudar a determinar se o aumento da contagem do pool de threads de upload pode melhorar a taxa de transferência do seu S3 File Gateway. Para acessar mais informações, consulte Noções básicas das métricas de gateway.

> **Note**
>
> Essa configuração consome recursos adicionais da CPU do gateway. Recomendamos monitorar o uso da CPU do gateway e, se necessário, aumentar os recursos alocados da CPU.

Aumentar as configurações de tempo limite do SMB

Quando o Gateway de Arquivos do S3 copia arquivos grandes para um compartilhamento de arquivos SMB, a conexão do cliente SMB pode expirar após um longo período.

Recomendamos estender a configuração de tempo limite da sessão SMB para seus clientes SMB para 20 minutos ou mais, dependendo do tamanho dos arquivos e da velocidade de gravação do seu gateway. O padrão é 300 segundos ou 5 minutos. Para acessar mais informações, consulte O trabalho de backup do gateway falha ou há erros ao gravar no gateway.

Ativar o bloqueio oportunista para aplicações compatíveis

O bloqueio oportunista, ou “oplocks”, é habilitado por padrão para cada novo Gateway de Arquivos do S3. Ao usar oplocks com aplicações compatíveis, o cliente agrupa várias operações menores em outras maiores, o que é mais eficiente para o cliente, o gateway e a rede. Recomendamos manter o bloqueio oportunista ativado se você usar aplicações que aproveitam o cache local do lado do cliente, como o Microsoft Office, o Adobe Suite e muitos outros, pois isso pode melhorar significativamente a performance.

Se você desativar o bloqueio oportunista, as aplicações que oferecem suporte a oplocks normalmente abrirão arquivos grandes (50 MB ou mais) muito mais lentamente. Esse atraso ocorre porque o gateway envia dados em partes de 4 KB, o que resulta em alta I/O e baixa taxa de transferência.

Ajuste a capacidade do gateway de acordo com o tamanho do conjunto de arquivos de trabalho

O parâmetro de capacidade do gateway especifica o número máximo de arquivos para os quais seu gateway armazenará metadados em seu cache local. Por padrão, a capacidade do gateway é definida como Pequena, o que significa que o gateway armazena metadados de até 5 milhões de arquivos. A configuração padrão funciona bem para a maioria das workloads, mesmo que haja centenas de milhões ou até bilhões de objetos no Amazon S3, porque somente um pequeno subconjunto de arquivos é acessado ativamente em determinado momento em uma implantação típica. Esse grupo de arquivos é chamado de “conjunto de trabalho”.

Se sua workload acessa regularmente um conjunto de arquivos de trabalho com mais de 5 milhões, seu gateway precisará realizar remoções frequentes de cache, que são pequenas operações de E/S armazenadas na RAM e persistentes no disco raiz. Isso pode afetar negativamente a performance do gateway, pois ele busca novos dados do Amazon S3.

Você pode monitorar a métrica `IndexEvictions` para determinar o número de arquivos cujos metadados foram removidos do cache para abrir espaço para novas entradas. Para acessar mais informações, consulte Noções básicas das métricas de gateway.

Recomendamos usar a ação da API `UpdateGatewayInformation` para aumentar a capacidade do gateway para corresponder ao número de arquivos em seu conjunto de trabalho típico. Para obter mais informações, consulte UpdateGatewayInformation.

> **Note**
>
> Aumentar a capacidade do gateway requer capacidade adicional de RAM e disco raiz.
>
> - Pequeno (5 milhões de arquivos) requer pelo menos 16 GB de RAM e 80 GB de disco raiz.
> - Médio (10 milhões de arquivos) requer pelo menos 32 GB de RAM e 160 GB de disco raiz.
> - Grande (20 milhões de arquivos) requer 64 GB de RAM e 240 GB de disco raiz.

> **Important**
>
> A capacidade do gateway não pode ser reduzida.

Implementar vários gateways para workloads maiores

Recomendamos dividir sua workload em vários gateways quando possível, em vez de consolidar muitos compartilhamentos de arquivos em um único gateway grande. Por exemplo, você pode isolar um compartilhamento de arquivos muito usado em um gateway e agrupar os compartilhamentos utilizados com menor frequência em outro gateway.

Ao planejar uma implantação com vários gateways e compartilhamentos de arquivos, pense no seguinte:

- O número máximo de compartilhamentos de arquivos em um único gateway é 50, mas o número de compartilhamentos de arquivos gerenciados por um gateway pode afetar a performance do gateway. Para acessar mais informações, consulte Orientação de performance para gateways com vários compartilhamentos de arquivos.
- Os recursos em cada Gateway de Arquivos do S3 são compartilhados em todos os compartilhamentos de arquivos, sem particionamento.

- Um único compartilhamento de arquivos com uso intenso pode afetar a performance de outros compartilhamentos no gateway.

> **Note**
>
> Não recomendamos a criação de vários compartilhamentos de arquivos associados ao mesmo local do Amazon S3 a partir de vários gateways, a menos que pelo menos um deles seja somente leitura.
> Gravações simultâneas no mesmo arquivo a partir de vários gateways são consideradas um cenário de várias gravações, o que pode causar problemas de integridade de dados.

Otimizar o Gateway de Arquivos do S3 para backups de bancos de dados do SQL Server

Os backups de banco de dados são um caso de uso comum e recomendado para o Gateway de Arquivos do S3, que fornece retenção econômica de curto e longo prazo ao armazenar backups de banco de dados no Amazon S3, com a capacidade de ciclo de vida para níveis de armazenamento de menor custo, conforme necessário. Com essa solução, você pode reduzir a necessidade de aplicações de backup empresarial utilizando ferramentas integradas, como o SQL Server Management Studio e o Oracle RMAN.

As seções a seguir descrevem as práticas recomendadas para ajustar sua implantação do Gateway de Arquivos do S3 para performance otimizada e suporte econômico para centenas de terabytes de backups de bancos de dados SQL. A orientação fornecida em cada seção contribui de modo incremental para melhorar o throughput geral. Embora nenhuma dessas recomendações seja necessária e não sejam interdependentes, elas foram selecionadas e ordenadas de uma forma lógica Suporte usada para testar e ajustar as implementações do S3 File Gateway. Ao implementar e testar essas sugestões, lembre-se de que cada implantação do Gateway de Arquivos do S3 é exclusiva, portanto, seus resultados podem variar.

O Gateway de Arquivos do S3 oferece uma interface de arquivo para armazenar e recuperar objetos do Amazon S3 utilizando protocolos de arquivo NFS ou SMB padrão do setor, com um mapeamento 1:1 nativo entre arquivo e objeto. Você implanta o S3 File Gateway como uma máquina virtual localmente em seu ambiente VMware Microsoft Hyper-V ou Linux KVM, ou na nuvem como AWS uma instância do Amazon EC2. O Gateway de Arquivos do S3 não foi projetado para atuar como um substituto completo do NAS empresarial. O Gateway de Arquivos do S3 emula um sistema

de arquivos, mas não se trata de um. Usar o Amazon S3 como armazenamento de back-end durável cria uma sobrecarga adicional em cada I/O operação, portanto, avaliar o desempenho do S3 File Gateway em relação a um NAS ou servidor de arquivos existente não é uma comparação equivalente.

Implantar seu gateway no mesmo local que seus servidores SQL

Recomendamos implantar seu dispositivo virtual do Gateway de Arquivos do S3 em um local físico com a menor latência de rede possível entre ele e seus servidores SQL. Ao escolher um local para o gateway, pense no seguinte:

- A menor latência de rede para o gateway pode ajudar a melhorar a performance de clientes SMB, como servidores SQL.
- O Gateway de Arquivos do S3 foi projetado para tolerar maior latência de rede entre o gateway e o Amazon S3 do que entre o gateway e os clientes.
- Para instâncias do Gateway de Arquivos do S3 implantadas no Amazon EC2, recomendamos manter o gateway e os servidores SQL no mesmo grupo de posicionamento. Para acessar mais informações, consulte Grupos de posicionamento de instâncias do Amazon EC2 no Guia do usuário do Amazon Elastic Compute Cloud.

Reduzir os gargalos causados por discos lentos

Recomendamos monitorar a `IoWaitPercent` CloudWatch métrica para identificar gargalos de desempenho que podem resultar da lentidão dos discos de armazenamento no S3 File Gateway. Ao tentar otimizar os problemas de performance relacionados ao disco, pense no seguinte:

- `IoWaitPercent` informa a porcentagem de tempo que a CPU está aguardando uma resposta do disco de cache ou local.
- Quando `IoWaitPercent` é maior que 5–10%, isso geralmente indica um gargalo no gateway causado por discos com performance insuficiente. Essa métrica deve ser a mais próxima possível de 0%, o que significa que o gateway nunca está esperando no disco, o que ajuda a otimizar os recursos da CPU.
- Você pode verificar `IoWaitPercent` a guia Monitoramento do console do Storage Gateway ou configurar CloudWatch os alarmes recomendados para notificá-lo automaticamente se a métrica ultrapassar um limite específico. Para obter mais informações, consulte Criação de CloudWatch alarmes recomendados para seu gateway.

- Recomendamos usar um NVMe ou um SSD para minimizar os discos raiz e de cache do seu gateway. `IoWaitPercent`

Ajustar a alocação de recursos da máquina virtual do Gateway de Arquivos do S3 para CPU, RAM e discos de cache

Ao tentar otimizar o throughput do Gateway de Arquivos do S3, é importante alocar recursos suficientes para a VM do gateway, incluindo CPU, RAM e discos de cache. Os requisitos mínimos de recursos virtuais de 4 CPUs, 16 GB de RAM e 150 GB de armazenamento em cache geralmente são adequados apenas para cargas de trabalho menores. Ao alocar recursos virtuais para workloads maiores, recomendamos o seguinte:

- Aumente o número alocado CPUs para entre 16 e 48, dependendo do uso típico da CPU gerado pelo seu S3 File Gateway. Você pode monitorar o uso da CPU usando a métrica `UserCpuPercent`. Para acessar mais informações, consulte Noções básicas das métricas de gateway.
- Aumente a RAM alocada para entre 32 e 64 GB.

  > **Note**
  >
  > O Gateway de Arquivos do S3 não pode utilizar mais de 64 GB de RAM.

- Use NVMe nosso SSD para discos raiz e disco de cache e dimensione seus discos de cache para se alinharem ao conjunto máximo de dados de trabalho que você planeja gravar no gateway. Para obter mais informações, consulte as melhores práticas de dimensionamento de cache do S3 File Gateway no canal oficial da Amazon Web Services YouTube .
- Adicione pelo menos quatro discos de cache virtual ao gateway, em vez de usar um único disco grande. Vários discos virtuais podem melhorar a performance mesmo que compartilhem o mesmo disco físico subjacente, mas as melhorias geralmente são maiores quando os discos virtuais estão localizados em discos físicos subjacentes diferentes.

  Por exemplo, se quiser implantar 12 TB de cache, poderá utilizar uma das seguintes configurações:

  - 4 discos de cache de 3 TB.
  - 8 discos de cache de 1,5 TB.
  - 12 discos de cache de 1 TB.

Além da performance, isso permite um gerenciamento mais eficiente da máquina virtual ao longo do tempo. Conforme sua workload muda, você pode aumentar de modo incremental o número de discos de cache e sua capacidade geral de cache, mantendo o tamanho original de cada disco virtual individual para preservar a integridade do gateway.

Para acessar mais informações, consulte Determinar o volume de armazenamento do disco local.

Ao implantar o Gateway de Arquivos do S3 como uma instância do Amazon EC2, pense no seguinte:

- O tipo de instância que você escolher pode afetar significativamente a performance do gateway. O Amazon EC2 oferece ampla flexibilidade para ajustar a alocação de recursos para sua instância do Gateway de Arquivos do S3.
- Para os tipos de instância do Amazon EC2 recomendados para o Gateway de Arquivos do S3, consulte Requisitos para tipos de instância do Amazon EC2.
- Você pode alterar o tipo de instância do Amazon EC2 que hospeda um Gateway de Arquivos do S3 ativo. Isso permite que você ajuste facilmente a geração de hardware e a alocação de recursos do Amazon EC2 para encontrar uma proporção ideal. price-to-performance Para alterar o tipo de instância, use o seguinte procedimento no console do Amazon EC2:

  1. Interrompe a instância do Amazon EC2.
  2. Altere o tipo de instância do Amazon EC2.
  3. Ligue a instância do Amazon EC2.

  > **Note**
  >
  > A interrupção de uma instância que hospeda um Gateway de Arquivos do S3 interromperá temporariamente o acesso ao compartilhamento de arquivos. Certifique-se de agendar uma janela de manutenção, se necessário.

- A price-to-performance proporção de uma instância do Amazon EC2 se refere à quantidade de poder computacional que você obtém pelo preço pago. Normalmente, as instâncias do Amazon EC2 de nova geração oferecem a price-to-performance melhor proporção, com hardware mais novo e desempenho aprimorado a um custo relativamente menor em comparação com as gerações anteriores. Fatores, como tipo de instância, região e padrões de uso, afetam essa proporção, por isso é importante selecionar a instância certa para sua workload específica a fim de otimizar a relação custo-benefício.

Melhorar o throughput do cliente SMB ajustando o nível de segurança do seu Gateway de Arquivos do S3

O SMBv3 protocolo permite tanto a assinatura SMB quanto a criptografia SMB, que têm algumas desvantagens em desempenho e segurança. Para otimizar o throughput, você pode ajustar o nível de segurança SMB do gateway a fim de especificar quais desses recursos de segurança são aplicados às conexões do cliente. Para acessar mais informações, consulte Definir um nível de segurança para seu gateway.

Ao ajustar o nível de segurança SMB, pense no seguinte:

- O nível de segurança padrão para o Gateway de Arquivos do S3 é Aplicar criptografia. Essa configuração aplica criptografia e assinatura para conexões de clientes SMB com compartilhamentos de arquivos do gateway, o que significa que todo o tráfego do cliente para o gateway é criptografado. Essa configuração não afeta o tráfego do gateway para AWS, que é sempre criptografado.

  O gateway limita cada conexão de cliente criptografada a uma única vCPU. Por exemplo, se você tiver apenas 1 cliente criptografado, esse cliente estará limitado a apenas 1 vCPU, mesmo que 4 ou mais v CPUs estejam alocados para o gateway. Por esse motivo, o throughput de conexões criptografadas de um único cliente para o Gateway de Arquivos do S3 normalmente fica entre 40 e 60 MB/s.
- Se seus requisitos de segurança permitirem um procedimento mais relaxado, você poderá alterar o nível de segurança para Negociado pelo cliente, o que desabilitará a criptografia SMB e aplicará somente a assinatura SMB. Com essa configuração, as conexões do cliente com o gateway podem utilizar vários vCPUs, o que normalmente resulta em maior desempenho de taxa de transferência.

> **Note**
>
> Depois de alterar o nível de segurança SMB do seu Gateway de Arquivos do S3, você deve esperar que o status do compartilhamento de arquivos mude de Atualizando para Disponível no console do Storage Gateway e, depois, desconectar e reconectar seus clientes SMB para que a nova configuração entre em vigor.

Melhorar o throughput do cliente SMB dividindo os backups SQL em vários arquivos

- É difícil ter a máxima performance de throughput com um Gateway de Arquivos do S3 que usa somente um servidor SQL para gravar um arquivo por vez, porque a gravação sequencial de um único servidor SQL é uma operação de encadeamento único. Em vez disso, recomendamos usar vários encadeamentos de cada cliente de servidor SQL para gravar vários arquivos em paralelo e usar vários servidores SQL simultaneamente no seu Gateway de Arquivos do S3 a fim de maximizar o throughput do gateway. Com os backups do SQL, dividir os backups em vários arquivos permite que cada arquivo utilize um encadeamento separado, que gravará vários arquivos simultaneamente no compartilhamento de arquivos do Gateway de Arquivos do S3. Quanto mais encadeamentos você tiver, maior será o throughput que poderá alcançar, até os limites do gateway.
- O SQL Server oferece suporte à gravação em vários arquivos ao mesmo tempo durante uma única operação de backup. Por exemplo, é possível especificar vários destinos de arquivos usando comandos T-SQL ou SQL Server Management Studio (SSMS). Cada arquivo usa um encadeamento separado para enviar dados do servidor SQL ao compartilhamento de arquivos do gateway. Essa abordagem permite uma melhor I/O taxa de transferência, o que pode melhorar significativamente a velocidade e a eficiência do backup.

Ao configurar os backups do servidor SQL, pense no seguinte:

- Ao dividir os backups em vários arquivos, os administradores do SQL Server podem otimizar os tempos de backup e gerenciar backups de grandes bancos de dados com maior eficiência.
- O número de arquivos usados depende da configuração de armazenamento e dos requisitos de performance do servidor. Para bancos de dados grandes, recomendamos dividir os backups em vários arquivos menores entre 10 GB e 20 GB cada.
- Não há limite estrito para quantos arquivos o SQL Server pode gravar durante um backup, mas considerações práticas, como arquitetura de armazenamento e largura de banda de rede, devem orientar essa escolha.

Para obter mais informações, consulte:

- Faça backup do SQL Server 43-67% mais rápido gravando em vários arquivos
- Armazene facilmente seus backups do SQL Server no Amazon S3 usando o Gateway de Arquivos

Evitar falhas de cópia de arquivos grandes aumentando as configurações de tempo limite de SMB

Quando o Gateway de Arquivos do S3 copia arquivos grandes de backup do SQL para um compartilhamento de arquivos SMB, a conexão do cliente SMB pode expirar após um longo período. Recomendamos estender a configuração de tempo limite da sessão SMB para seus clientes SMB do servidor SQL para 20 minutos ou mais, dependendo do tamanho dos arquivos e da velocidade de gravação do seu gateway. O padrão é 300 segundos ou 5 minutos. Para acessar mais informações, consulte O trabalho de backup do gateway falha ou há erros ao gravar no gateway.

Aumentar o número de encadeamentos de upload do Amazon S3

Por padrão, o Gateway de Arquivos do S3 abre oito encadeamentos para upload de dados do Amazon S3, o que oferece capacidade de upload suficiente para a maioria das implantações típicas. No entanto, é possível que um gateway receba dados de servidores SQL a uma taxa maior do que a que pode ser carregada para o Amazon S3 com a capacidade padrão de oito encadeamentos, o que pode fazer com que o cache local atinja seu limite de armazenamento.

Em circunstâncias específicas, Suporte pode aumentar a contagem do pool de threads de upload do Amazon S3 para seu gateway de 8 para 40, o que permite que mais dados sejam carregados paralelamente. Dependendo da largura de banda e de outros fatores específicos de sua implantação, isso pode aumentar significativamente a performance do upload e ajudar a reduzir a quantidade de armazenamento em cache necessária para oferecer suporte à sua workload.

Recomendamos usar a `CachePercentDirty` CloudWatch métrica para monitorar a quantidade de dados armazenados nos discos de cache do gateway local que ainda não foram enviados para o Amazon S3 e Suporte entrar em contato para ajudar a determinar se o aumento da contagem do pool de threads de upload pode melhorar a taxa de transferência do seu S3 File Gateway. Para acessar mais informações, consulte Noções básicas das métricas de gateway.

> **Note**
>
> Essa configuração consome recursos adicionais da CPU do gateway. Recomendamos monitorar o uso da CPU do gateway e, se necessário, aumentar os recursos alocados da CPU.

Desativa a atualização automática do cache.

O recurso de atualização automática de cache permite que seu Gateway de Arquivos do S3 atualize seus metadados automaticamente, o que pode ajudar a capturar quaisquer alterações que usuários ou aplicações façam em seu conjunto de arquivos gravando diretamente no bucket do Amazon S3, em vez de por meio do gateway. Para acessar mais informações, consulte Atualizar o cache de objetos do bucket do Amazon S3.

Para otimizar o throughput do gateway, recomendamos desativar esse recurso em implantações em que todas as leituras e gravações no bucket do Amazon S3 serão realizadas por meio do Gateway de Arquivos do S3.

Ao configurar a atualização automatizada de cache, pense no seguinte:

- Se você precisar usar a atualização automática de cache porque os usuários ou aplicações em sua implantação ocasionalmente gravam diretamente no Amazon S3, recomendamos configurar o maior intervalo de tempo possível entre as atualizações, o que ainda seja prático para suas necessidades comerciais. Um intervalo maior de atualização do cache ajuda a reduzir o número de operações de metadados que o gateway precisa realizar ao navegar em diretórios ou modificar arquivos.

  Por exemplo: defina a atualização automática do cache como 24 horas, em vez de 5 minutos, se isso for tolerável para sua workload.
- O intervalo de tempo mínimo é 5 minutos. O intervalo máximo é de 30 dias.
- Se você optar por definir um intervalo de atualização de cache muito curto, recomendamos testar a experiência de navegação em diretórios para seus servidores SQL. O tempo necessário para atualizar o cache do gateway pode aumentar substancialmente, dependendo do número de arquivos e subdiretórios em seu bucket do Amazon S3.

Implantar vários gateways para oferecer suporte à workload

É possível que o Storage Gateway comporte backups SQL para grandes ambientes com centenas de bancos de dados SQL, vários servidores SQL e centenas de terabytes de dados de backup dividindo a workload em vários gateways.

Ao planejar uma implantação com vários gateways e servidores SQL, pense no seguinte:

- Normalmente, um único gateway pode carregar até 20 TB por dia, com recursos de hardware e largura de banda suficientes. Você pode aumentar esse limite em até 40 TB por dia aumentando o número de encadeamentos de upload do Amazon S3.
- Recomendamos realizar um proof-of-concept teste para medir o desempenho e considerar todas as variáveis em sua implantação. Depois de determinar o throughput máximo da sua workload de backup SQL, você pode escalar o número de gateways para atender aos seus requisitos.
- Recomendamos projetar sua solução pensando no crescimento, pois o número e o tamanho dos bancos de dados podem aumentar com o tempo. Para continuar a escalar e oferecer suporte a uma workload crescente, você pode implantar gateways adicionais conforme necessário.

Recursos adicionais para workloads de backup de banco de dados

- Armazene backups do SQL Server no Amazon S3 usando AWS Storage Gateway
- Armazene facilmente seus backups do SQL Server no Amazon S3 usando o Gateway de Arquivos
- Usando AWS Storage Gateway para armazenar backups de bancos de dados Oracle no Amazon S3
- Backing up Oracle databases to Amazon S3 at scale
- Integre um banco de dados SAP ASE ao Amazon S3 usando AWS Storage Gateway
- Como um AWS herói usa AWS Storage Gateway para backup na nuvem
- Práticas recomendadas de dimensionamento de cache do Gateway de Arquivos do S3

Segurança no AWS Storage Gateway

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao AWS Storage Gateway, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Storage Gateway. Os tópicos a seguir mostram como configurar o Storage Gateway para atender aos seus objetivos de segurança e de conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Storage Gateway.

Proteção de dados no AWS Storage Gateway

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no AWS Storage Gateway. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para saber mais sobre a privacidade de dados, consulte as Data Privacy FAQ. Para saber mais sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access

Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Storage Gateway ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia de dados usando AWS KMS

O Amazon FSx File Gateway oferece suporte à criptografia SMB até a especificação SMB v3.1.1 mais recente, incluindo AES 128 CCM e AES 128 GCM. Clientes compatíveis se conectarão usando criptografia automaticamente. Além disso, FSx o File Gateway usa criptografia SMB quando se comunica com FSx o Windows File Server em. AWS Você deve configurar um Direct Connect link e definir políticas apropriadas para permitir que o tráfego SMB e o tráfego de gerenciamento passem para AWS. AWS

Criptografar um sistema de arquivos

Para obter informações, consulte Criptografia de dados FSx na Amazon no Guia do usuário do Amazon FSx para Windows File Server.

Ao usar 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 . FSx
- Os usuários do IAM devem ter as permissões necessárias para chamar as operações AWS KMS da API. Para obter mais informações, consulte Como usar políticas do IAM com o AWS KMS no Guia do desenvolvedor do AWS Key Management Service .

> **Important**
>
> Ao usar uma AWS KMS chave para criptografia do lado do servidor, você deve escolher uma chave simétrica. O Storage Gateway não é compatível com chaves assimétricas. Para obter mais informações, consulte Como usar chaves simétricas e assimétricas no AWS Key Management Service Guia do desenvolvedor.

Para obter mais informações sobre AWS KMS, consulte O que é AWS Key Management Service?

Gerenciamento de identidade e acesso para AWS Storage Gateway

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do AWS SGW. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como o AWS Storage Gateway funciona com o IAM

- Exemplos de políticas baseadas em identidade para AWS Storage Gateway
- Solução de problemas AWS de identidade e acesso ao Storage Gateway
- Usar tags para controlar o acesso ao gateway e aos recursos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas AWS de identidade e acesso ao Storage Gateway).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como o AWS Storage Gateway funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade para AWS Storage Gateway)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas

políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o AWS Storage Gateway funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AWS SGW, saiba quais recursos do IAM estão disponíveis para uso com o AWS SGW.

Recursos do IAM que você pode usar com o AWS Storage Gateway

Recurso do IAM	AWS Suporte SGW
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim

Recurso do IAM	AWS Suporte SGW
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados a serviço	Sim

Para ter uma visão de alto nível de como o AWS SGW e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para SGW AWS

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para SGW AWS

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte. Exemplos de políticas baseadas em identidade para AWS Storage Gateway

Políticas baseadas em recursos no SGW AWS

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para a AWS SGW

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do AWS SGW, consulte Ações definidas pelo AWS Storage Gateway na Referência de Autorização de Serviço.

As ações de política no AWS SGW usam o seguinte prefixo antes da ação:

```
sgw
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "sgw:action1",
```

```
      "sgw:action2"
         ]
```

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte. Exemplos de políticas baseadas em identidade para AWS Storage Gateway

Recursos de política para AWS SGW

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do AWS SGW e seus ARNs, consulte Resources Defined by AWS Storage Gateway na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Storage Gateway.

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte. Exemplos de políticas baseadas em identidade para AWS Storage Gateway

Chaves de condição de política para AWS SGW

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a”

ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do AWS SGW, consulte Chaves de condição do AWS Storage Gateway na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Actions Defined by AWS Storage Gateway.

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte. Exemplos de políticas baseadas em identidade para AWS Storage Gateway

ACLs em AWS SGW

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS SGW

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS o SGW

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Sessões de acesso direto para AWS SGW

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para AWS SGW

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do AWS SGW. Edite as funções de serviço somente quando o AWS SGW fornecer orientação para fazer isso.

Funções vinculadas a serviços para SGW AWS

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções

vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para AWS Storage Gateway

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS SGW. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS SGW, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição do AWS Storage Gateway na Referência de Autorização de Serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Usando o console AWS SGW
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos AWS SGW em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões

definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o console AWS SGW

Para acessar o console do AWS Storage Gateway, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AWS SGW em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do AWS SGW, anexe também o AWS SGW *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
```

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

Solução de problemas AWS de identidade e acesso ao Storage Gateway

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS SGW e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no AWS SGW
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do AWS SGW

Não estou autorizado a realizar uma ação no AWS SGW

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `sgw:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `sgw:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS SGW.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no AWS Storage Gateway. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

> **Important**
>
> O Storage Gateway pode assumir perfis de serviço existentes que são passados usando a ação de política `iam:PassRole`, mas não oferece suporte às políticas do IAM que usam a chave de contexto `iam:PassedToService` para limitar a ação a serviços específicos. Para saber mais, consulte os seguintes tópicos no Manual do usuário do AWS Identity and Access Management :
>
> - IAM: passe uma função do IAM para um AWS serviço específico
> - Conceder permissões a um usuário para passar uma função para um serviço AWS
> - Chaves disponíveis para IAM

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do AWS SGW

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AWS SGW oferece suporte a esses recursos, consulteComo o AWS Storage Gateway funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Usar tags para controlar o acesso ao gateway e aos recursos

Para controlar o acesso aos recursos e ações do gateway, você pode usar políticas AWS Identity and Access Management (IAM) com base 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.

Controle do acesso baseado 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`.

JSON

```
{
    "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:us-east-1:111122223333:*/*"
        }
    ]
}
```

Controlar o acesso baseado em tags em uma solicitação do IAM

Para controlar o que um usuário pode fazer em 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 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 permitirá 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.

JSON

```
{
   "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"
            }
         }
      }
   ]
```

```
}
```

Validação de conformidade para AWS Storage Gateway

Auditores terceirizados avaliam a segurança e a conformidade do AWS Storage Gateway como parte de vários programas de AWS conformidade. Eles incluem SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR e HITRUST CSF.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS Serviços no escopo do programa de conformidade AWS . Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade com relação à conformidade ao usar o Storage Gateway é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido sobre sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos com foco em segurança e conformidade em. AWS
- Documento técnico sobre arquitetura para segurança e conformidade com a HIPAA — Este whitepaper descreve como as empresas podem usar para criar aplicativos compatíveis com a HIPAA. AWS
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- Avaliação de recursos com as regras do Guia do AWS Config Desenvolvedor — O AWS Config serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub CSPM— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência no AWS Storage Gateway

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade.

An Região da AWS é um local físico em todo o mundo onde os data centers estão agrupados. Cada grupo de data centers lógicos é chamado de zona de disponibilidade (AZ). Cada um Região da AWS consiste em um mínimo de três isolados e fisicamente separados AZs dentro de uma área geográfica. Ao contrário de outros provedores de nuvem, que geralmente definem uma região como um único data center, o design de múltiplas AZ de cada um Região da AWS oferece vantagens distintas. Cada AZ tem alimentação, resfriamento e segurança física independentes e está conectada por meio de redes redundantes. ultra-low-latency Se sua implantação exigir um foco na alta disponibilidade, você poderá configurar serviços e recursos de forma múltipla AZs para obter maior tolerância a falhas.

Regiões da AWS atenda aos mais altos níveis de segurança de infraestrutura, conformidade e proteção de dados. Todo o tráfego entre eles AZs é criptografado. O desempenho da rede é suficiente para realizar a replicação síncrona entre. AZs AZs simplifique os serviços e recursos de particionamento para alta disponibilidade. Se sua implantação for particionada AZs, seus recursos ficarão melhor isolados e protegidos de problemas como quedas de energia, quedas de raios, tornados, terremotos e muito mais. AZs estão fisicamente separados por uma distância significativa de qualquer outra AZ, embora todos estejam a 100 km (60 milhas) um do outro.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Storage Gateway oferece suporte ao 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, consulte Usando o VMware vSphere High Availability com o Storage Gateway Usando o Gateway.

Segurança da infraestrutura no AWS Storage Gateway

Como serviço gerenciado, o AWS Storage Gateway é protegido pelos procedimentos AWS globais de segurança de rede descritos em Security Pillar - AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Storage Gateway pela rede. Os clientes devem ser compatíveis com o Transport Layer Security (TLS) 1.2. Os clientes também devem ter compatibilidade com 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 compatibilidade com 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 é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

> **Note**
>
> Você deve tratar o dispositivo AWS Storage Gateway como uma máquina virtual gerenciada e não deve tentar acessar ou modificar sua instalação de forma alguma. A tentativa de instalar um software de digitalização ou atualizar qualquer pacote de software usando métodos diferentes do mecanismo normal de atualização do gateway pode causar um mau funcionamento do gateway e afetar nossa capacidade de oferecer suporte ou corrigir o gateway.
> AWS revisa, analisa e corrige CVEs regularmente. Incorporamos correções para esses problemas no Storage Gateway como parte do nosso ciclo normal de lançamento de software. Essas correções são normalmente aplicadas como parte do processo normal de atualização do gateway durante as janelas de manutenção programada. Para obter mais informações sobre atualizações de gateway, consulte Gerenciando atualizações de gateway usando o AWS Storage Gateway console.

AWS Práticas recomendadas de segurança

AWS fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. Essas melhores práticas são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no ambiente, trate-as como considerações úteis em vez de requisitos. Para obter mais informações, consulte Práticas recomendadas de segurança da AWS.

Registro e monitoramento em AWS Storage Gateway

O Storage Gateway é integrado com AWS CloudTrail um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Storage Gateway. CloudTrail captura todas as chamadas de API para o Storage Gateway como eventos. As chamadas capturadas incluem as

chamadas do console do Storage Gateway e as chamadas de código para as operações de API do Storage Gateway. Se você criar uma trilha, poderá ativar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Storage Gateway. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Storage Gateway, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações do Storage Gateway em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no Storage Gateway, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Storage Gateway, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Storage Gateway são registradas em log e documentadas no tópico Ações. Por exemplo, chamadas para as `ShutdownGateway` ações `ActivateGatewayListGateways`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Noções básicas sobre as entradas dos arquivos de log do Storage Gateway

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a ação.

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "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 CloudTrail registro que demonstra a ListGateways 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 - 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"
              }]
}
```

Solucionar problemas com a implantação do Storage Gateway

A seguir, você encontrará informações sobre as práticas recomendadas e a solução de problemas relacionados a gateways, plataformas de host, sistemas de arquivos, alta disponibilidade, recuperação de dados e snapshots. As informações de solução de problemas do gateway on-premises abrangem gateways implantados em plataformas de virtualização compatíveis. As informações de solução de problemas de alta disponibilidade abrangem gateways em execução na plataforma VMware vSphere High Availability (HA).

Tópicos

- Solucionar problemas de gateway off-line: saiba como diagnosticar problemas que podem fazer com que seu gateway apareça off-line no console do Storage Gateway.
- Solucionar problemas: problemas no Active Directory: saiba o que fazer se você receber mensagens de erro, como `NETWORK_ERROR`, `TIMEOUT` ou `ACCESS_DENIED` ao tentar associar seu Gateway de Arquivos a um domínio do Microsoft Active Directory.
- Solução de problemas: problemas de ativação do gateway: saiba o que fazer se você receber uma mensagem de erro interna ao tentar ativar seu Storage Gateway.
- Solução de problemas: problemas no gateway on-premises- Saiba mais sobre problemas típicos que você pode encontrar ao trabalhar com seus gateways locais e como permitir Suporte a conexão com seu gateway para ajudar na solução de problemas.
- Solução de problemas: problemas de configuração do Microsoft Hyper-V: saiba mais sobre problemas comuns que podem ser encontrados ao implantar o Storage Gateway na plataforma Microsoft Hyper-V.
- Solução de problemas: problemas no gateway do Amazon EC2: encontre informações sobre problemas típicos que podem ocorrer ao trabalhar com gateways implantados no Amazon EC2.
- Solução de problemas: problemas no dispositivo de hardware- Saiba como resolver problemas que você possa encontrar com o AWS Storage Gateway Hardware Appliance.
- Solução de problemas: problemas no Gateway de Arquivos- Encontre informações que possam ajudar você a entender a causa dos erros e das notificações de saúde que aparecem nos CloudWatch registros do seu File Gateway.
- Solução de problemas: problemas de alta disponibilidade- Saiba o que fazer se você tiver problemas com gateways implantados em um ambiente de VMware HA.

Solução de problemas: gateway offline no console do Storage Gateway

Use as informações de solução de problemas a seguir para determinar o que fazer se o console do AWS Storage Gateway mostrar que seu gateway está off-line.

Seu gateway pode estar sendo exibido como off-line por um ou mais dos seguintes motivos:

- O gateway não consegue alcançar os endpoints do serviço Storage Gateway.
- O gateway foi desligado inesperadamente.
- Um disco de cache associado ao gateway foi desconectado, modificado ou falhou.

Para colocar o gateway novamente on-line, identifique e resolva o problema que fez com que ele ficasse off-line.

Verificar o firewall ou proxy associado

Se você configurou o gateway para usar um proxy ou colocou o gateway atrás de um firewall, revise as regras de acesso do proxy ou do firewall. O proxy ou firewall deve permitir o tráfego de e para as portas de rede e os endpoints de serviço exigidos pelo Storage Gateway. Para obter mais informações, consulte Requisitos de rede e firewall.

Verifique se há uma inspeção contínua de SSL ou pacotes profundos do tráfego do gateway

Se uma inspeção SSL ou profunda de pacotes estiver sendo executada atualmente no tráfego de rede entre seu gateway e AWS, talvez seu gateway não consiga se comunicar com os endpoints de serviço necessários. Para colocar o gateway novamente on-line, você deve desabilitar a inspeção.

Verifique a métrica IOWait Porcentagem após uma reinicialização ou atualização de software

Depois de uma reinicialização ou atualização de software, verifique se a métrica `IOWaitPercent` do Gateway de Arquivos é 10 ou maior. Isso pode fazer com que o gateway demore a responder enquanto reconstrói o cache de índice na RAM. Para obter mais informações, consulte Solução de problemas: uso de CloudWatch métricas.

Verificar se há queda de energia ou falha de hardware no host do hipervisor

Uma queda de energia ou falha de hardware no host do hipervisor do gateway pode fazer com que o gateway seja desligado inesperadamente e fique inacessível. Depois de restaurar a energia e a conectividade de rede, o gateway ficará acessível novamente.

Assim que o gateway estiver on-line novamente, tome medidas para recuperar seus dados. Para obter mais informações, consulte Práticas recomendadas para a recuperação de dados.

Verificar se há problemas com um disco de cache associado

Seu gateway pode ficar off-line se pelo menos um dos discos de cache associados ao gateway tiver sido removido, alterado ou redimensionado, ou se estiver corrompido.

Se um disco de cache funcional foi removido do host do hipervisor:

1. Encerre o gateway.
2. Adicione novamente o disco.

   > **Note**
   >
   > Adicione o disco ao mesmo nó de disco.

3. Reinicie o gateway.

Se um disco de cache estiver corrompido, tiver sido substituído ou redimensionado:

- Siga o procedimento do Método 2 descrito em Substituir seu Gateway de Arquivos do S3 existente por uma nova instância para configurar um novo gateway e baixar novamente as informações do disco de cache da Nuvem AWS .

Solução de problemas: problemas ao associar o gateway ao Active Directory

Use as informações de solução de problemas a seguir para saber o que fazer se você receber mensagens de erro, como `NETWORK_ERROR`, `TIMEOUT` ou `ACCESS_DENIED` ao tentar associar o Gateway de Arquivos a um domínio do Microsoft Active Directory.

Para resolver esses erros, realize as verificações e configurações a seguir.

Confirmar se o gateway pode acessar o controlador de domínio executando um teste de nping

Para executar um teste de nping:

1. Conecte-se ao console local do gateway utilizando seu software de gerenciamento de hipervisor (VMware, Hyper-V ou KVM) para gateways on-premises ou utilizando ssh para gateways do Amazon EC2.
2. Digite o número correspondente para selecionar Console do Gateway e, depois, insira h para listar todos os comandos disponíveis. Para testar a conectividade entre a máquina virtual do Storage Gateway e o domínio, execute o seguinte comando:

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > Substitua `corp.domain.com` pelo nome DNS do seu domínio do Active Directory e substitua 389 pela porta LDAP do seu ambiente.
   > Verifique se você abriu as portas necessárias no seu firewall.

Veja a seguir um exemplo de teste de nping bem-sucedido em que o gateway conseguiu acessar o controlador de domínio bem-sucedido:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>

Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

Veja a seguir um exemplo de teste de nping em que não há conectividade ou resposta do destino `corp.domain.com`:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Conferir as opções de DHCP definidas para a VPC da sua instância de gateway do Amazon EC2

Se o Gateway de Arquivos estiver sendo executado em uma instância do Amazon EC2, assegure-se de que um conjunto de opções de DHCP esteja devidamente configurado e anexado à nuvem privada virtual (VPC) que contém a instância do gateway. Para acessar mais informações, consulte Conjuntos de opções DHCP na Amazon VPC.

Confirmar se o gateway pode resolver o domínio executando uma consulta dig

Se o domínio não puder ser resolvido pelo gateway, este não poderá ingressar no domínio.

Como executar uma consulta dig:

1. Conecte-se ao console local do gateway utilizando seu software de gerenciamento de hipervisor (VMware, Hyper-V ou KVM) para gateways on-premises ou utilizando ssh para gateways do Amazon EC2.
2. Digite o número correspondente para selecionar Console do Gateway e, depois, insira h para listar todos os comandos disponíveis. Para testar se o gateway pode resolver o domínio, execute o seguinte comando:

   ```
   dig -d corp.domain.com
   ```

> **Note**
>
> Substitua `corp.domain.com` pelo nome DNS do seu domínio do Active Directory.

Veja a seguir um exemplo de resposta bem-sucedida:

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

Conferir as configurações e perfis do controlador de domínio

Verifique se o controlador de domínio não está definido como somente leitura e se ele tem perfis suficientes para a associação dos computadores. Para testar isso, tente associar outros servidores da mesma sub-rede da VPC que a VM do gateway ao domínio.

Conferir se o gateway está associado ao controlador de domínio mais próximo

Como prática recomendada, recomendamos associar seu gateway a um controlador de domínio que esteja geograficamente próximo ao dispositivo de gateway. Se o dispositivo de gateway não conseguir se comunicar com o controlador de domínio em 20 segundos devido à latência da rede,

o processo de associação ao domínio poderá expirar. Por exemplo, o processo pode expirar se o dispositivo de gateway estiver no Leste dos EUA (Norte da Virgínia) Região da AWS e o controlador de domínio estiver na Ásia-Pacífico (Cingapura). Região da AWS

> **Note**
>
> Para aumentar o valor de tempo limite padrão de 20 segundos, você pode executar o comando join-domain no AWS Command Line Interface (AWS CLI) e incluir a `--timeout-in-seconds` opção de aumentar o tempo. Você também pode usar a chamada JoinDomain da API e incluir o `TimeoutInSeconds` parâmetro para aumentar o tempo. O valor de tempo limite máximo é 3.600 segundos.
> Se você receber erros ao executar AWS CLI comandos, verifique se está usando a AWS CLI versão mais recente.

Confirmar se o Active Directory cria objetos de computador na unidade organizacional (UO) padrão

Assegure-se de que o Microsoft Active Directory não tenha nenhum objeto de política de grupo que crie objetos de computador em qualquer local que não seja a UO padrão. Antes de associar seu gateway ao domínio do Active Directory, deve existir um novo objeto de computador na UO padrão. Alguns ambientes do Active Directory são personalizados para serem diferentes OUs para objetos recém-criados. Para garantir que exista um novo objeto de computador para a VM do gateway na UO padrão, tente criar o objeto de computador manualmente no controlador de domínio antes de associar o gateway ao domínio. Você também pode executar o comando join-domain utilizando a AWS CLI. Depois, especifique a opção para `--organizational-unit`.

> **Note**
>
> O processo de criação do objeto de computador é chamado de pré-preparação.

Conferir os logs de eventos do seu controlador de domínio

Se você não conseguir associar o gateway ao domínio depois de tentar todas as outras verificações e configurações descritas nas seções anteriores, recomendamos examinar os logs de eventos do controlador de domínio. Confira se há erros no visualizador de eventos do controlador de domínio. Verifique se as consultas do gateway chegaram ao controlador de domínio.

Solução de problemas: erro interno durante a ativação do gateway

As solicitações de ativação do Storage Gateway atravessam dois caminhos de rede. As solicitações de ativação recebidas que são enviadas por um cliente se conectam à máquina virtual (VM) do gateway ou à instância do Amazon Elastic Compute Cloud (Amazon EC2) pela porta 80. Se o gateway receber com êxito a solicitação de ativação, ele se comunicará com os endpoints do Storage Gateway para receber uma chave de ativação. Se o gateway não conseguir alcançar os endpoints do Storage Gateway, ele responderá ao cliente com uma mensagem de erro interna.

Use as informações de solução de problemas a seguir para determinar o que fazer se você receber uma mensagem de erro interna ao tentar ativar o AWS Storage Gateway.

> **Note**
>
> - Implante novos gateways usando o arquivo de imagem de máquina virtual mais recente ou a versão da imagem de máquina da Amazon (AMI). Ocorrerá um erro interno se tentar ativar um gateway que usa uma AMI desatualizada.
> - Antes de baixar a AMI, selecione o tipo de gateway correto que você pretende implantar. Os arquivos.ova e AMIs para cada tipo de gateway são diferentes e não são intercambiáveis.

Resolver erros ao ativar o gateway usando um endpoint público

Para resolver erros de ativação ao ativar seu gateway usando um endpoint público, execute as verificações e configurações a seguir.

Verificar as portas necessárias

Para gateways implantados no ambiente on-premises, verifique se as portas estão abertas no firewall local. Para gateways implantados em uma instância do Amazon EC2, verifique se as portas estão abertas no grupo de segurança da instância. Para confirmar se as portas estão abertas, execute um comando telnet no endpoint público por meio de um servidor. Esse servidor deve estar na mesma sub-rede do gateway. Por exemplo, os seguintes comandos telnet testam a conexão com a porta 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
```

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

Para confirmar se o próprio gateway pode alcançar o endpoint, acesse o console da VM local do gateway (para gateways com implantação no ambiente on-premises). Ou você pode usar SSH para a instância do gateway (para gateways implantados no Amazon EC2). Em seguida, execute um teste de conectividade de rede. Confirme se o teste retorna a mensagem `[PASSED]`. Para obter mais informações, consulte Testing your gateway's network connectivity.

> **Note**
>
> O nome de usuário de login padrão para o console do gateway é `admin` e a senha padrão é `password`.

Garantir que a segurança do firewall não modifique os pacotes enviados do gateway para os endpoints públicos

Inspeções SSL, inspeções profundas de pacotes ou outras formas de segurança de firewall podem interferir nos pacotes enviados do gateway. O handshake de SSL falhará se o certificado SSL for modificado de acordo com o que o endpoint de ativação espera. Para confirmar que não há nenhuma inspeção de SSL em andamento, execute um comando OpenSSL no endpoint de ativação principal (`anon-cp.storagegateway.region.amazonaws.com`) na porta 443. Você deve executar esse comando em uma máquina que esteja na mesma sub-rede do gateway:

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> *region*Substitua pelo seu Região da AWS.

Se não houver inspeção de SSL em andamento, o comando retornará uma resposta similar à seguinte:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Se houver uma inspeção SSL em andamento, a resposta mostrará uma cadeia de certificados alterada, semelhante à seguinte:

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

O endpoint de ativação aceita handshakes de SSL somente se reconhecer o certificado SSL. Isso significa que o tráfego de saída do gateway para os endpoints deve estar isento das inspeções realizadas por firewalls em sua rede. Essas inspeções podem ser uma inspeção SSL ou uma inspeção profunda de pacotes.

Verificar a sincronização de horas do gateway

Distorções de tempo excessivas podem causar erros de handshake de SSL. Para gateways on-premises, você pode usar o console da VM local do gateway para verificar a sincronização de horário do gateway. A diferença de tempo não deve ser superior a 60 segundos. Para obter mais informações, consulte Synchronizing Your Gateway VM Time.

A opção Gerenciamento de tempo do sistema não está disponível em gateways hospedados em instâncias do Amazon EC2. Para garantir que os gateways do Amazon EC2 possam sincronizar adequadamente o horário, confirme se a instância do Amazon EC2 pode se conectar à seguinte lista de grupos de servidores de NTP pelas portas UDP e TCP 123:

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Resolver erros ao ativar o gateway usando um endpoint da Amazon VPC

Para resolver erros de ativação ao ativar seu gateway usando um endpoint da Amazon Virtual Private Cloud (Amazon VPC), faça as seguintes verificações e configurações:

Verificar as portas necessárias

Certifique-se de que as portas necessárias em seu firewall local (para gateways com implantação no ambiente on-premises) ou grupo de segurança (para gateways implantados no Amazon EC2) estejam abertas. As portas necessárias para conectar um gateway a um endpoint da VPC do Storage Gateway são diferentes das necessárias para conectar um gateway a endpoints públicos. As seguintes portas são necessárias para estabelecer conexão com a um endpoint da VPC do Storage Gateway:

- TCP 443

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

Para obter mais informações, consulte Como criar um endpoint da VPC para o Storage Gateway.

Além disso, verifique o grupo de segurança conectado ao endpoint da VPC do Storage Gateway. O grupo de segurança padrão anexado ao endpoint pode não permitir acesso às portas necessárias. Crie um grupo de segurança que permita o tráfego do intervalo de endereços IP do seu gateway pelas portas necessárias. Em seguida, anexe esse grupo de segurança ao endpoint da VPC.

> **Note**
>
> Use o console da Amazon VPC para verificar o grupo de segurança que está conectado ao endpoint da VPC. Visualize o endpoint da VPC do Storage Gateway no console e escolha a guia Grupos de segurança.

Para confirmar se as portas necessárias estão abertas, você pode executar comandos telnet no endpoint da VPC do Storage Gateway. Você deve executar esses comandos em um servidor que esteja na mesma sub-rede do gateway. Você pode executar os testes no primeiro nome DNS que não especifique uma zona de disponibilidade. Por exemplo, os seguintes comandos telnet testam as conexões de porta necessárias usando o nome DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Garantir que a segurança do firewall não modifique os pacotes enviados do gateway ao endpoint da Amazon VPC do Storage Gateway

Inspeções SSL, inspeções profundas de pacotes ou outras formas de segurança de firewall podem interferir nos pacotes enviados do gateway. O handshake de SSL falhará se o certificado SSL for modificado de acordo com o que o endpoint de ativação espera. Para confirmar se não há nenhuma inspeção de SSL em andamento, execute um comando OpenSSL no endpoint da VPC do Storage Gateway. Você deve executar esse comando em uma máquina que esteja na mesma sub-rede do gateway. Execute o comando para cada porta necessária:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Se não houver inspeção de SSL em andamento, o comando retornará uma resposta similar à seguinte:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
```

```
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Se houver uma inspeção SSL em andamento, a resposta mostrará uma cadeia de certificados alterada, semelhante à seguinte:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

O endpoint de ativação aceita handshakes de SSL somente se reconhecer o certificado SSL. Isso significa que o tráfego de saída do gateway para o endpoint da VPC pelas portas necessárias está isento das inspeções realizadas pelos firewalls de sua rede. Essas inspeções podem ser inspeções SSL ou inspeções profundas de pacotes.

Verificar a sincronização de horas do gateway

Distorções de tempo excessivas podem causar erros de handshake de SSL. Para gateways on-premises, você pode usar o console da VM local do gateway para verificar a sincronização de horário do gateway. A diferença de tempo não deve ser superior a 60 segundos. Para obter mais informações, consulte Synchronizing Your Gateway VM Time.

A opção Gerenciamento de tempo do sistema não está disponível em gateways hospedados em instâncias do Amazon EC2. Para garantir que os gateways do Amazon EC2 possam sincronizar adequadamente o horário, confirme se a instância do Amazon EC2 pode se conectar à seguinte lista de grupos de servidores de NTP pelas portas UDP e TCP 123:

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

Verificar se há um proxy HTTP e confirme as configurações do grupo de segurança associado

Antes da ativação, verifique se você tem um proxy HTTP no Amazon EC2 configurado na VM do gateway on-premises como um proxy Squid na porta 3128. Nesse caso, verifique se:

- O grupo de segurança anexado ao proxy HTTP no Amazon EC2 deve ter uma regra de entrada. Essa regra de entrada deve permitir o tráfego do proxy Squid na porta 3128 pelo endereço IP da VM do gateway.
- O grupo de segurança anexado ao endpoint da VPC do Amazon EC2 deve ter regras de entrada. Essas regras de entrada devem permitir o tráfego nas portas 1026-1028, 1031, 2222 e 443 pelo endereço IP do proxy HTTP no Amazon EC2.

Resolver erros ao ativar o gateway usando um endpoint público e quando há um endpoint da VPC do Storage Gateway na mesma VPC

Para resolver erros ao ativar seu gateway usando um endpoint público quando há um endpoint da Amazon Virtual Private Cloud (Amazon VPC) na mesma VPC, execute as verificações e configurações a seguir.

Confirmar se a configuração Habilitar nome de DNS privado não está habilitada no endpoint da VPC do Storage Gateway

Se a opção Habilitar nome de DNS privado estiver habilitada, você não poderá ativar nenhum gateway dessa VPC para o endpoint público.

Para desabilitar a opção de nome de DNS privado:

1. Abra o console da Amazon VPC.
2. No painel de navegação, escolha Endpoints.
3. Escolha seu endpoint da VPC do Storage Gateway.
4. Escolha Ações.
5. Escolha Gerenciar nomes DNS privados.
6. Em Habilitar nome de DNS privado, selecione Habilitar para este endpoint.
7. Escolha Modificar nomes DNS privados para salvar a configuração.

Solução de problemas: problemas no gateway on-premises

Você pode encontrar informações a seguir sobre problemas típicos que você pode encontrar ao trabalhar com seus gateways locais e como permitir Suporte a conexão com seu gateway para ajudar na solução de problemas.

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
	• Pois VMware ESXi, o endereço IP da VM pode ser encontrado no cliente vSphere na guia Resumo. • 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 usar um firewall ou roteador para filtrar ou limitar o tráfego de rede, você deverá configurar o firewall e o roteador para permitir a comunicação externa com a AWS nesses endpoints de serviço. 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 no botão Prosseguir para a ativação no 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 Como testar a conectividade de rede do gateway. • Verifique se o horário do host está correto, se o host está configurado para sincronizar seu horário automaticamente com um servidor Network Time Protocol (NTP) e se o horário da VM do gateway está correto. Para obter informações sobre como sincronizar a hora dos hosts do hipervisor VMs, consulte. Configurar um servidor de NTP para seu gateway • Depois que executar essas etapas, poderá realizar novamente a implantação de gateway usando o console do Storage Gateway e o assistente Definir e ativar gateway. • Confira se a VM tem pelo menos 16 GB de RAM. A alocação do gateway falhará se houver menos de 16 GB de RAM. Para obter mais informações, consulte Requisitos de configuração do Gateway de Arquivos.

Problema	Medida a ser tomada
É necessário melhorar a largura de banda entre o gateway e a AWS.	Você pode melhorar a largura de banda do seu gateway AWS configurando sua conexão com a Internet AWS em um adaptador de rede (NIC) separado daquele que conecta seus aplicativos e a VM do gateway. Essa abordagem é útil se você tiver uma conexão de alta largura de banda AWS e quiser evitar a contenção de largura de banda, especialmente durante a restauração de um instantâneo. Em caso de necessidades de workloads com alto throughput, é possível usar o Direct Connect para estabelec er uma conexão de rede exclusiva entre o gateway on-premis es e a AWS. Para medir a largura de banda da conexão do seu gateway para AWS, use as `CloudBytesUploaded` métricas `CloudBytesDownloaded` e do gateway. Para saber mais sobre esse assunto, consulte Performance e otimização. 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.	• Na guia Gateway do console do Storage Gateway, verifique se os endereços IP da VM do gateway são os mesmos que você vê usando o software cliente hipervisor (ou seja, o VMware cliente vSphere ou o Microsoft Hyper-V Manager). Se você encontrar alguma incompatibilidade, reinicie seu gateway no console do Storage Gateway, conforme mostrado em Encerrar a VM do gateway. Após a reinicialização, os endereços na lista Endereços IP, na guia Gateway do console do Storage Gateway, devem corresponder aos endereços IP de seu gateway, que são determinados no cliente do hipervisor.
	  • Pois VMware ESXi, o endereço IP da VM pode ser encontrado no cliente vSphere na guia Resumo.
	  • No caso do Microsoft Hyper-V, para encontrar o endereço IP da VM, faça login no console local.
	• Verifique a conectividade do seu gateway AWS conforme descrito emComo testar a conectividade de rede do gateway.
	• Confira a configuração do adaptador de rede do gateway no cliente de gerenciamento do hipervisor e garanta que todas as interfaces que você pretende usar para o gateway estão ativadas.
	• Confira a configuração do adaptador de rede do seu gateway no console local do gateway. Para instruções, consulte Definir configurações de rede do gateway.
	
	Você pode visualizar a taxa de transferência de e para seu gateway no CloudWatch console da Amazon. Para obter mais informações sobre como medir a taxa de transferência de e para seu gateway até AWS, consultePerformance e otimização.

Você está tendo problemas para importar (implanta r) o Storage Gateway no Microsoft Hyper-V.	Consulte Solução de problemas: configuração do Microsoft Hyper-V, que examina alguns dos problemas comuns na implantação de um gateway no Microsoft Hyper-V.

Problema	Medida a ser tomada
É exibida uma mensagem que diz: "Os dados que foram gravados no volume do seu gateway não estão armazenados com segurança na AWS".	Você receberá essa mensagem se a VM do gateway foi criada a partir de um clone ou snapshot de outra VM do gateway. Se este não for o caso, entre em contato com o Suporte.

Ativando o Suporte acesso para ajudar a solucionar problemas em seu gateway hospedado localmente

O Storage Gateway fornece um console local que você pode usar para realizar várias tarefas de manutenção, incluindo Suporte permitir o acesso ao gateway para ajudá-lo a solucionar problemas do gateway. Por padrão, o Suporte acesso ao seu gateway está desativado. Esse acesso é ativado por meio do console local do host. Para dar Suporte acesso ao seu gateway, primeiro faça login no console local do host, navegue até o console do Storage Gateway e, em seguida, conecte-se ao servidor de suporte.

Para ativar o Suporte acesso ao seu gateway

1. Faça login no console local do host.
   - VMware ESXi — para obter mais informações, consulteAcessando o console local do Gateway com VMware ESXi.
   - Microsoft Hyper-V: para obter mais informações, consulte Acessar o console local do gateway com o Microsoft Hyper-V.
2. No prompt, insira o numeral correspondente para selecionar Console do gateway.
3. Insira **h** para abrir a lista de comandos disponíveis.
4. Execute um destes procedimentos:
   - Se o gateway estiver usando um endpoint público, na janela COMANDO DISPONÍVEIS, insira **`open-support-channel`** para se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.

- Se o gateway estiver usando um VPC endpoint, na janela AVAILABLE COMMANDS (Comandos disponíveis) insira **`open-support-channel`**. Se o gateway não estiver ativado, forneça o endpoint da VPC ou o endereço IP para o qual se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.

> **Note**
>
> O número do canal não é um número de porta Protocol/User Datagram Protocol (TCP/UDP (Controle de Transmissão). Na verdade, o gateway faz uma conexão Secure Shell (SSH) (TCP 22) com os servidores do Storage Gateway e providencia o canal de suporte para a conexão.

5. Depois que o canal de suporte for estabelecido, forneça seu número de serviço de suporte para Suporte que Suporte possa fornecer assistência na solução de problemas.
6. Quando a sessão de suporte for concluída, insira **`q`** para finalizá-la. Não feche a sessão até que o Suporte da Amazon Web Services notifique você que a sessão de suporte foi concluída.
7. Digite **`exit`** para encerrar a sessão do console do Storage Gateway.
8. Siga as instruções para sair do console local.

Solução de problemas: configuração do Microsoft Hyper-V

A tabela a seguir lista problemas comuns que podem ser encontrados ao implantar o Storage Gateway na plataforma Microsoft Hyper-V.

Problema	Medida a ser tomada
Você tenta importar um gateway e recebe a seguinte mensagem de erro: “A server error occurred while attempting to import the virtual machine. Import	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 Importar máquina virtual deve ser `AWS-Storage-Gateway` . Por exemplo:

Problema	Medida a ser tomada
failed. Unable to find virtual machine import files under location [...]. You can import a virtual machine only if you used Hyper-V to create and export it”.	`C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\ .` • 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. Se você planeja criar vários gateways por meio de um local de arquivos de origem descompactado, você deve selecionar Copiar a máquina virtual e marcar a caixa Duplicar todos os arquivos na caixa de diálogo Importar máquina virtual.
Você tenta importar um gateway e recebe a seguinte mensagem de erro: “A server error occurred while attempting to import the virtual machine. Import failed. Import task failed to copy file from [...]: The file exists. (0x80070050)”.	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 em Servidor no painel à esquerda da caixa de diálogo Configurações do Hyper-V.

Problema	Medida a ser tomada
Você tenta importar um gateway e recebe a seguinte mensagem de erro: “A server error occurred while attempting to import the virtual machine. Import failed. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again".	Ao importar o gateway, lembre-se de selecionar a opção Copiar a máquina virtual e de marcar a opção Duplicar todos os arquivos na caixa de diálogo Importar máquina virtual para criar um ID exclusivo para a VM.
Você tenta iniciar uma VM de gateway e recebe a seguinte mensagem de erro: “An error occurred while attempting to start the selected virtual machine(s). The child partition processor setting is incompatible with parent partition. ‘AWS-Storage-Gateway’ could not initializ e. (Virtual machine ID [...])”.	Esse erro provavelmente é causado por uma discrepância de CPU entre o necessário CPUs para o gateway e o disponível CPUs no host. Confirme se o hipervisor subjacente comporta a contagem de CPU da VM. Para obter mais informações sobre os requisitos do Storage Gateway, consulte Requisitos de configuração do Gateway de Arquivos.

Problema	Medida a ser tomada
Você tenta iniciar uma VM de gateway e recebe a seguinte mensagem de erro: “An error occurred while attempting to start the selected virtual machine(s). ‘AWS-Storage-Gateway’ could not initialize. (Virtual machine ID [...]) Failed to create partition: Insuffici ent system resources exist to complete the requested service. (0x800705AA)”.	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, consulte Requisitos de configuração do Gateway de Arquivos.
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 de NTP para seu gateway.
É necessário colocar os arquivos descompactados do Storage Gateway para o Microsoft Hyper-V no sistema de arquivos do host.	Acesse o host do mesmo modo que faz para acessar um servidor Microsoft Windows comum. Por exemplo, se o nome do host do hipervisor for `hyperv-server` , você poderá usar o seguinte caminho UNC `\\hyperv-server\c$` , que pressupõe que o nome `hyperv-server` pode ser resolvido ou é definido em seu arquivo de hosts locais.
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.

Problema	Medida a ser tomada
É possível notar um desempenho de rede ruim ao ativar a fila de máquinas virtuais (VMQ) para um host Hyper-V que esteja usando um adaptador de rede Broadcom.	Para obter informações sobre uma solução alternativa, consulte a documentação da Microsoft: Poor network performance on virtual machines on a Windows Server 2012 Hyper-V host if VMQ is enabled.

Solução de problemas: problemas no gateway do Amazon EC2

Nas seções a seguir, você encontrará problemas comuns que podem ocorrer ao trabalhar com um gateway implantado no Amazon EC2. Para obter mais informações sobre a diferença entre um gateway on-premises e um gateway implantado no Amazon EC2, consulte Implante um host padrão do Amazon EC2 para FSx o File Gateway.

Tópicos

A ativação do gateway não aconteceu após alguns minutos

Verifique o seguinte no console do Amazon EC2:

- A porta 80 está aberta no grupo de segurança associado à instância. Para obter mais informações sobre como modificar regras de grupos de segurança, consulte Adding a security group rule no Guia do usuário do Amazon EC2.
- A instância do gateway está marcada como em execução. No console do Amazon EC2, o valor do Estado para a instância deve ser EXECUTANDO.
- Certifique-se de que o tipo de instância do Amazon EC2 atende aos requisitos mínimos, conforme descrito em Requisitos de armazenamento.

Depois de corrigir o problema, tente ativar o gateway novamente. Para fazer isso, abra o console do Storage Gateway, selecione Implantar um novo gateway no Amazon EC2 e insira novamente o endereço IP da instância.

Não é possível encontrar a instância do gateway do EC2 na lista de instâncias

Se você não tiver atribuído uma tag de recurso à sua instância e tiver muitas instâncias em execução, talvez seja difícil saber em qual instância executou. Nesse caso, você pode executar as ações a seguir para encontrar a instância do gateway:

- Verifique o nome da imagem de máquina da Amazon (AMI) na guia Description (Descrição) da instância. Uma instância baseada na AMI do Storage Gateway deve iniciar com as palavras **`aws-storage-gateway-ami`**.
- Se tiver várias instâncias baseadas na AMI do Storage Gateway, verifique o horário de execução da instância para localizar a instância correta.

Você deseja se conectar à instância do gateway usando o Console de Série do Amazon EC2

É possível usar o Console de Série do Amazon EC2 para solucionar a inicialização, a configuração de rede e outros problemas. Consulte as instruções e dicas de solução de problemas em Amazon EC2 Serial Console no Guia do usuário do Amazon Elastic Compute Cloud.

Você quer ajudar Suporte a solucionar problemas do seu gateway Amazon EC2

O Storage Gateway fornece um console local que você pode usar para realizar várias tarefas de manutenção, incluindo Suporte permitir o acesso ao gateway para ajudá-lo a solucionar problemas do gateway. Por padrão, o Suporte acesso ao seu gateway está desativado. Esse acesso é ativado por meio do console local do Amazon EC2. O login no console local do Amazon EC2 é feito por meio do Secure Shell (SSH). Para conseguir fazer login por meio do SSH, o security group da instância deve ter uma regra que abre a porta TCP 22.

> **Note**
>
> Se você adicionar uma nova regra a um security group existente, essa nova regra será aplicada a todas as instâncias que usam esse security group. Para obter mais informações sobre grupos de segurança e como adicionar regras a eles, consulte Grupos de segurança do Amazon EC2 no Guia do usuário do Amazon EC2.

Para permitir a Suporte conexão com seu gateway, primeiro faça login no console local da instância do Amazon EC2, navegue até o console do Storage Gateway e, em seguida, forneça o acesso.

Para ativar o Suporte acesso a um gateway implantado em uma instância do Amazon EC2

1. Faça login no console local da instância do Amazon EC2. Para obter instruções, consulte Conectar-se à instância no Guia do usuário do Amazon EC2.

   Você pode usar o comando a seguir para fazer login no console local da Instância EC2.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*É o `.pem` arquivo que contém o certificado privado do par de chaves do EC2 que você usou para iniciar a instância do Amazon EC2. Para obter mais informações, consulte Recuperar a chave pública para seu par de chaves no Guia do usuário do Amazon EC2.
   > *INSTANCE-PUBLIC-DNS-NAME*É o nome público do Sistema de Nomes de Domínio (DNS) da sua instância do Amazon EC2 na qual seu gateway está sendo executado. Para obter esse nome DNS público, selecione a instância do Amazon EC2 no console do EC2 e clique na guia Descrição.

2. No prompt, insira **`6 - Command Prompt`** para abrir o console do canal do Suporte .
3. Insira **h** para abrir a janela COMANDOS DISPONÍVEIS.
4. Execute um destes procedimentos:

   - Se o gateway estiver usando um endpoint público, na janela COMANDO DISPONÍVEIS, insira **`open-support-channel`** para se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando

se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.

- Se o gateway estiver usando um VPC endpoint, na janela AVAILABLE COMMANDS (Comandos disponíveis) insira **`open-support-channel`**. Se o gateway não estiver ativado, forneça o endpoint da VPC ou o endereço IP para o qual se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.

> **Note**
>
> O número do canal não é um número de porta Protocol/User Datagram Protocol (TCP/UDP (Controle de Transmissão). Na verdade, o gateway faz uma conexão Secure Shell (SSH) (TCP 22) com os servidores do Storage Gateway e providencia o canal de suporte para a conexão.

5. Depois que o canal de suporte for estabelecido, forneça seu número de serviço de suporte para Suporte que Suporte possa fornecer assistência na solução de problemas.
6. Quando a sessão de suporte for concluída, insira **`q`** para finalizá-la. Não feche a sessão até que o Suporte da Amazon Web Services notifique você que a sessão de suporte foi concluída.
7. Digite **`exit`** para sair do console do Storage Gateway.
8. Siga os menus do console para encerrar a sessão na instância do Storage Gateway.

Solução de problemas: problemas no dispositivo de hardware

> **Note**
>
> Aviso de fim de disponibilidade: a partir de 12 de maio de 2025, o AWS Storage Gateway Hardware Appliance não será mais oferecido. Os clientes existentes com o AWS Storage Gateway Hardware Appliance podem continuar usando e recebendo suporte até maio de 2028. Como alternativa, você pode usar o AWS Storage Gateway serviço para dar aos seus aplicativos acesso local e na nuvem a armazenamento em nuvem praticamente ilimitado.

Os tópicos a seguir discutem problemas que você pode encontrar com o AWS Storage Gateway Hardware Appliance e sugestões para solucioná-los.

Tópicos

Não é possível determinar o endereço IP do serviço

Ao tentar se conectar ao serviço, verifique se você está usando o endereço IP do serviço, e não o do host. Configure o endereço IP do serviço no console de serviço e o do host, no console de hardware. Você verá o console de hardware quando iniciar o dispositivo de hardware. Para acessar o console de serviço do console de hardware, escolha Open Service Console (Abrir console de serviço).

Como executar uma redefinição de fábrica?

Se você precisar fazer uma redefinição de fábrica em seu equipamento, entre em contato com a equipe do AWS Storage Gateway Hardware Appliance para obter suporte, conforme descrito na seção Support a seguir.

Como executar uma reinicialização remota?

Se precisar reiniciar remotamente seu equipamento, é possível fazer isso usando a interface de gerenciamento do Dell iDRAC. Para obter mais informações, consulte i Ciclo de alimentação DRAC9 virtual: reinicialize remotamente PowerEdge os servidores Dell EMC no InfoHub site da Dell Technologies.

Onde encontrar suporte para o Dell iDRAC?

O PowerEdge servidor Dell vem com a interface de gerenciamento Dell iDRAC. Recomendamos o seguinte:

- Se você usar a interface de gerenciamento do iDRAC, deverá alterar a senha padrão. Para obter mais informações sobre as credenciais do iDRAC, consulte PowerEdge Dell - Quais são as credenciais de login padrão do iDRAC? .
- Certifique-se de que o firmware evite violações de segurança. up-to-date
- Mover a interface de rede do iDRAC para uma porta normal (`em`) poderá causar problemas de performance ou impedir o funcionamento normal do dispositivo.

Não é possível encontrar o número de série do dispositivo de hardware

Você pode encontrar o número de série do seu dispositivo de hardware AWS Storage Gateway usando o console do Storage Gateway.

Como descobrir o número de série do dispositivo de hardware:

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Selecione Hardware no menu de navegação no lado esquerdo da página.
3. Selecione o dispositivo de hardware na lista.
4. Localize o campo Número de série na guia Detalhes do dispositivo.

Onde obter suporte para o dispositivo de hardware

Para entrar em contato AWS sobre suporte técnico para seu dispositivo de hardware, consulte Suporte.

A Suporte equipe pode pedir que você ative o canal de suporte para solucionar seus problemas de gateway remotamente. Você não precisa dessa porta aberta para a operação normal do gateway, mas ela é necessária para a solução de problemas. Você pode ativar o canal de suporte no console de hardware, conforme mostrado no procedimento a seguir.

Para abrir um canal de suporte para AWS

1. Abra o console de hardware.
2. Escolha Abrir canal de suporte na parte inferior da página principal do console de hardware e pressione `Enter`.

   Se não houver problemas de conectividade de rede ou firewall, o número da porta atribuída será exibido em até 30 segundos. Por exemplo:

Status: aberto na porta 19599

3. Anote o número da porta e forneça-o para Suporte.

Solução de problemas: problemas no Gateway de Arquivos

Você pode configurar seu gateway de arquivos para gravar entradas de registro em um grupo de CloudWatch registros da Amazon. Se fizer isso, você receberá notificações sobre o status de integridade do gateway e sobre erros encontrados pelo gateway. Você pode encontrar informações sobre essas notificações de erro e integridade nos CloudWatch Registros.

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

Erro: FileMissing

O erro `FileMissing` é semelhante ao `ObjectMissing` e as etapas para resolvê-lo são idênticas. Você pode receber um `FileMissing` erro quando um gravador diferente do File Gateway especificado exclui o arquivo especificado da Amazon FSx. Qualquer upload subsequente para a Amazon FSx ou recuperações do objeto na Amazon FSx falhará.

Para resolver um FileMissing erro

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB (você precisará dessa cópia de arquivo na etapa 3).
2. Exclua o arquivo do Gateway de Arquivos utilizando o cliente SMB.
3. Copie a versão mais recente do arquivo que você salvou na etapa 1 da Amazon FSx usando seu cliente SMB. Faça isso por meio do Gateway de Arquivos.

Erro: FsxFileSystemAuthenticationFailure

Você pode receber um erro `FsxFileSystemAuthenticationFailure` quando as credenciais fornecidas ao anexar o sistema de arquivos expirarem ou seus privilégios forem revogados.

Para resolver um FsxFileSystemAuthenticationFailure erro

1. Certifique-se de que as credenciais fornecidas no momento da anexação do sistema de FSx arquivos da Amazon ainda sejam válidas.
2. Certifique-se de que o usuário tenha todas as permissões necessárias, conforme descrito em Anexar um sistema de arquivos Amazon FSx para Windows File Server.

Erro: FsxFileSystemConnectionFailure

Você pode receber uma `FsxFileSystemConnectionFailure` mensagem de erro quando o FSx servidor da Amazon estiver inacessível a partir da máquina gateway.

Para resolver um FsxFileSystemConnectionFailure erro

1. Certifique-se de que todas as regras de firewall e VPC estejam permitindo a conexão entre a máquina gateway e o servidor Amazon FSx .
2. Certifique-se de que o FSx servidor da Amazon esteja em execução.

Erro: FsxFileSystemFull

Você pode receber uma `FsxFileSystemFull` mensagem de erro quando não há espaço livre em disco suficiente no sistema de FSx arquivos da Amazon.

Para resolver um FsxFileSystemFull erro

- Aumente o espaço de armazenamento para o sistema de FSx arquivos da Amazon.

Erro: GatewayClockOutOfSync

Você pode receber um `GatewayClockOutOfSync` erro quando o gateway detecta uma diferença de 5 minutos ou mais entre a hora do sistema local e a hora informada pelos servidores do AWS Storage Gateway. Problemas de sincronização do relógio podem afetar negativamente a conectividade entre o gateway e. AWS Se o relógio do gateway estiver fora de sincronia, poderão ocorrer erros de E/S nas conexões NFS e SMB, e os usuários SMB poderão enfrentar erros de autenticação.

Para resolver um GatewayClockOutOfSync erro

- Confira a configuração de rede entre o gateway e o servidor NTP. Para acessar mais informações sobre como sincronizar a hora da VM do gateway e atualizar a configuração do servidor NTP, consulte Configurar um servidor Network Time Protocol (NTP) para seu gateway.

Erro: InvalidFileState

Você pode receber um erro `InvalidFileState` quando um gravador diferente do gateway determinado modifica o arquivo especificado no compartilhamento de arquivos estabelecido. Como resultado, o estado do arquivo no gateway não corresponde ao estado na Amazon FSx. Qualquer upload ou recuperação subsequente do arquivo da Amazon FSx pode falhar.

Para resolver um InvalidFileState erro

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB (você precisará desse arquivo para cópia na etapa 4). Se a versão do arquivo na Amazon FSx for a mais recente, faça o download dessa versão. Você pode fazer isso acessando diretamente o FSx compartilhamento da Amazon usando qualquer cliente SMB.
2. Exclua o arquivo FSx diretamente na Amazon.
3. Exclua o arquivo do gateway utilizando o cliente SMB.
4. Usando seu cliente SMB, copie a versão mais recente do arquivo que você salvou na etapa 1, por meio do seu File Gateway, para a Amazon FSx.

Erro: ObjectMissing

Você pode receber um `ObjectMissing` erro quando um gravador diferente do File Gateway especificado exclui o arquivo especificado da Amazon FSx. Qualquer upload subsequente para a Amazon FSx ou recuperações do objeto na Amazon FSx falhará.

Para resolver um ObjectMissing erro

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB (você precisará dessa cópia de arquivo na etapa 3).
2. Exclua o arquivo do Gateway de Arquivos utilizando o cliente SMB.
3. Copie a versão mais recente do arquivo que você salvou na etapa 1 da Amazon FSx usando seu cliente SMB. Faça isso por meio do Gateway de Arquivos.

Erro: DroppedNotifications

Você pode ver um `DroppedNotifications` erro em vez de outros tipos esperados de entradas de CloudWatch registro quando o espaço livre de armazenamento no disco raiz do gateway for menor que 1 GB ou se mais de 100 notificações de saúde forem geradas em um intervalo de 1 minuto. Nessas circunstâncias, o gateway deixa de gerar notificações de CloudWatch log detalhadas como medida de precaução.

Para resolver um DroppedNotifications erro

1. Confira a métrica `Root Disk Usage` na guia Monitoramento do seu gateway no console do Storage Gateway para determinar se o espaço disponível no disco raiz está acabando.
2. Aumente o tamanho do disco de armazenamento raiz do gateway se o espaço disponível for menor que 1 GB. Consulte a documentação do hipervisor da sua máquina virtual para receber instruções.

   Para aumentar o tamanho do disco raiz dos gateways do Amazon EC2, consulte Solicitar modificações em seus volumes do EBS no Guia do usuário do Amazon Elastic Compute Cloud.

   > **Note**
   >
   > Não é possível aumentar o tamanho do disco raiz do Dispositivo de Hardware do AWS Storage Gateway.

3. Reinicie o gateway.

Notificação: HardReboot

Você pode receber uma notificação `HardReboot` quando a VM do gateway é reiniciada inesperadamente. Essa reinicialização pode ocorrer devido à falta de energia, à uma falha de hardware ou a outro evento. Para VMware gateways, uma redefinição do vSphere High Availability Application Monitoring pode causar esse evento.

Quando seu gateway é executado em tal ambiente, verifique a presença da `HealthCheckFailure` notificação e consulte o registro de VMware eventos da VM.

Notificação: Reinicializar

É possível obter uma notificação de reinicialização quando a VM do gateway é reiniciada. É possível reiniciar a VM de um gateway usando o console VM Hypervisor Management ou o console do Storage Gateway. Também é possível reiniciar usando o software de gateway durante o ciclo de manutenção do gateway.

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.

Solução de problemas: problemas no domínio do Active Directory

FSx O File Gateway não gera mensagens de log específicas para problemas de domínio do Active Directory. Se você tiver problemas para associar o gateway ao domínio do Active Directory, faça o seguinte:

- Verifique se o gateway não está tentando usar um controlador de domínio somente leitura (RODC) para ingressar no domínio.
- Verifique se o gateway está configurado para usar os servidores DNS corretos.

  Por exemplo, se você estiver tentando unir uma instância de gateway do Amazon EC2 a um Active Directory AWS gerenciado, verifique se a opção DHCP definida para sua VPC EC2 especifica os servidores DNS gerenciados do Active Directory. AWS

Os servidores DNS configurados por meio do conjunto de opções DHCP da VPC são fornecidos para todas as instâncias do EC2 na VPC. Se quiser especificar um servidor DNS para um gateway individual, você pode fazer isso usando o console local do EC2 desse gateway.

Em relação a gateways on-premises, você especifica um servidor DNS usando o console local da VM.

- Verifique a conectividade da rede do gateway executando os comandos a seguir no prompt de comando no console local do gateway. Substitua as variáveis destacadas pelo nome de domínio e endereços IP reais da sua implantação.

```
dig -d ExampleDomainName
ncport -d ExampleDomainControllerIPAddress -p 445
ncport -d ExampleDomainControllerIPAddress -p 389
```

- Verifique se sua conta de serviço do Active Directory tem as permissões necessárias. Para acessar mais informações, consulte Requisitos de permissão da conta de serviço do Active Directory.
- Verifique se o gateway se associa à unidade organizacional (UO) correta.

  A associação a um domínio criará uma conta de computador do Active Directory no contêiner de computadores padrão (que não é uma UO), usando o ID do gateway como nome da conta (por exemplo, SGW-1234ADE). Não é possível personalizar o nome dessa conta.

  Se seu ambiente do Active Directory tiver uma UO designada para novos objetos de computador, você deverá especificar essa UO ao ingressar no domínio.

  Se você encontrar erros de acesso negado ao tentar ingressar na UO designada, consulte o administrador do domínio do Active Directory. Talvez o administrador precise pré-preparar a conta do computador do gateway para que ele possa ingressar no domínio. Para acessar mais informações, consulte Como soluciono problemas ao associar meu Gateway de Arquivos do Storage Gateway a um domínio para autenticação do Microsoft Active Directory?.
- Verifique se o nome do host do seu gateway pode ser resolvido no DNS executando o comando a seguir no prompt de comando, no console local do gateway. Substitua a variável destacada pelo nome de host real do gateway.

```
dig -d ExampleHostName -r A
```

Se você configurou um nome de host personalizado para seu gateway, deverá adicionar manualmente um registro A de DNS que aponte para seu endereço IP.

- Verifique se a latência da rede entre o gateway e o controlador de domínio está razoavelmente baixa. A consulta para ingressar em um domínio poderá expirar se o gateway não receber uma resposta do controlador de domínio em 20 segundos.

  Se você unir o gateway ao domínio usando o comando JoinDomainCLI, poderá adicionar o `--timeout-in-seconds` sinalizador para aumentar o tempo limite para um máximo de 3.600 segundos.

- Confirme se o usuário do Active Directory que você está usando para associar o gateway ao domínio tem os privilégios necessários para isso.

Solução de problemas: usando CloudWatch métricas

A seguir, você pode encontrar informações sobre ações para resolver problemas usando as CloudWatch métricas da Amazon com o Storage Gateway.

Tópicos

O gateway reage lentamente quando você navega por diretórios

Se o File Gateway reagir lentamente quando você executa o ls comando ou navega pelos diretórios, verifique as métricas `IndexFetch` e `IndexEviction` CloudWatch :

- Se a `IndexFetch` métrica for maior que 0 quando você executa um `ls` comando ou navega pelos diretórios, seu gateway de arquivos começou sem informações sobre o conteúdo do diretório afetado e precisou acessar o S3 para Windows File Server. Os esforços subsequentes para listar o conteúdo desse diretório deverão ocorrer com mais rapidez.

- Se a métrica `IndexEviction` for 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 acessado há mais tempo para listar um novo diretório. Se isso ocorrer com frequência e houver um impacto no desempenho, entre em contato Suporte.

  Discuta com Suporte o conteúdo do sistema de FSx arquivos relacionado da Amazon e as recomendações para melhorar o desempenho com base no seu caso de uso.

O 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 em que a CPU fica ociosa quando há uma I/O solicitação 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 estar sendo limitado por um disco raiz lento à medida que ele recria o cache de índice para RAM. É possível resolver esse problema usando um disco físico mais rápido para o disco raiz.
- Caso a métrica `MemUsedBytes` seja igual ou quase igual à métrica `MemTotalBytes`, 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, pense em adicionar mais RAM ao Gateway de Arquivos com base na workload 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 no seu sistema de FSx arquivos da Amazon

Se você perceber que os arquivos no gateway não estão refletidos no sistema de FSx arquivos da Amazon, verifique a `FilesFailingUpload` métrica. Se a métrica informar que alguns arquivos estão falhando no upload, confira suas notificações de integridade. Quando não é feito upload dos arquivos, o gateway gera uma notificação de integridade que contém mais detalhes sobre o problema.

Você não vê snapshots mais antigos em seu sistema de FSx arquivos da Amazon

Algumas operações de FSx arquivo no File Gateway, como renomeações de pastas de nível superior ou alterações de permissão, podem resultar em várias operações de arquivo que causam uma alta I/O carga no sistema de arquivos do Windows File Server. FSx Se seu sistema de arquivos não tiver recursos de desempenho suficientes para sua carga de trabalho, o sistema de arquivos poderá excluir cópias paralelas porque prioriza a disponibilidade da cópia paralela contínua em I/O relação à retenção histórica de cópias paralelas.

No FSx console da Amazon, verifique a página de monitoramento e desempenho para ver se seu sistema de arquivos está subprovisionado. Se estiver, você poderá mudar para o armazenamento de SSD, aumentar a capacidade de throughput ou aumentar o IOPS da SSD para lidar com sua workload.

Seu gateway está lento ao transferir dados para a Amazon FSx

Se o seu File Gateway estiver demorando a transferir dados FSx para o Amazon for Windows File Server, faça o seguinte:

- Se a `CachePercentDirty` métrica for 80 ou maior, seu File Gateway está gravando dados em disco mais rápido do que pode fazer o upload dos dados FSx para o Amazon for Windows File Server. Considere aumentar a largura de banda para upload do seu gateway de arquivos, adicionar um ou mais discos de cache, reduzir a velocidade de gravação do cliente ou aumentar a capacidade de taxa de transferência do Amazon FSx for Windows File Server associado.
- Se a métrica `CachePercentDirty` estiver baixa, confira a métrica `IoWaitPercent`. Caso `IoWaitPercent` seja maior que 10, pode ser que o Gateway de Arquivos esteja sendo limitado pela velocidade do disco de cache local. Recomendamos discos locais de unidade de estado sólido (SSD) para seu cache, preferencialmente NVM Express (). NVMe Se esses discos não estiverem disponíveis, tente usar vários discos de cache de discos físicos separados para melhorar o desempenho.

O trabalho de backup do gateway falha ou há erros quando você grava no gateway

Se o trabalho de backup do Gateway de Arquivos falhar ou se houver erros quando você gravar nele, faça o seguinte:

- Se a métrica `CachePercentDirty` for 90% ou mais, o Gateway de Arquivos não poderá aceitar novas gravações em disco porque não há espaço disponível suficiente no disco de cache. Para

ver a rapidez com que seu gateway de arquivos está sendo carregado para o S3 para Windows File Server, veja `CloudBytesUploaded` a métrica. Compare essa métrica com a métrica `WriteBytes`, que mostra a rapidez com que o cliente está gravando arquivos no Gateway de Arquivos. Se o cliente SMB estiver gravando no seu gateway de arquivos mais rápido do que pode fazer o upload para o S3 para Windows File Server, adicione mais discos de cache para cobrir, no mínimo, o tamanho da tarefa de backup. Ou aumente a largura de banda de upload.

- Se a cópia de um arquivo grande, como um trabalho de backup falhar, mas a métrica `CachePercentDirty` for inferior a 80%, o Gateway de Arquivos poderá estar atingindo um tempo limite de sessão no lado do cliente. Para SMB, você pode aumentar esse tempo limite usando o PowerShell comando. `Set-SmbClientConfiguration -SessionTimeout 300` A execução desse comando define o tempo limite para 300 segundos.

Notificações de integridade de alta disponibilidade

Ao executar seu gateway na plataforma VMware vSphere High Availability (HA), você pode receber notificações de saúde. Para obter mais informações sobre notificações de integridade, consulte Solução de problemas: problemas de alta disponibilidade.

Solução de problemas: problemas de alta disponibilidade

Você pode encontrar informações a seguir sobre as ações que deverão ser executadas se tiver problemas de disponibilidade.

Tópicos

- Notificações de integridade
- Metrics

Notificações de integridade

Quando você executa seu gateway no VMware vSphere HA, todos os gateways produzem as seguintes notificações de saúde para seu grupo de log configurado da Amazon CloudWatch . Essas notificações entram em um fluxo de log chamado `AvailabilityMonitor`.

Tópicos

- Notificação: Reinicializar

Notificação: Reinicializar

É possível obter uma notificação de reinicialização quando a VM do gateway é reiniciada. É possível reiniciar a VM de um gateway usando o console VM Hypervisor Management ou o console do Storage Gateway. Também é possível reiniciar usando o software de gateway durante o ciclo de manutenção do gateway.

Medida a ser tomada

Se a hora da reinicialização estiver dentro de 10 minutos da hora de início da manutenção configurada do gateway, isso provavelmente será uma ocorrência normal e não um sinal de algum problema. Se a reinicialização ocorreu significativamente fora da janela de manutenção, verifique se o gateway foi reiniciado manualmente.

Notificação: HardReboot

Você pode receber uma notificação `HardReboot` quando a VM do gateway é reiniciada inesperadamente. Essa reinicialização pode ocorrer devido à falta de energia, à uma falha de hardware ou a outro evento. Para VMware gateways, uma redefinição do vSphere High Availability Application Monitoring pode causar esse evento.

Medida a ser tomada

Quando seu gateway é executado em tal ambiente, verifique a presença da `HealthCheckFailure` notificação e consulte o registro de VMware eventos da VM.

Notificação: HealthCheckFailure

Para um gateway no VMware vSphere HA, você pode receber uma `HealthCheckFailure` notificação quando uma verificação de integridade falhar e uma reinicialização da VM for 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**
>
> Essa notificação é somente para VMware gateways.

Medida a ser tomada

Se esse evento ocorrer repetidamente sem uma notificação `AvailabilityMonitorTest`, verifique se a infraestrutura da VM está com problemas (armazenamento, memória e assim por diante). Se precisar de assistência adicional, entre em contato com Suporte.

Notificação: AvailabilityMonitorTest

Para um gateway no VMware vSphere HA, você pode receber uma `AvailabilityMonitorTest` notificação ao executar um teste da disponibilidade e do sistema de monitoramento de aplicativos no. VMware

Metrics

A métrica `AvailabilityNotifications` está disponível em todos os gateways. Essa métrica é uma contagem do número de notificações de integridade relacionadas à disponibilidade geradas pelo gateway. Use a estatística `Sum` para observar se o gateway está enfrentando eventos relacionados à disponibilidade. Consulte seu grupo de CloudWatch registros configurado para obter detalhes sobre os eventos.

Práticas recomendadas para o Gateway de Arquivos

Esta seção contém os tópicos a seguir, que fornecem informações sobre as práticas recomendadas para trabalhar com gateways, compartilhamentos de arquivos, buckets e dados. Recomendamos que você se familiarize com as informações descritas nesta seção e tente seguir essas diretrizes para evitar problemas com o AWS Storage Gateway. Para obter orientação adicional sobre como diagnosticar e solucionar problemas comuns que você pode encontrar com sua implantação, consulte Solucionar problemas com a implantação do Storage Gateway.

Tópicos

Práticas recomendadas para a recuperação de 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 imagem de máquina da Amazon (AMI) do Amazon EC2. Se a VM do gateway apresentar problemas, ative um novo gateway e recupere seus dados para esse gateway usando as instruções a seguir.

Como se recuperar de um caso de encerramento inesperado da máquina virtual

Se sua VM encerrar-se inesperadamente – por exemplo, durante uma queda de energia –, seu gateway ficará inacessível. Quando a energia e a conectividade de rede são restauradas, o gateway fica novamente acessível e começa a funcionar normalmente. Veja a seguir algumas medidas que você pode tomar em momentos como esse para ajudar a recuperar os dados:

- Se uma interrupção provocar problemas de conectividade de rede, é possível solucionar esse problema. Para obter informações sobre como testar a conectividade de rede, consulte Como testar a conectividade de rede do gateway.

Como recuperar seus dados de um disco de cache com falha

Se seu disco de cache encontrar uma falha, é recomendável usar as etapas a seguir para recuperar seus dados, de acordo com sua situação:

- Se a falha ocorreu porque um disco de cache foi removido do host, desligue o gateway, adicione novamente o disco e reinicie o gateway.

Como recuperar seus dados de um datacenter inacessível

Se o gateway ou datacenter ficar inacessível por algum motivo, é possível recuperar seus dados em um outro gateway em outro datacenter ou recuperar um gateway hospedado em uma instância do Amazon EC2. Se você não tiver acesso a outro datacenter, recomendamos criar o gateway em uma instância do Amazon EC2. As etapas que você segue dependem do tipo de gateway cujos dados você está cobrindo.

Como recuperar dados de um Gateway de Arquivos em um data center inacessível

Para o File Gateway, você mapeia um novo sistema de arquivos de de arquivos para o para Windows File Server que contém os dados que você deseja recuperar.

1. Crie e ative um Gateway de Arquivos em um host do Amazon EC2. Para obter mais informações, consulte Implante um host padrão do Amazon EC2 para FSx o File Gateway.
2. Crie um sistema de arquivos no gateway do EC2 que você criou. Para obter mais informações, consulte Criar um sistema de arquivos FSx para Windows File Server.
3. Monte seu sistema de arquivos de de arquivos em seu cliente e mapeie-o para o para Windows File Server que contém os dados que você deseja recuperar. Para obter mais informações, consulte Montar e usar um compartilhamento de arquivos.

Restauração a partir de backups ou snapshots diretamente na Amazon FSx

Em alguns casos, talvez seja necessário restaurar dados diretamente no sistema de FSx arquivos da Amazon, usando um backup ou um snapshot de um momento anterior. Nesses casos, existe o risco de criar um cenário de gravação dupla entre o aplicativo de backup e o FSx File Gateway, o que pode resultar em arquivos bloqueados ou incompatíveis. Para evitar problemas ao restaurar seu sistema de FSx arquivos da Amazon a partir de backups ou snapshots, use o procedimento a seguir.

> **Note**
>
> Todos os dados em cache atualmente armazenados no seu FSx File Gateway não serão válidos depois que você restaurar o sistema de FSx arquivos da Amazon a partir de um backup ou snapshot usando este procedimento.

Para evitar problemas ao restaurar seu sistema de FSx arquivos da Amazon a partir de backups ou snapshots

1. Separe o sistema de FSx arquivos da Amazon do FSx File Gateway usando o console do Storage Gateway.
2. Restaure o backup ou o snapshot diretamente no seu sistema de FSx arquivos da Amazon.
3. Reconecte o sistema de FSx arquivos da Amazon ao FSx File Gateway usando o console do Storage Gateway.

Limpar recursos desnecessários

Como prática recomendada, indicamos limpar os recursos do Storage Gateway para evitar alterações inesperadas ou desnecessárias. Por exemplo, se você criou um gateway como um exercício de demonstração ou teste, pense em excluí-lo, bem como o dispositivo virtual da sua implantação. Use o procedimento a seguir para limpar recursos.

Para limpar os recursos dos quais você não necessita

1. Se você não planeja mais continuar usando um gateway, exclua-o. Para obter mais informações, consulte Como excluir o gateway e remover recursos associados.

2. Exclua a VM do Storage Gateway do host on-premises. Se tiver criado seu gateway em uma instância do Amazon EC2, encerre a instância.

Recursos adicionais do Storage Gateway

Esta seção contém os seguintes tópicos, que fornecem informações e recursos adicionais relacionados à configuração e ao uso do AWS Storage Gateway:

Tópicos

- Configuração do host: saiba como implantar e configurar um host de máquina virtual para o gateway.
- Usando o Storage Gateway com VMware HA- Saiba como configurar o Storage Gateway para trabalhar com os recursos de alta disponibilidade do VMware vSphere.
- Obter a chave de ativação: saiba onde encontrar a chave de ativação que você precisa fornecer ao implantar um novo gateway.
- Usando Direct Connect: aprenda a criar uma conexão de rede dedicada entre o gateway on-premises e a Nuvem AWS .
- Permissões do Active Directory: saiba quais permissões a conta de serviço deve ter para poder unir o gateway ao domínio do Active Directory.
- Como obter o endereço IP do dispositivo de gateway: saiba onde encontrar o endereço IP do host da máquina virtual do gateway, que você precisa fornecer ao implantar um novo gateway.
- Entendendo os recursos e os recursos IDs- Saiba como AWS identifica os recursos e sub-recursos criados pelo Storage Gateway.
- Marcar recursos: aprenda a usar tags de metadados para categorizar recursos e torná-los mais fáceis de gerenciar.
- Componentes de código aberto: conheça as ferramentas e licenças de terceiros usadas para oferecer a funcionalidade do Gateway de Volumes.
- Cotas: saiba mais sobre limites e cotas para o Gateway de Arquivos, incluindo limitações mínimas e máximas para compartilhamentos de arquivos e discos de cache local.

Como implantar e configurar o host da VM do gateway

Os tópicos a seguir fornecem informações sobre como configurar a plataforma host de máquina virtual para um gateway.

Tópicos

- Implante um host padrão do Amazon EC2 para FSx o File Gateway

- Implante um host Amazon EC2 personalizado para FSx o File Gateway
- Modificar as opções de metadados da instância do Amazon EC2
- Sincronizar o horário da VM com o horário do host Hyper-V ou Linux KVM
- Sincronize o horário da VM com VMware o horário do host
- Como configurar adaptadores de rede para o gateway
- Usando o VMware vSphere High Availability com Storage Gateway

Implante um host padrão do Amazon EC2 para FSx o File Gateway

Este tópico lista as etapas para implantar um host Amazon EC2 usando as especificações padrão.

Você pode implantar e ativar um Gateway) em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). A Imagem de máquina da Amazon (AMI) do AWS Storage Gateway está disponível como uma AMI de comunidade.

> **Note**
>
> A comunidade Storage Gateway AMIs é publicada e totalmente apoiada pela AWS. Você pode ver que o editor é AWS um provedor verificado.

1. Para configurar a instância do Amazon EC2, escolha Amazon EC2 como Plataforma host na seção Opções da plataforma do fluxo de trabalho. Para obter instruções sobre como configurar a instância do Amazon EC2, . FSx
2. Selecione Launch instance para abrir o modelo de AWS Storage Gateway AMI no console do Amazon EC2 e personalizar configurações adicionais, como tipos de instância, configurações de rede e Configurar armazenamento.
3. Opcionalmente, é possível selecionar Usar configurações padrão no console do Storage Gateway para implantar uma instância do Amazon EC2 com a configuração padrão.

   A instância do Amazon EC2 criada por Usar configurações padrão tem as seguintes especificações padrão:

   - Tipo de instância: m5.xlarge
   - Configurações de rede
     - Em VPC, selecione a VPC na qual você deseja que sua instância do EC2 seja executada.

- Em Sub-rede, especifique a sub-rede na qual sua instância do EC2 deve ser executada.

> **Note**
>
> As sub-redes da VPC aparecerão na lista suspensa somente se tiverem a configuração de atribuição automática de endereço IP público ativada no console de gerenciamento da VPC.

- Atribuição automática de IP público: ativada
- Um grupo de segurança do EC2 é criado e associado à instância do EC2. O grupo de segurança tem as seguintes regras de porta de entrada:

> **Note**
>
> Será preciso ter a porta 80 aberta durante a ativação do gateway. A porta é fechada imediatamente após a ativação. Depois disso, sua instância do EC2 só pode ser acessada pelas outras portas da VPC selecionada.
> Os compartilhamentos de arquivos em seu gateway só podem ser acessados por meio dos hosts na mesma VPC que o gateway. Se os compartilhamentos de arquivos precisarem ser acessados de hosts fora da VPC, você deverá atualizar as regras de grupo de segurança adequadas.
> É possível editar grupos de segurança a qualquer momento navegando até a página de detalhes da instância do Amazon EC2, selecionando Segurança, navegando até Detalhes do grupo de segurança e escolhendo o ID do grupo de segurança.

Porta	Protocolo	Protocolo do sistema de arquivos				
80	TCP	Acesso HTTP para ativação				
137	UDP	NetBIOS				
138	UDP	NetBIOS				
139	TCP e UDP	SMB				
389	TCP	LDAP				
445	TCP	SMB				

- Configurar armazenamento

Configurações padrão	Volume do dispositivo raiz da AMI	Cache do volume 2				
Nome do dispositivo		'/dev/sdb'				
Tamanho	80 GiB	165 GiB				
Tipo de volume	gp3	gp3				

Configurações padrão	Volume do dispositivo raiz da AMI	Cache do volume 2				
IOPS	3000	3000				
Excluir no encerramento	Sim	Sim				
Encriptado	Não	Não				
Throughput	125	125				

Implante um host Amazon EC2 personalizado para FSx o File Gateway

Você pode implantar e ativar um Gateway) em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). A Imagem de máquina da Amazon (AMI) do AWS Storage Gateway está disponível como uma AMI de comunidade.

> **Note**
>
> A comunidade Storage Gateway AMIs é publicada e totalmente apoiada pela AWS. Você pode ver que o editor é AWS um provedor verificado.
> File Gateway AMIs usa a seguinte convenção de nomenclatura. O número da versão anexado ao nome da AMI muda a cada lançamento da versão.
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

Para implantar uma instância do Amazon EC2 para hospedar seu Amazon FSx File Gateway

1. Comece a conectar um novo gateway de fitas usando o console do Storage Gateway. Para obter instruções, consulte Configurar um Amazon FSx File Gateway. Ao chegar à seção Opções

de plataforma, escolha o Amazon EC2 como Plataforma host e use as etapas a seguir para inicializar a instância do Amazon EC2 que hospedará o Gateway de Arquivos.

2. Escolha Launch instance para abrir o modelo de AWS Storage Gateway AMI no console do Amazon EC2, onde você pode definir configurações adicionais.

   Use o Quicklaunch para iniciar a instância do Amazon EC2 com as configurações padrão. Para obter mais informações sobre as especificações padrão de início rápido do Amazon EC2, consulte Especificações de configuração de início rápido para o Amazon EC2.

3. Em Nome, insira um nome para a instância do Amazon EC2. Depois que a instância for implantada, será possível pesquisar esse nome para encontrar sua instância nas páginas de lista no console do Amazon EC2.

4. Em Tipo de instância, na lista Tipo de instância, escolha a configuração de hardware para a instância. A configuração do hardware deve atender a determinados requisitos mínimos para ser compatível com o gateway. É recomendável começar com o tipo de instância m5.xlarge, que atende aos requisitos mínimos de hardware para o gateway funcionar corretamente. Para obter mais informações, consulte Requisitos para tipos de instância do Amazon EC2.

   Você pode redimensionar sua instância depois de executá-la, se necessário. Para obter mais informações, consulte Resizing your instance no Guia do usuário do Amazon EC2.

   > **Note**
   >
   > Alguns tipos de instância, especialmente i3 EC2, usam discos NVMe SSD. Isso pode gerar problemas quando você inicia ou interrompe o Gateway de Arquivos. Por exemplo, você pode perder dados do cache. Monitore a CloudWatch métrica da `CachePercentDirty` Amazon e inicie ou pare seu sistema somente quando esse parâmetro for`0`. Para saber mais sobre as métricas de monitoramento do seu gateway, consulte as métricas e dimensões do Storage Gateway na CloudWatch documentação.

5. Na seção Par de chaves (login), em Nome do par de chaves - obrigatório, selecione o par de chaves que você deseja usar para se conectar à sua instância com segurança. Se necessário, é possível criar um novo par de chaves. Para ter mais informações, consulte Criar um par de chaves no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

6. Na seção Configurações de rede, revise as configurações pré-definidas e escolha Editar para fazer alterações nos seguintes campos:

a. Em VPC - obrigatório, escolha a VPC em que você deseja iniciar sua instância do Amazon EC2. Para receber mais informações, consulte Como funciona a Amazon VPC no Guia do usuário do Amazon Virtual Private Cloud.

b. (Opcional) Em Sub-rede, escolha a sub-rede em que você deseja iniciar sua instância do Amazon EC2.

c. Para Auto-assign Public IP (Atribuir IP público automaticamente), selecione Permitir.

7. Na subseção Firewall (grupos de segurança), revise as configurações pré-definidas. É possível alterar o nome padrão e a descrição do novo grupo de segurança a ser criado para sua instância do Amazon EC2, se quiser, ou optar por aplicar regras de firewall de um grupo de segurança existente.

8. Na subseção Regras de grupos de segurança de entrada, adicione regras de firewall para abrir as portas que os clientes usarão para se conectar à sua instância. Para obter mais informações sobre as portas necessárias para o Gateway), consulte de porta. Para obter mais informações sobre regras de firewall, consulte Regras de grupo de segurança no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

> **Note**
>
> O Amazon FSx File Gateway exige que a porta TCP 80 esteja aberta para tráfego de entrada e acesso HTTP único durante a ativação do gateway. Após a ativação, será possível fechar essa porta.
> Além disso, você deve abrir a porta TCP 445 para acesso SMB, a porta UDP 137 para acesso NetBIOS, a porta UDP 138 para acesso NetBIOS e a porta TCP 389 para acesso LDAP.

9. Na subseção Configuração de rede avançada, revise as configurações pré-definidas e faça alterações, se necessário.

10. Na seção Configurar armazenamento, escolha Adicionar novo volume para adicionar armazenamento à instância do gateway.

> **Important**
>
> Você deve adicionar pelo menos um volume do Amazon EBS com pelo menos 150 GiB de capacidade para o armazenamento em cache além do Volume raiz pré-configurado.

Para aumentar o desempenho, recomendamos alocar vários volumes do EBS para armazenamento em cache com pelo menos 150 GiB cada.

11. Na seção Detalhes avançados, revise as configurações pré-definidas e faça alterações, se necessário.
12. Escolha Iniciar instância para iniciar a nova instância de gateway do Amazon EC2 com as configurações definidas.
13. Para verificar se sua nova instância foi executada com sucesso, navegue até a página Instâncias no console do Amazon EC2 e pesquise a nova instância pelo nome. Certifique-se de que o estado da instância exiba Executando com uma marca de seleção verde e que a verificação de status esteja concluída e mostre uma marca de seleção verde.
14. Selecione sua instância na página de detalhes. Copie o endereço IP público da seção Resumo da instância e, em seguida, retorne à página Configurar gateway no console do Storage Gateway para continuar a configuração do Gateway).

Você pode determinar o ID da AMI a ser usado para iniciar um gateway de arquivos usando o console do Storage Gateway ou consultando o repositório de AWS Systems Manager parâmetros.

Para determinar o ID da AMI, execute uma das seguintes ações:

- Comece a conectar um novo gateway de fitas usando o console do Storage Gateway. Para obter instruções, consulte Configurar um Amazon FSx File Gateway. Ao chegar à seção Opções de plataforma, escolha Amazon EC2 como plataforma Host e, em seguida, escolha Launch instance para abrir o modelo de AWS Storage Gateway AMI no console do Amazon EC2.

  Você é redirecionado para a página da AMI da comunidade EC2, onde pode ver o ID da AMI AWS da sua região na URL.

- Consulte o repositório de parâmetros do Systems Manager. Você pode usar a API AWS CLI ou Storage Gateway para consultar o parâmetro público do Systems Manager no namespace `/aws/service/storagegateway/ami/FILE_FSX_SMB/latest`. Por exemplo, o uso do comando CLI a seguir retorna o ID da AMI atual no Região da AWS que você especificar.

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  FILE_FSX_SMB/latest
  ```

  O comando da CLI retorna uma saída semelhante à seguinte:

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 18,
         "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_FSX_SMB/latest",
         "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
        "Value": "ami-033d1edba5606cffb"
    }
}
```

Modificar as opções de metadados da instância do Amazon EC2

O serviço de metadados de instância (IMDS) é um componente na instância que oferece acesso seguro a metadados da instância do Amazon EC2. Uma instância pode ser configurada para aceitar solicitações de metadados recebidas que usam o IMDS versão 1 (IMDSv1) ou exigir que todas as solicitações de metadados usem o IMDS versão 2 (). IMDSv2 IMDSv2 usa solicitações orientadas à sessão e mitiga vários tipos de vulnerabilidades que poderiam ser usadas para tentar acessar o IMDS. Para obter informações sobre IMDSv2, consulte Como o Instance Metadata Service versão 2 funciona no Amazon Elastic Compute Cloud User Guide.

Recomendamos que você exija o IMDSv2 para todas as instâncias do Amazon EC2 que hospedam o Storage Gateway. IMDSv2 é exigido por padrão em todas as instâncias de gateway recém-lançadas. Se você tiver instâncias existentes que ainda estão configuradas para aceitar solicitações de IMDSv1 metadados, consulte Exigir o uso de IMDSv2 no Guia do usuário do Amazon Elastic Compute Cloud para obter instruções sobre como modificar as opções de metadados de sua instância para exigir o uso de. IMDSv2 A aplicação dessa alteração não exige a reinicialização da instância.

Sincronizar o horário da VM com o horário do host Hyper-V ou Linux KVM

Para um gateway implantado em VMware ESXi, definir a hora do host do hipervisor e sincronizar a hora da máquina virtual com o host é suficiente para evitar o desvio de tempo. Para obter mais informações, consulte Sincronize o horário da VM com VMware o horário do host. Para um gateway implantado no Microsoft Hyper-V ou Linux KVM, recomendamos que você verifique periodicamente o tempo da máquina virtual usando o procedimento descrito a seguir.

Como exibir e sincronizar o tempo de uma máquina virtual do gateway do hipervisor para um servidor de Network Time Protocol (NTP)

1. Faça login no console local do seu gateway:
   - 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 máquina virtual baseada em kernel (KVM), consulte Acessar o console local do gateway com o Linux KVM.
2. Na tela do menu principal Configuração do Storage Gateway, insira o número correspondente para selecionar Gerenciamento de tempo do sistema.
3. No menu Gerenciamento do tempo do sistema, insira o número correspondente para selecionar Visualizar e sincronizar o tempo do sistema.

   O console local do gateway exibe a hora atual do sistema e a compara com a hora relatada pelo servidor de NTP e, em seguida, relata a discrepância exata entre as duas vezes em segundos.
4. Se a discrepância de tempo for maior que 60 segundos, digite **y** para sincronizar a hora do sistema com a hora do NTP. Caso contrário, digite **n**.

   A sincronização do horário pode demorar alguns instantes.

Sincronize o horário da VM com VMware o horário 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, clique com o botão direito do mouse no nome da sua VM de gateway no painel no lado esquerdo da janela da aplicação para abrir o menu de contexto da VM e escolha Editar configurações.

   A caixa de diálogo Virtual Machine Properties é aberta.

b. Escolha a guia Opções e, em seguida, escolha VMware Ferramentas na lista de opções.

c. Marque a opção Sincronizar horário de acesso com o host na seção Avançado no lado direito da caixa de diálogo Propriedades da máquina virtual 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 host do vSphere no painel esquerdo e, em seguida, escolha a guia Configuração.

   b. Selecione Time Configuration no painel Software e escolha o link Properties.

      A caixa de diálogo Time Configuration é exibida.

   c. Em Data e hora, defina a data e a hora do host vSphere.

   d. Configure o host para sincronizar seu tempo automaticamente com um servidor NTP.

      i. Escolha Opções na caixa de diálogo Configuração de tempo e, na caixa de diálogo Opções de daemon NTP (ntpd), escolha Configurações de NTP 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` como nome de domínio.

      iv. Na caixa de diálogo Opções de NTP Daemon (ntpd), escolha Geral, no painel esquerdo.

      v. No painel Comandos de serviço, escolha Iniciar 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 configurar adaptadores de rede para o gateway

O Storage Gateway usa um único adaptador de rede VMXNET3 (10 GbE) por padrão, mas você pode configurar seu gateway para usar mais de um adaptador de rede para que ele possa ser acessado por vários endereços IP. Talvez você queira fazer isso nas seguintes situações:

- Maximizar o throughput: você pode maximizar o throughput de um gateway quando os adaptadores de rede forem um gargalo.
- Separação de aplicações: talvez seja necessário distinguir o modo como suas aplicações gravam nos volumes de um gateway. Por exemplo, você pode determinar que um aplicativo de armazenamento essencial use exclusivamente um adaptador específico definido para o gateway.
- Restrições de rede: seu ambiente de aplicações pode exigir que você mantenha os compartilhamentos de arquivos e os iniciadores que se conectam a eles em uma rede separada. Essa rede é diferente daquela por meio da qual o gateway se comunica com a AWS.

Em um caso de uso típico de vários adaptadores, um adaptador é configurado como a rota pela qual o gateway se comunica AWS (ou seja, como o gateway padrão). Exceto esse adaptador específico, os iniciadores devem estar na mesma sub-rede que o adaptador que contém os compartilhamentos de arquivos aos quais eles se conectam. Do contrário, a comunicação com os destinos pode não ser possível. Se um destino estiver configurado no mesmo adaptador usado para comunicação com AWS, o tráfego de compartilhamento de arquivos desse destino e o AWS tráfego fluirão pelo mesmo adaptador.

Em alguns casos, você pode configurar um adaptador para se conectar ao console do Storage Gateway, depois adicionar um segundo adaptador. Nesse caso, o Storage Gateway configura automaticamente a tabela de rotas para usar o segundo adaptador como rota preferida. Para conferir instruções sobre como configurar vários adaptadores, consulte os seguintes tópicos:

Tópicos

- Configurando seu gateway para vários NICs em um host VMware ESXi
- Configurando seu gateway para vários NICs no Microsoft Hyper-V Host

Configurando seu gateway para vários NICs em um host VMware ESXi

O procedimento a seguir pressupõe que sua VM de gateway já tenha um adaptador de rede definido e descreve como adicionar um adaptador. VMware ESXi

Para configurar seu gateway para usar um adaptador de rede adicional no VMware ESXi host

1. Encerre o gateway.
2. No cliente VMware vSphere, selecione sua VM de 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.

      Recomendamos que você use o adaptador de VMXNET3 rede com o Storage Gateway. Para obter mais informações sobre os tipos de adaptadores que podem aparecer na lista de adaptadores, consulte Tipos de adaptadores de rede ESXi e a documentação do vCenter Server.

   c. No painel Pronto para Completar, reveja as informações e escolha Terminar.
6. Escolha a guia Resumo da VM e escolha Visualizar tudo, ao lado da caixa Endereço IP. A janela Endereços IP da Máquina Virtual exibe todos os endereços IP que podem ser usados para acessar o gateway. Confirme se um segundo endereço IP é listado para o gateway.

   > **Note**
   >
   > Pode demorar vários minutos para as alterações do adaptador entrarem em vigor e as informações resumidas da VM atualizarem.
7. No console do Storage Gateway, ative o gateway.

8. No painel Navegação do console do Storage Gateway, escolha Gateways e o gateway ao qual você adicionou o adaptador. Confirme se o segundo endereço IP está listado na guia Details.

Para obter informações sobre tarefas do console local comuns aos VMware hosts Hyper-V e KVM, consulte Realizar tarefas no console local da máquina virtual

Configurando seu gateway para vários NICs no Microsoft Hyper-V Host

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 de gateway no painel Máquinas virtuais.
3. Se a VM do gateway ainda não estiver desativada, clique com o botão direito do mouse no nome da VM para abrir o menu de contexto e escolha Desativar.
4. Clique com o botão direito do mouse no nome da VM de gateway para abrir o menu de contexto e escolha Configurações.
5. Na caixa de diálogo Configurações, em Hardware, escolha Adicionar hardware.
6. No painel Adicionar hardware no lado direito da caixa de diálogo Configurações, escolha Adaptador de rede e selecione Adicionar para adicionar um dispositivo.
7. Configure o adaptador de rede e escolha Apply para aplicar as configurações.
8. Na caixa de diálogo Configurações, para Hardware, confirme se o novo adaptador foi adicionado à lista de hardware e escolha OK.
9. Ative o gateway usando o console do Storage Gateway.
10. No painel Navegação do console do Storage Gateway, escolha Gateways e o gateway ao qual você adicionou o adaptador. Confirme se o segundo endereço IP está listado na guia Detalhes.

Para obter informações sobre tarefas do console local comuns aos VMware hosts Hyper-V e KVM, consulte Realizar tarefas no console local da máquina virtual

Usando o VMware vSphere High Availability com Storage Gateway

O Storage Gateway fornece alta disponibilidade VMware por meio de um conjunto de verificações de integridade em nível de aplicativo integradas ao VMware vSphere High Availability (HA). VMware 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 VMware ambiente local ou em um VMware Cloud on se recupera AWS automaticamente da maioria das interrupções de serviço. Ele geralmente faz isso em menos de 60 segundos sem perda de dados.

> **Note**
>
> Recomendamos fazer o seguinte se você implantar o Storage Gateway em um cluster VMware de alta disponibilidade:
>
> - Implante o pacote VMware ESX .ova disponível para download que contém a VM do Storage Gateway em apenas um host em um cluster.
> - Quando você 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 você implantar o pacote .ova para o cluster, selecione um host quando solicitado. Outra opção é implantá-lo diretamente no host de um cluster.

Os tópicos a seguir descrevem como implantar o Storage Gateway em um cluster VMware de alta disponibilidade:

Tópicos

- Teste sua configuração VMware de alta disponibilidade

Configure seu cluster vSphere HA VMware

Primeiro, se você ainda não criou um VMware cluster, crie um. Para obter informações sobre como criar um VMware cluster, consulte Criar um cluster vSphere HA na VMware documentação.

Em seguida, configure seu VMware cluster para funcionar com o Storage Gateway.

Para configurar seu VMware cluster

1. Na página Editar configurações de cluster no VMware vSphere, certifique-se de que o monitoramento de VM esteja configurado para monitoramento de VM e aplicativo. Para isso, defina os seguintes valores para cada opção:

   - Resposta de falha do host: reiniciar VMs
   - Resposta para isolamento do host: desligue e reinicie VMs
   - Datastore with PDL (Armazenamento de dados com PDL): Disabled (Desativado)
   - Datastore with APD (Armazenamento de dados com APD): Disabled (Desativado)
   - VM Monitoring (Monitoramento de VM): VM and Application Monitoring (Monitoramento de VM e aplicativos)
2. Ajuste a sensibilidade do cluster ajustando os seguintes valores:

   - Intervalo de falha: após esse intervalo, a VM será reiniciada se uma pulsação da VM não for recebida.
   - Tempo mínimo de atividade: o cluster aguarda esse tempo depois que uma VM começa a monitorar as pulsações das ferramentas de VM.
   - Redefinições máximas por VM: define o máximo de vezes que o cluster reinicia a VM durante a janela temporal para o máximo de redefinições.
   - Janela de tempo de redefinições máximas: a janela de tempo na qual ocorre a contagem de redefinições máximas por VM.

   Se você não tiver certeza de quais valores definir, use estas configurações de exemplo:

   - Failure interval (Intervalo de falha): **30** segundos
   - Minimum uptime (Tempo mínimo de atividade): **120** segundos

- Maximum per-VM resets (Máximo de redefinições por VM): **3**
- Maximum resets time window (Janela temporal para o máximo de redefinições): **1** hora

Se você tiver outros em VMs execução no cluster, talvez 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) Adicione opções de substituição para outras VMs em seu cluster.

Configurar o tipo de gateway

Use o procedimento a seguir para configurar o gateway.

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 — Crie e ative um Amazon FSx File Gateway

Implantar o gateway

No cluster configurado, implante a imagem .ova em um dos hosts do cluster. Para obter instruções, consulte Implantar um modelo OVF ou OVA na documentação on-line do VMware vSphere.

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) Adicione opções de substituição para outras VMs em seu cluster

Se você tiver outros em VMs execução no seu cluster, talvez queira definir os valores do cluster especificamente para cada VM. Para obter instruções, consulte Personalizar uma máquina virtual individual na documentação on-line do VMware vSphere.

Para adicionar opções de substituição para outras VMs em seu cluster

1. Na página Resumo do VMware vSphere, escolha seu cluster para abrir a página do cluster e, em seguida, escolha 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.

   Defina os seguintes valores para cada opção em vSphere HA - Monitoramento de VM:

   - Monitoramento de VM: substituição habilitada - Monitoramento de VM e aplicações
   - Sensibilidade de monitoramento de VM: Substituição habilitada - Monitoramento de VMs e aplicações
   - Monitoramento de VM: Personalizar
   - Intervalo de falha: **30** segundos
   - Tempo mínimo de atividade: **120** segundos
   - Maximum per-VM resets (Máximo de redefinições por VM): **5**
   - Janela máxima de tempo de reinicialização: em **1** hora

Ativar o gateway.

Depois que o .ova for implantado em seu VMware ambiente, ative seu gateway usando o console do Storage Gateway. Para obter instruções, consulte Review e ative o Amazon FSx File Gateway.

Teste sua configuração VMware de alta disponibilidade

Depois de ativar o gateway, teste a configuração.

Para testar sua configuração de VMware HA

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, escolha Gateways e, em seguida, escolha o gateway que você deseja testar para VMware HA.
3. Em Ações, escolha Verificar VMware HA.
4. Na caixa Verificar configuração de VMware alta disponibilidade exibida, escolha OK.

> **Note**
>
> O teste VMware da configuração de 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 de VMware HA nos grupos de CloudWatch registros da Amazon. Para obter mais informações, consulte Obtendo registros de integridade do File Gateway com grupos CloudWatch de registros.

Como obter a chave de ativação para o gateway

Para receber uma chave de ativação para seu gateway, faça uma solicitação pela web para a máquina virtual (VM) do gateway. A VM retorna um redirecionamento que contém a chave de ativação, que é passada como um dos parâmetros da ação `ActivateGateway` da API para especificar a configuração do seu gateway. Para obter mais informações, consulte ActivateGatewayna Referência da API do Storage Gateway.

> **Note**
>
> Se não forem usadas, as chaves de ativação do gateway expiram em 30 minutos.

A solicitação que você faz à VM do gateway inclui a AWS região em que a ativação ocorre. O URL que é retornado pelo redirecionamento na resposta contém um parâmetro de string de consulta denominado `activationkey`. Esse parâmetro de string de consulta é a sua chave de ativação. O formato da string de consulta é semelhante ao seguinte: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. A saída dessa consulta retorna a região de ativação e a chave.

O URL também inclui `vpcEndpoint` o ID do endpoint da VPC para gateways que se conectam usando o tipo de endpoint da VPC.

> **Note**
>
> O AWS Storage Gateway Hardware Appliance, os modelos de imagem de VM e as Amazon Machine Images (AMI) do Amazon EC2 vêm pré-configurados com os serviços HTTP

necessários para receber e responder às solicitações da web descritas nesta página. Não é necessário nem recomendado instalar nenhum serviço adicional em seu gateway.

Tópicos

- Linux (curl)
- Linux (bash/zsh)
- Microsoft Windows PowerShell
- Como usar seu console local

Linux (curl)

Os exemplos a seguir mostram como obter uma chave de ativação com o Linux (curl).

> **Note**
>
> Substitua as variáveis destacadas por valores reais para o gateway. Os valores aceitáveis são os seguintes:
>
> - *`gateway_ip_address`*- O IPv4 endereço do seu gateway, por exemplo `172.31.29.201`
> - *`gateway_type`*- O tipo de gateway que você deseja ativar, como `STOREDCACHED`,`VTL`,`FILE_S3`, ou`FILE_FSX_SMB`.
> - *`region_code`*- A região em que você deseja ativar seu gateway. Consulte os endpoints regionais no Guia de referência geral da AWS . Se esse parâmetro não for especificado ou se o valor fornecido estiver escrito incorretamente ou não corresponder a uma região válida, o comando usará a região `us-east-1` como padrão.
> - *`vpc_endpoint`*- O nome do VPC endpoint do seu gateway, por exemplo. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Para obter a chave de ativação de um endpoint público:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Para obter a chave de ativação de um endpoint da VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

O exemplo a seguir mostra como usar o Linux (bash/zsh) para buscar a resposta HTTP, analisar cabeçalhos HTTP e obter a chave de ativação.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

O exemplo a seguir mostra como usar o Microsoft Windows PowerShell para buscar a resposta HTTP, analisar cabeçalhos HTTP e obter a chave de ativação.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
```

```
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Como usar seu console local

O exemplo a seguir mostra como usar o console local para gerar e exibir uma chave de ativação.

Para obter uma chave de ativação para o gateway do seu console local

1. Faça login no console local como admin.
2. Depois de fazer login e ver o menu principal de Ativação de dispositivos da AWS : configuração, selecione `0` para escolher Obter chave de ativação.
3. Selecione Storage Gateway para a opção da família de gateways.
4. Quando solicitado, insira o Região da AWS local em que você deseja ativar seu gateway.
5. Insira 1 para pública ou 2 para um endpoint da VPC como o tipo de rede.
6. Insira 1 para padrão ou 2 para FIPS (Padrões Federais de Processamento de Informações) como o tipo de endpoint.

Usando Direct Connect com o Storage Gateway

Direct Connect vincula sua rede interna à Amazon Web Services Cloud. Ao usar Direct Connect com o Storage Gateway, você pode criar uma conexão para necessidades de carga de trabalho de alto rendimento, fornecendo uma conexão de rede dedicada entre seu gateway local e. AWS

O Storage Gateway usa endpoints públicos. Com uma Direct Connect conexão estabelecida, você pode criar uma interface virtual pública para permitir que o tráfego seja roteado para os endpoints do Storage Gateway. A interface virtual pública evita os provedores de serviço de Internet do caminho da sua rede. O endpoint público do serviço Storage Gateway pode estar na mesma AWS região do Direct Connect local ou em uma AWS região diferente.

A ilustração a seguir mostra um exemplo de como Direct Connect funciona com o Storage Gateway. arquitetura de rede mostrando o Storage Gateway conectado à nuvem usando conexão AWS direta.

O procedimento a seguir pressupõe que você tenha criado um gateway operacional.

Para usar Direct Connect com o Storage Gateway

1. Crie e estabeleça uma AWS Direct Connect conexão entre seu data center local e seu endpoint do Storage Gateway. Para obter mais informações sobre como criar uma conexão, consulte Conceitos básicos do Direct Connect no Guia do usuário do Direct Connect .
2. Conecte seu dispositivo Storage Gateway local ao Direct Connect roteador.
3. Crie uma interface virtual pública e configure seu roteador local de forma adequada. Para obter mais informações, consulte Como criar uma interface virtual no Guia do usuário do Direct Connect .

Para obter detalhes sobre Direct Connect, consulte O que é Direct Connect? no Guia do Direct Connect usuário.

Requisitos de permissões da conta de serviço do Active Directory

Se você planeja usar o Microsoft Active Directory para fornecer acesso autenticado pelo usuário aos sistemas de arquivos em seu AWS Storage Gateway, você precisa se certificar de que tem uma conta de serviço do Active Directory e que a conta de serviço tenha permissões delegadas para associar computadores ao seu domínio. Conta de serviço é uma conta de usuário no Active Directory que recebeu permissão para realizar determinadas tarefas. Você fornece as credenciais de nome de usuário e senha para essa conta ao associar um Storage Gateway ao domínio do Active Directory.

As seguintes permissões devem ser delegadas à conta de serviço do Active Directory na UO à qual você está associando o gateway:

- Capacidade para criar e excluir objetos de computador
- Capacidade de redefinir senhas
- Capacidade de modificar permissões
- Capacidade de restringir contas de ler e gravar dados
- Capacidade validada para ler e gravar restrições de conta
- Capacidade validada para gravar no nome da entidade principal de serviço

- Capacidade validada para gravar no nome do host DNS

Elas representam o conjunto mínimo de permissões necessárias para associar objetos de computador ao Active Directory. Para obter mais informações, consulte o tópico da documentação do Microsoft Windows Server Erro: o acesso é negado quando usuários não administradores aos quais foi delegado o controle tentam associar computadores a um controlador de domínio.

Como obter o endereço IP do dispositivo de gateway

Assim que escolher um host e implantar a VM do gateway, conecte e ative seu gateway. Para isso, você precisará do endereço IP VM do gateway. O endereço IP pode ser obtido no console local de seu gateway. Faça login no console local e obtenha o endereço IP na parte superior da página do console.

Para gateways implantados no local, é também possível obter o endereço IP no hipervisor. Para gateways do Amazon EC2, é possível obter o endereço IP da instância do Amazon EC2, no Amazon EC2 Management Console. Para saber como obter o endereço IP do gateway, consulte uma das opções a seguir:

- VMware hospedeiro: Acessando o console local do Gateway com VMware ESXi
- Host do HyperV: Acessar o console local do gateway com o Microsoft Hyper-V
- Host da Linux Kernel-based Virtual Machine (KVM): Acessar o console local do gateway com o Linux KVM
- Host do EC2: Como obter um endereço IP em um host do Amazon EC2

Quando você localizar o endereço IP, anote-o. Em seguida, retorne ao console do Storage Gateway e digite o endereço IP no console.

Como obter um endereço IP em um host do Amazon EC2

Para obter o endereço IP da instância do Amazon EC2 na qual seu gateway está implantado, faça login no console local da instância do EC2. Obtenha então o endereço IP na parte superior da página do console. Para instruções, consulte .

Também é possível obter o endereço IP no Amazon EC2 Management Console. É recomendável usar o endereço IP público na ativação. Para obter o endereço IP público, use o procedimento 1. Se você optar por usar o endereço IP elástico, consulte o procedimento 2.

Procedimento 1: para se conectar ao gateway usando o endereço IP público

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances e selecione a Instância EC2 na qual seu gateway está implantado.
3. Escolha a guia Description na parte inferior e anote o endereço IP público. Você usará esse endereço IP para se conectar ao gateway. Retorne ao console do Storage Gateway e insira o endereço IP.

Se você desejar usar o endereço IP elástico na ativação, use o procedimento a seguir.

Procedimento 2: para se conectar ao gateway usando o endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances e selecione a Instância EC2 na qual seu gateway está implantado.
3. Escolha a guia Description na parte inferior e tome nota do número presente em Elastic IP. Você usa o endereço IP elástico para se conectar ao gateway. Retorne ao console do Storage Gateway e insira o endereço IP elástico.

Compreendendo os recursos e recursos do Storage Gateway IDs

No Storage Gateway, o recurso principal é um gateway, mas outros tipos de recurso são o compartilhamento de arquivos. Os compartilhamentos de arquivos 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 nesta tabela.

Tipo de recurso	Formato do ARN
ARN de gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN de compartil	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

Tipo de recurso	Formato do ARN
hamento de arquivos	

Trabalhando com o recurso IDs

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.

Os IDs de recursos do Storage Gateway estão em letras maiúsculas. No entanto, quando você usa esses IDs de recurso com a API do Amazon EC2, o Amazon EC2 espera que os IDs de recurso estejam em letra minúscula. Você deve alterar o ID do recurso para minúscula para usá-lo com a API do EC2. Por exemplo, no Storage Gateway o ID de um volume deve ser `vol-1122AABB`. Ao usar esse ID com a API do EC2, você deve alterá-lo para `vol-1122aabb`. Do contrário, a API do EC2 talvez não se comporte como esperado.

> **Important**
>
> IDs para volumes do Storage Gateway e os snapshots do Amazon EBS criados a partir de volumes do 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 usá-los IDs por mais tempo para testar seus sistemas com o novo formato. Para obter mais informações, consulte Longer EC2 e EBS Resource. IDs
>
> 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, consulte Anúncio: Heads-up — Volume e instantâneo mais longos do Storage Gateway, que IDs serão lançados em 2016.

Atribuir tags a recursos do Storage Gateway

No Storage Gateway, é possível usar tags para gerenciar seus recursos. As tags permitem que você adicione metadados e categorize os recursos para torná-los mais fáceis de gerenciar. Toda tag é composta de um par de valores de chave, que são definidos por você. Você pode adicionar tags a gateways, volumes e fitas virtuais. Você pode pesquisar e filtrar esses recursos de acordo com as tags que adicionar.

Por exemplo, é possível usar tags para identificar quais recursos do Storage Gateway são usados por cada departamento em sua organização. Você pode atribuir tags a gateways e volumes usados pelo departamento de contabilidade da seguinte forma: (`key=department` e `value=accounting`). Em seguida, você pode usar essa tag como filtro para identificar todos os gateways e volumes usados pelo departamento de contabilidade e usar essas informações para determinar o custo. Para obter mais informações, consulte Usar tags de alocação de custos e Trabalhar com o Tag Editor.

Se você arquivar uma fita virtual marcada, ela manterá a tag no arquivo. Da mesma forma, se você recuperar uma fita do arquivo em outro gateway, as tags serão mantidas no novo gateway.

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.

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 marcas diferenciam maiúsculas de minúsculas.
- O número máximo de tags para cada recurso é 50.
- As chaves de tag não podem começar com `aws:`. O uso deste prefixo é reservado para a AWS .
- Os caracteres válidos para a propriedade da chave são letras e números UTF-8, espaço e os caracteres especiais + - = . _ : / e @.

Como trabalhar com tags

É possível trabalhar com tags usando o console, a API ou a interface de linha de comandos (CLI) do Storage Gateway. Os procedimentos a seguir mostram como adicionar, editar e excluir uma tag no console.

Para adicionar uma tag

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, escolha o recurso o qual você deseja atribui uma tag.

   Por exemplo, para atribuir uma tag a um gateway, escolha Gateways e, na lista de gateways, escolha o gateway ao qual deseja atribuir a tag.
3. Escolha Tags e em seguida Add/edit tags.
4. Na caixa de diálogo Add/edit tags, escolha Create tag.
5. Digite uma chave em Key e um valor em Value. Por exemplo, você pode digitar **`Department`** para a chave e **`Accounting`** para o valor.

   > **Note**
   >
   > Você pode deixar a caixa Value em branco.
6. Escolha Create Tag para adicionar mais tags. Você pode adicionar várias tags a um recurso.
7. Quando terminar de adicionar tags, escolha Save.

Para editar uma tag

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha o recurso cuja tag você deseja editar.
3. Escolha Tags para abrir a caixa de diálogo Add/edit tags.
4. Escolha o ícone de lápis ao lado da tag que deseja editar e edite-a.
5. Quando terminar de editar a tag, escolha Save.

Para excluir uma tag

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.

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.

Trabalhando com componentes de código aberto para AWS Storage Gateway

Esta seção descreve as ferramentas e licenças de terceiros das quais dependemos para oferecer a funcionalidade do AWS Storage Gateway .

Tópicos

Componentes de código aberto para o Storage Gateway

Várias ferramentas e licenças de terceiros são usadas para fornecer a funcionalidade do Gateway de Volumes, Gateway de Fitas e Gateway de Arquivos do Amazon S3.

Use os links a seguir para baixar o código-fonte de determinados componentes de software de código aberto incluídos no AWS Storage Gateway software:

- Para dispositivos Storage Gateway implantados em VMware ESXi: sources.tar
- Para dispositivos do Storage Gateway implantados no Microsoft Hyper-V: sources_hyperv.tar.
- Para dispositivos do Storage Gateway implantados na máquina virtual baseada em kernel (KVM) do Linux: sources_KVM.tar

Esse produto inclui software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit (http://www.openssl.org/). Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulte Licenças de terceiros.

Componentes de código aberto para o Amazon FSx File Gateway

Várias ferramentas e licenças de terceiros são usadas para fornecer a funcionalidade do 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 no software FSx File Gateway:

- Para o Amazon FSx File Gateway 2021-07-07, versão: -open-source.tgz sgw-file-fsx-smb
- Para a versão 2021-04-06 FSx do Amazon File Gateway: -20210406-open-source.tgz sgw-file-fsx-smb

Esse produto inclui software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit (http://www.openssl.org/). Para conferir as licenças relevantes para todas as ferramentas de terceiros dependentes, consulte os seguintes links:

- Para a versão 2021-07-07 FSx do Amazon File Gateway: Licença de terceiros.
- Para a versão 2021-04-06 FSx do Amazon File Gateway: Licença de terceiros.

Limites e cotas para o FSx

Cotas para sistemas de FSx arquivos da Amazon

A tabela a seguir lista os limites e cotas mínimos e máximos para os sistemas de FSx arquivos da Amazon.

Recurso	Limite por sistema de FSx arquivos da Amazon
Número máximo de tags	50 tags
Período máximo de retenção para backups automatizados	90 dias
Número máximo de solicitações de cópia de backup em andamento para uma única região de destino por conta.	5 solicitações
Capacidade mínima de armazenamento para sistemas de arquivos SSD	32 GiB
Capacidade mínima de armazenamento para sistemas de arquivos HDD	2 mil GiB

Recurso	Limite por sistema de FSx arquivos da Amazon
Capacidade máxima de armazenamento para sistemas de arquivos SSD e HDD	64 TiB
Capacidade de throughput mínima	8 MBps
Capacidade de throughput máxima	2.048 MBps
Número máximo de compartilhamentos de FSx arquivos da Amazon	100.000

Tamanhos de disco local recomendados para seu gateway

A tabela a seguir recomenda tamanhos de armazenamento em disco local para cada um AWS Storage Gateway em sua implantação.

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

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

Referência de API para o Storage Gateway

Além de usar o console, você pode usar a AWS Storage Gateway API para configurar e gerenciar programaticamente seus gateways. Esta seção descreve as AWS Storage Gateway operações, a assinatura de solicitações para autenticação e o tratamento de erros. Para obter informações sobre os endpoints disponíveis para o Storage Gateway, consulte Endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.

> **Note**
>
> Você também pode usar o AWS SDKs ao desenvolver aplicativos com o Storage Gateway. O AWS SDKs para Java, .NET e PHP envolve a API subjacente do Storage Gateway, simplificando suas tarefas de programação. Para obter informações sobre como fazer download de bibliotecas de SDKs, consulte Bibliotecas de códigos de exemplo.

Tópicos

AWS Storage Gateway Cabeçalhos de solicitação obrigatórios

Esta seção descreve os cabeçalhos requeridos que você precisa enviar em cada solicitação POST ao AWS 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 ActivateGatewayoperação.

```
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 para AWS Storage Gateway. Os cabeçalhos mostrados abaixo que começam com “x-amz” são AWS cabeçalhos específicos. Todos os outros cabeçalhos listados são cabeçalhos comuns usados em transações HTTP.

Cabeçalho	Description
`Authorization`	O cabeçalho de autorização contém várias informações sobre a solicitaç ão que permitem AWS Storage Gateway 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 legibilid ade): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= CalculatedSignature` Na sintaxe anterior, você especifica o ano YourAccessKey, mês e dia (aaaammdd), a região e o. CalculatedSignature O formato do cabeçalho de autorização é determinado pelos requisitos do processo de assinatur a AWS V4. Os detalhes da assinatura são discutidos no tópico Solicitaç ões de assinatura.
`Content-Type`	Use `application/x-amz-json-1.1` como tipo de conteúdo para todas as solicitações de AWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Cabeçalho	Description
`Host`	Use o cabeçalho do host para especificar o AWS Storage Gateway endpoint para o qual você envia sua solicitação. Por exemplo, `storagegateway.us-east-2.amazonaws.com` é o endpoint para a região Leste dos EUA (Ohio). Para obter mais informações sobre os endpoints disponíveis para AWS Storage Gateway, consulte AWS Storage Gateway Endpoints and Quotas no. Referência geral da AWS `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` cabeçalho está presente, AWS Storage Gateway ele ignora qualquer `Date` cabeçalho durante a autenticação da solicitação. O `x-amz-date` formato deve ser ISO8601 Básico no formato YYYYMMDD' T'HHMMSS'Z'. Se o `x-amz-date` cabeçalho `Date` e for usado, o formato do cabeçalho de data não precisa ser 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 APIs,. Referência de API para o Storage Gateway

Solicitações de assinatura

O Storage Gateway exige que toda solicitação enviada seja autenticada com uma assinatura. Para assinar uma solicitação, calcule uma assinatura digital usando a função de hash criptográfico. Hash criptográfico é uma função que retorna um valor de hash exclusivo com base na entrada. A entrada da função de hash inclui o texto da solicitação e a chave de acesso secreta. A função de hash retorna um valor de hash que você inclui na solicitação como sua assinatura. A assinatura é parte do cabeçalho `Authorization` de sua solicitação.

Depois de receber a solicitação, o Storage Gateway recalculará a assinatura usando a mesma função de hash e a entrada que você usou para assinar a solicitação. Quando a assinatura resultante corresponde à assinatura na solicitação, o Storage Gateway processa a solicitação. Do contrário, a solicitação é rejeitada.

O Storage Gateway é compatível com a autenticação usando o Signature versão 4 da AWS. O processo para calcular uma assinatura pode ser dividido em três tarefas:

- Tarefa 1: criar uma solicitação canônica

  Reorganize sua solicitação HTTP em um formato canônico. É necessário usar uma forma canônica, pois o Storage Gateway usa a mesma forma canônica quando recalcula uma assinatura para compará-la com a que você enviou.

- Tarefa 2: criar uma string para assinar

  Crie uma string que será usada como um dos valores de entrada para sua função hash criptográfica. A string, chamada string-to-sign, é uma concatenação do nome do algoritmo hash, da data da solicitação, de uma string do escopo da credencial e da solicitação canonizada da tarefa anterior. A string do escopo credencial em si é uma concatenação da data, da região e de informações do serviço.

- Tarefa 3: Crie uma assinatura

  Crie uma assinatura para sua solicitação usando uma função hash criptográfica que aceita duas strings de entrada: sua string para assinar e uma chave derivada. A chave derivada é calculada começando com sua chave de acesso secreta e usando a string do escopo da credencial para criar uma série de códigos de autenticação de mensagens 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.

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 para qualquer Storage Gateway APIs).

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: Crie uma assinatura, a chave derivada pode ser representada como:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Se a chave de acesso secreta, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, for usada, a assinatura calculada será:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

A etapa final é construir o cabeçalho `Authorization`. Para a chave de acesso de demonstração AKIAIOSFODNN7EXAMPLE, o cabeçalho (com quebras de linha adicionadas por motivo de legibilidade) é:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Respostas de erro

Tópicos

- Exceções
- Códigos de erro de operação
- Respostas de erro

Esta seção fornece informações de referência sobre AWS Storage Gateway erros. Esses erros são representados por uma exceção de erro e um código de erro de operação. Por exemplo, a exceção de erro `InvalidSignatureException` é retornada por qualquer resposta à API

se houver um problema na assinatura da solicitação. No entanto, o código de erro da operação `ActivationKeyInvalid` é retornado somente para a ActivateGatewayAPI.

Dependendo do tipo de erro, o Storage Gateway pode retornar somente uma exceção ou então um código de erro de exceção e de operação. Exemplos de respostas de erro são mostrados em Respostas de erro.

Exceções

A tabela a seguir lista as exceções AWS Storage Gateway da API. Quando uma AWS Storage Gateway operação retorna uma resposta de erro, o corpo da resposta contém uma dessas exceções. As exceções `InternalServerError` e `InvalidGatewayRequestException` retornam um dos códigos de mensagem de Códigos de erro de operação que geram os códigos de erro de operação específicos.

Exceção	Mensagem	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 ou ID da chave de AWS acesso fornecido não existe em nossos registros.	403 proibido
`InvalidGatewayRequestException`	Uma das mensagens de código de erro de operação em Códigos de erro de operação.	400 solicitação inválida

Exceção	Mensagem	Código de status HTTP
`InvalidSignatureException`	A assinatura da solicitação que calculamos não corresponde à assinatura que você forneceu. Verifique sua chave de AWS acesso e método de assinatura.	400 solicitação inválida
`MissingAction`	Está faltando um parâmetro de ação ou operação na solicitação.	400 solicitação inválida
`MissingAuthenticationToken`	A solicitação deve conter uma ID de chave de AWS acesso válida (registrada) ou um 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`	O ID da chave de AWS acesso precisa de uma assinatura para o serviço.	400 solicitação inválida
`ThrottlingException`	Taxa excedida.	400 solicitação inválida

Exceção	Mensagem	Código de status HTTP
`TooManyRequests`	Muitas solicitações.	429, muitas solicitações
`UnknownOperationException`	Foi especificada uma operação desconhecida. As operações válidas estão relacionadas em Ações de API do Storage Gateway.	400 solicitação inválida
`UnrecognizedClientException`	O token de segurança incluído na solicitação é inválido.	400 solicitação inválida
`ValidationException`	O valor de um parâmetro de entrada é inválido ou está fora do intervalo.	400 solicitação inválida

Códigos de erro de operação

A tabela a seguir mostra o mapeamento entre os códigos de erro de AWS Storage Gateway operação e APIs que pode 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	Mensagem	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	Mensagem	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	Mensagem	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 do endpoint da associação de sistema de arquivos existente entra em conflito com a configuração especificada.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	O endereço IP do endpoint especificado já está em uso.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	O endereço IP do endpoint da associação de sistema de arquivos está ausente.	AssociateFileSystem
FileSystemAssociationNotFound	A associação especificada do sistema de arquivos não foi encontrada.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	O sistema de arquivos especificado não foi encontrado.	AssociateFileSystem

Código de erro de operação	Mensagem	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	Mensagem	Operações que retornam esse código de erro
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Mensagem	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	Mensagem	Operações que retornam esse código de erro
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Mensagem	Operações que retornam esse código de erro
`GatewayNotFound`	O gateway especificado não foi encontrado.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

Código de erro de operação	Mensagem	Operações que retornam esse código de erro
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Mensagem	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	Mensagem	Operações que retornam esse código de erro
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Mensagem	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	Mensagem	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	Mensagem	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	Mensagem	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	Mensagem	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	Mensagem	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	Mensagem	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	Mensagem	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	Mensagem	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	Mensagem	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:

- Tipo de conteúdo: aplicativo/ -1,1 x-amz-json
- Um código de status HTTP `4xx` ou `5xx` apropriado

O corpo de uma resposta de erro contém informações sobre o erro que ocorreu. A resposta de erro de exemplo a seguir mostra a sintaxe de saída dos elementos comuns a todas as respostas de erro.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

A tabela a seguir explica os campos de resposta de erro JSON mostrados na sintaxe anterior.

__type

Uma das exceções de Exceções.

Tipo: string

error

Contém detalhes de erro específicos à API. Em erros genéricos (isto é, não específicos a nenhuma API), essa informação não é mostrada.

Tipo: Coleção

errorCode

Um dos códigos de erro de operação .

Tipo: string

errorDetails

Esse campo não é usado na versão atual da API.

Tipo: string

mensagem

Uma das mensagens de código de erro de operação em .

Tipo: string

Exemplos de resposta de erro

O corpo JSON a seguir será retornado se você usar a DescribeStoredi SCSIVolumes API e especificar uma entrada de solicitação ARN do gateway que não existe.

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

O seguinte corpo JSON será retornado se o Storage Gateway calcular uma assinatura que não corresponda à assinatura enviada com uma solicitação.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Ações de API do Storage Gateway

Para conferir uma lista completa de operações da API do Storage Gateway, consulte Ações na Referência de API do AWS Storage Gateway .

Histórico de documentos do Guia do usuário do Amazon FSx File Gateway

A tabela a seguir descreve as alterações importantes em cada versão deste guia do usuário depois de abril de 2018. Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

Alteração	Descrição	Data
Aviso de alteração de disponibilidade do FSx File Gateway	O Amazon FSx File Gateway não está mais disponíve l para novos clientes. Os clientes existentes do FSx File Gateway podem continuar usando o serviço normalmen te. Para recursos semelhant es ao FSx File Gateway, visite esta postagem do blog.	28 de outubro de 2024
Aviso de alteração de disponibilidade do FSx File Gateway	AWS Storage Gateway O FSx File Gateway não estará mais disponível para novos clientes a partir de 28/10/24. Para usar o serviço, você deve se inscrever antes dessa data. Os clientes existentes do FSx File Gateway podem continuar usando o serviço normalmen te. Para recursos semelhant es ao FSx File Gateway, visite esta postagem do blog.	26 de setembro de 2024
Opção adicionada para ativar ou desativar as atualizações de manutenção	O Storage Gateway recebe atualizações de manutenção regulares que podem incluir atualizações de sistema	6 de junho de 2024

	operacional e software, correções para tratar de estabilidade, desempenho e segurança, além de acesso a novos recursos. Agora você pode definir uma configura ção para ativar ou desativar essas atualizações para cada gateway individual em sua implantação. Para obter mais informações, consulte Gerenciando atualizações de gateway usando o AWS Storage Gateway console.	
CloudWatch Alarmes recomendados atualizados	O CloudWatch `HealthNot ifications` alarme agora se aplica e é recomenda do para todos os tipos de gateway e plataformas de host. As configurações recomendadas também foram atualizadas para `HealthNot ifications` e `Availabil ityNotifications` . Para obter mais informações, consulte .	2 de outubro de 2023

Dicas de GatewayClockOutOfSync solução de problemas adicionadas	A seção Solução de problemas: problemas do File Gateway agora inclui diretrizes de solução de problemas para ajudar a diagnosticar problemas que você pode encontrar se o relógio do sistema de gateway não estiver sincronizado com a hora do servidor do AWS Storage Gateway. Para obter mais informações, consulte Erro: GatewayClockOutOfSync.	19 de outubro de 2022
Adição de dicas de solução de problemas na associação do domínio ao Active Directory	A seção Solução de problemas: problemas do Gateway de Arquivos agora inclui diretrizes de solução de problemas para ajudar a diagnosticar problemas que você pode encontrar ao tentar associar seu gateway a um domínio do Active Directory. Para acessar mais informações, consulte Solução de problemas: problemas de domínio do Active Directory.	19 de outubro de 2022

Procedimentos atualizados de criação de gateway	O procedimento para criar um gateway foi atualizado para exibir as alterações no console do Storage Gateway. Para acessar mais informaçõ es, consulte Criar e ativar um Gateway de Arquivos do Amazon S3.	12 de outubro de 2021
Suporte a vários sistemas de arquivos	O Amazon FSx File Gateway agora suporta até cinco sistemas de FSx arquivos Amazon conectados. Para obter mais informações, consulte Anexar um sistema de arquivos Amazon FSx para Windows File Server.	7 de julho de 2021

Suporte à FSx cota de armazenamento virtual da Amazon	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 FSx arquivos anexados da Amazon nos quais as cotas de armazenam ento estão configuradas. As cotas rígidas (que impõem limites de dados ao negar o acesso de gravação) não são aceitas. As cotas flexíveis funcionam para todos os usuários, exceto para o usuário FSx administrador da Amazon. Para obter mais informações sobre a configura ção de cotas de armazenam ento, consulte Cotas de armazenamento no Guia do usuário do Amazon FSx para Windows File Server.	7 de julho de 2021

Novo guia	Além do File Gateway original (agora conhecido como Amazon S3 File Gateway), o Storage Gateway fornece o Amazon FSx File Gateway (FSx File Gateway). FSx O File Gateway fornece baixa latência e acesso eficiente à nuvem FSx para compartil hamentos de arquivos do Windows File Server a partir de suas instalações locais. Para obter mais informações, consulte O que é o Amazon FSx File Gateway?	27 de abril de 2021
Conformidade com o FedRAMP	O Storage Gateway agora está em conformidade com o FedRAMP. Para acessar mais informações, consulte Validação de conformidade para o Storage Gateway.	24 de novembro de 2020
Migração do Gateway de Arquivos	Agora é oferecido um processo documentado para substituir um Gateway de Arquivos existente por outro. Para acessar mais informaçõ es, consulte Substituir um Gateway de Arquivos por outro.	30 de outubro de 2020

A performance de leitura do cache frio do Gateway de Arquivos aumentou em quatro vezes	A performance de leitura do cache frio do Storage Gateway aumentou em quatro vezes. Para acessar mais informaçõ es, consulte Orientação de performance para Gateways de Arquivos.	31 de agosto de 2020
Solicite o dispositivo de hardware por meio do console	Agora você pode solicitar o dispositivo de hardware por meio do AWS Storage Gateway console. Para acessar mais informações, consulte Usar o Dispositivo de Hardware do AWS Storage Gateway.	12 de agosto de 2020
Support para endpoints do Federal Information Processin g Standard (FIPS) em novas regiões AWS	Agora é possível ativar um gateway com endpoints FIPS nas regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (N. da Califórnia), Oeste dos EUA (Oregon) e Canadá (Central). Para obter mais informações, consulte endpoints e cotas do AWS Storage Gateway na Referênci a geral da AWS.	31 de julho de 2020

O armazenamento em cache local do Gateway de Arquivos é quatro vezes maior	O Storage Gateway agora oferece suporte a um cache local de até 64 TB para o Gateway de Arquivos, melhorando a performance de aplicações on-premises ao fornecer acesso de baixa latência a conjuntos de dados de trabalho maiores. Para acessar mais informações, consulte Tamanhos de disco local recomendados para seu gateway no Guia do usuário do Storage Gateway.	7 de julho de 2020
Veja os CloudWatch alarmes da Amazon no console do Storage Gateway	Agora você pode ver CloudWatch os alarmes no console do Storage Gateway. Para obter mais informaçõ es, consulte Entendendo CloudWatch os alarmes.	29 de maio de 2020
Compatibilidade com endpoints do padrão FIPS (Padrão federal de processam ento de informações)	Agora, é possível ativar um gateway com endpoints de FIPS nas regiões AWS GovCloud (US) . Para escolher um endpoint FIPS para um Gateway de Arquivos, consulte Escolher um endpoint de serviço.	22 de maio de 2020

Novas AWS regiões	Agora o Storage Gateway está disponível nas regiões África (Cidade do Cabo) e Europa (Milão). Para obter mais informações, consulte endpoints e cotas do AWS Storage Gateway na Referênci a geral da AWS.	7 de maio de 2020
Compatibilidade com a classe de armazenamento S3 Intelligent-Tiering	Agora o Storage Gateway é compatível com a classe de armazenamento S3 Intelligent-Tiering. A classe de armazenamento S3 Intelligent-Tiering otimiza os custos de armazenamento movendo automaticamente os dados para o nível de acesso ao armazenamento mais econômico, sem impacto no desempenho ou sobrecarg a operacional. Para obter mais informações, consulte Classe de armazenamento para otimizar automaticamente os objetos acessados com frequência e pouca frequênci a no Guia do usuário do Amazon Simple Storage Service.	30 de abril de 2020

Nova AWS região	O Storage Gateway agora está disponível na região AWS GovCloud (Leste dos EUA). Para obter mais informações, consulte Endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.	12 de março de 2020
Compatibilidade com o hipervisor de máquina virtual baseada em kernel (KVM) do Linux	Agora o Storage Gateway oferece a possibilidade de implantar um gateway on-premises na plataforma de virtualização da KVM. Os gateways implantados na KVM têm todos as mesmas funcionalidades e recursos que os gateways locais existentes. Para obter mais informações, consulte Hipervisores compatíveis e requisitos de host no Guia do usuário do Storage Gateway.	4 de fevereiro de 2020

Support for VMware vSphere High Availability	O Storage Gateway agora fornece suporte para alta disponibilidade VMware para ajudar a proteger as cargas de trabalho de armazenamento contra falhas de hardware, hipervisor ou rede. Para obter mais informações, consulte Usando o VMware vSphere High Availability with Storage Gateway no Guia do usuário do Storage Gateway. Esta versão também inclui melhorias de desempenho. Para obter mais informaçõ es, consulte Desempenho no Guia do usuário do Storage Gateway.	20 de novembro de 2019
Support para Amazon CloudWatch Logs	Agora você pode configura r gateways de arquivos com Amazon CloudWatch Log Groups para ser notificad o sobre erros e a integrida de do seu gateway e de seus recursos. Para obter mais informações, consulte Receber notificações sobre a integridade e os erros do Gateway com grupos de CloudWatch log da Amazon no Guia do usuário do Storage Gateway.	4 de setembro de 2019

Novo Região da AWS	Agora o Storage Gateway está disponível na região Ásia-Pacífico (Hong Kong) . Para obter mais informações, consulte Endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.	14 de agosto de 2019
Novo Região da AWS	Agora o Storage Gateway está disponível na região do Oriente Médio (Bahrein) . Para obter mais informações, consulte Endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.	29 de julho de 2019
Compatibilidade com a ativação de um gateway em uma nuvem privada virtual (VPC)	Agora é possível ativar um gateway em uma VPC. É possível criar uma conexão privada entre o dispositivo de software local e a infraestrutura de armazenamento baseada em nuvem. Para obter mais informações, consulte Ativar um gateway em uma nuvem privada virtual.	20 de junho de 2019

O Gateway de Arquivos oferece suporte à autorização com base em tag	O Gateway de Arquivos agora oferece suporte à autorizaç ão com base em tag. Você pode controlar o acesso aos recursos do Gateway de Arquivos com base nas tags desses recursos. Também é possível controlar o acesso com base nas tags que podem ser transmiti das em uma condição de solicitação do IAM. Para obter mais informações, consulte Controlar o acesso aos recursos do gateway de arquivos.	4 de março de 2019
Disponibilidade do dispositi vo de hardware AWS Storage Gateway na Europa	O AWS Storage Gateway Hardware Appliance agora está disponível na Europa. Para obter mais informaçõ es, consulte Regiões do equipamento de hardware do AWS Storage Gateway na Referência geral da AWS. Além disso, agora você pode aumentar o armazenamento utilizável no Storage Gateway Hardware Appliance de 5 TB para 12 TB e substituir a placa de rede de cobre instalada por uma placa de rede de fibra óptica de 10 gigabits. AWS Para obter mais informaçõ es, consulte Configurar seu dispositivo de hardware.	25 de fevereiro de 2019

Support for AWS Storage Gateway Hardware Appliance	O AWS Storage Gateway Hardware Appliance inclui o software Storage Gateway pré-instalado em um servidor de terceiros. Você pode gerenciar o dispositivo do Console de gerenciamento da AWS. O dispositivo pode hospedar gateways de arquivos, fitas e volumes. Para obter mais informações, consulte Como usar o Storage Gateway Hardware Appliance.	18 de setembro de 2018

Atualizações anteriores

A tabela a seguir descreve alterações importantes em cada versão do Guia do usuário do AWS Storage Gateway antes de maio de 2018.

Alteração	Descrição	Alterado em
Novo Região da AWS	Agora o gateway de fitas está disponível na região Ásia-Pacífico (Singapura). Para obter informações detalhadas, consulte Regiões da AWS que suportam Storage Gateway.	3 de abril de 2018
Novo Região da AWS	Agora o Storage Gateway está disponível na região Europa (Paris). Para obter informações detalhada s, consulte Regiões da AWS que suportam Storage Gateway.	18 de dezembro de 2017
Support for VMware ESXi Hypervisor versão 6.5	AWS Storage Gateway agora oferece suporte à versão 6.5 do VMware ESXi Hypervisor. Além das versões 4.1, 5.0, 5.1, 5.5 e 6.0. Para obter mais informações, consulte Hipervisores compatíveis e requisitos de host.	13 de setembro de 2017

Alteração	Descrição	Alterado em
Compatibilidade com gateway de arquivos do hipervisor do Microsoft Hyper-V	Agora é possível implantar um gateway de arquivos em um hipervisor do Microsoft Hyper-V. Para mais informações, consulte Hipervisores compatíveis e requisitos de host.	22 de junho de 2017
Novo Região da AWS	Agora o Storage Gateway está disponível na região da Ásia-Pacífico (Mumbai). Para obter informações detalhadas, consulte Regiões da AWS que suportam Storage Gateway.	02 de maio de 2017
Compatibilidade com gateways de arquivos no Amazon EC2	AWS Storage Gateway agora fornece a capacidad e de implantar um gateway de arquivos no Amazon EC2. É possível ativar um gateway de arquivos no Amazon EC2 usando a Imagem de Máquina da Amazon (AMI) do Storage Gateway, agora disponíve l como uma AMI de comunidade. Para acessar informações sobre como criar um Gateway de Arquivos e implantá-lo em uma instância do EC2, consulte Crie e ative um Amazon FSx File Gateway. Para acessar informações sobre como iniciar uma AMI de Gateway de Arquivos, consulte Implante um host padrão do Amazon EC2 para FSx o File Gateway. Além disso, agora o Gateway de Arquivos oferece suporte à configuração de proxy HTTP. Para obter mais informações, consulte Encaminhar o gateway implantado no Amazon EC2 por meio de um proxy HTTP.	08 de fevereiro de 2017
Novo Região da AWS	Agora o Storage Gateway está disponível na região da Europa (Londres). Para obter informações detalhada s, consulte Regiões da AWS que suportam Storage Gateway.	13 de dezembro de 2016

Alteração	Descrição	Alterado em
Novo Região da AWS	Agora o Storage Gateway está disponível na região Canadá (Central). Para obter informações detalhadas, consulte Regiões da AWS que suportam Storage Gateway.	08 de dezembro de 2016
Suporte para gateway de arquivos	Além dos gateways de volumes e do gateway de fitas, o Storage Gateway agora fornece o gateway de arquivos. O gateway de arquivos é ao mesmo tempo um serviço e um dispositivo de software virtual que permite que você armazene e recupere objetos no Amazon S3 usando protocolos de arquivo padrão do setor, como o Network File System (NFS). O gateway oferece acesso a objetos no Amazon S3 como arquivos em um ponto de montagem NFS.	29 de novembro de 2016