Guia do usuário do Gateway de Arquivos do Amazon S3

AWS Storage Gateway

Versão da API 2013-06-30

AWS Storage Gateway: Guia do usuário do Gateway de Arquivos do Amazon S3

Table of Contents

O que é o Gateway de Arquivos do Amazon S3

Gateway de Arquivos do Amazon S3: o Gateway de Arquivos do Amazon S3 oferece suporte a uma interface de arquivos no Amazon Simple Storage Service (Amazon S3) e combina um serviço e um dispositivo de software virtual. Quando você usa essa combinação, é possível armazenar e recuperar objetos no Amazon S3 por meio de protocolos de arquivo padrão do setor, como o Network File System (NFS) e o Server Message Block (SMB). Você implanta o gateway em seu ambiente local como uma máquina virtual (VM) em execução no VMware ESXi, Microsoft ou Linux Kernel-based Virtual Machine (KVM) Hyper-V, ou como um dispositivo de hardware que você compra de seu revendedor preferido. Você também pode implantar a VM do Storage Gateway no VMware Cloud on AWS ou como uma AMI no Amazon EC2. O gateway oferece acesso a objetos no S3 como arquivos ou pontos de montagem de compartilhamento de arquivos. Com um Gateway de Arquivos do S3, você pode fazer o seguinte:

- Agora você pode armazenar e recuperar arquivos diretamente usando o protocolo NFS versão 3 ou 4.1.
- Agora você pode armazenar e recuperar arquivos diretamente usando a versão de sistema de arquivo SMB, protocolo 2 e 3.
- Você pode acessar seus dados diretamente no Amazon S3 a partir de qualquer aplicativo ou AWS serviço na nuvem.
- Você pode gerenciar seus dados do S3 usando políticas de ciclo de vida, replicação entre regiões e versionamento. Você pode pensar em um Gateway de Arquivos do S3 como uma montagem de sistema de arquivos no Amazon S3.

O Gateway de Arquivos do S3 simplifica o armazenamento de arquivos no Amazon S3, integra-se a aplicações existentes por meio de protocolos de sistema de arquivos padrão do setor e constitui uma alternativa econômica de armazenamento on-premises. Além disso, oferece acesso de baixa latência aos dados por meio de armazenamento em cache local transparente. O S3 File Gateway gerencia a transferência de dados de e para AWS, protege os aplicativos do congestionamento da rede, otimiza e transmite dados em paralelo e gerencia o consumo de largura de banda.

O S3 File Gateway se integra a outros AWS serviços, por exemplo:

- Gerenciamento de acesso comum usando AWS Identity and Access Management (IAM)
- Criptografia usando AWS Key Management Service (AWS KMS)
- Monitoramento usando Amazon CloudWatch (CloudWatch)

- Auditoria usando AWS CloudTrail (CloudTrail)
- Operações usando o Console de gerenciamento da AWS e AWS Command Line Interface (AWS CLI)
- Faturamento e gerenciamento de custos

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

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

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

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

Como funciona o Gateway de Arquivos do Amazon S3

Para usar um Gateway de Arquivos do S3, comece baixando uma imagem da VM para o gateway. Em seguida, você ativa o gateway a partir da Console de gerenciamento da AWS ou por meio da API Storage Gateway. Você também pode criar um Gateway de Arquivos do S3 usando uma imagem do Amazon EC2.

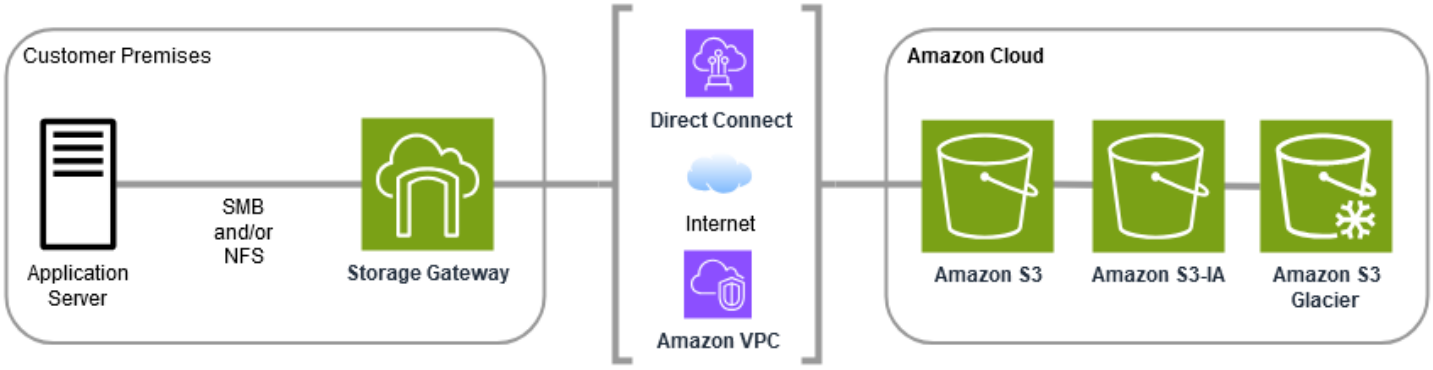
Depois que o Gateway de Arquivos do S3 for ativado, crie e configure o compartilhamento de arquivos e associe-o ao bucket do Amazon Simple Storage Service (Amazon S3). Assim, clientes que usam o protocolo Network File System (NFS) ou Server Message Block (SMB) poderão acessar o compartilhamento. Os arquivos gravados em um compartilhamento de arquivos tornam-se objetos no Amazon S3, com o caminho atuando como chave. Não há um mapeamento individualizado entre arquivos e objetos, e o gateway atualiza assincronamente os objetos no Amazon S3 com o mesmo procedimento usado em alterações nos arquivos. Os objetos existentes no bucket do Amazon S3 aparecem como arquivos no sistema de arquivos e a chave transforma-se o caminho. Os objetos são

criptografados com chaves de criptografia do lado do servidor do Amazon S3 (). SSE-S3 Todas as transferências de dados são feitas por meio de HTTPS.

Ao enviar solicitações de upload de dados HTTPS para o Amazon S3, o File Gateway preenche o Content-MD5 cabeçalho com a soma de verificação MD5 dos dados que estão sendo carregados. O uso desse cabeçalho faz com que o Amazon S3 exiba uma falha em caso de incompatibilidade entre a soma de verificação MD5 calculada pelo Amazon S3 e o valor recebido do Gateway de Arquivos. Se essa falha for exibida, o Gateway de Arquivos reenviará a solicitação.

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

Com o armazenamento do Gateway de Arquivos do S3, é possível realizar tarefas, como ingerir workloads da nuvem para o Amazon S3, fazer backup e arquivamento, hierarquização e migração de dados de armazenamento para a Nuvem AWS . O diagrama a seguir fornece uma visão geral da implantação do armazenamento de arquivos para o Storage Gateway.



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

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

Operação de arquivo	Impacto do objeto do S3	Implicação de classe de armazenamento
Renomear um arquivo	Substitui o objeto do S3 existente e cria um objeto do S3 para cada arquivo.	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas.
Renomear pasta	Substitui todos os objetos do S3 existentes e cria objetos do S3 para cada pasta e arquivos na estrutura de pastas.	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas.
Alterar file/folder permissões	Substitui o objeto do S3 existente e cria um objeto do S3 para cada arquivo ou pasta.	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas.
Alterar file/folder propriedade	Substitui o objeto do S3 existente e cria um objeto do S3 para cada arquivo ou pasta.	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas.
Anexar a um arquivo	Substitui o objeto do S3 existente e cria um objeto do S3 para cada arquivo.	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas.

Quando um arquivo é gravado no Gateway de Arquivos do S3 por um cliente NFS ou SMB, o Gateway de Arquivos faz upload dos dados do arquivo para o Amazon S3 seguidos por seus metadados (propriedades, carimbos de data/hora etc.). O upload dos dados do arquivo cria um objeto do S3, e o upload dos metadados atualiza os metadados do objeto do S3. Esse processo cria outra versão do objeto, gerando duas versões dele. Se o versionamento do S3 estiver ativado, as duas versões serão armazenadas.

Quando um arquivo é modificado no Gateway de Arquivos do S3 por um cliente NFS ou SMB após o upload para o Amazon S3, o Gateway de Arquivos do S3 faz upload dos dados novos ou modificados em vez de fazer upload do arquivo inteiro. A modificação do arquivo gera a criação de uma versão do objeto do S3.

Quando o Gateway de Arquivos do S3 faz upload de arquivos maiores, talvez seja necessário fazer upload de partes menores do arquivo antes que o cliente termine de gravar no Gateway de Arquivos do S3. Alguns motivos para isso são liberar espaço no cache ou uma alta taxa de gravações em um compartilhamento de arquivos. Isso pode gerar diversas versões de um objeto no bucket do S3.

Monitore seu bucket do S3 para saber quantas versões de um objeto existem antes de configurar políticas de ciclo de vida a fim de migrar objetos para diferentes classes de armazenamento. Configurar a expiração do ciclo de vida das versões anteriores para minimizar o número de versões de um objeto em seu bucket do S3. O uso de Same-Region replicação (SRR) ou Cross-Region replicação (CRR) entre buckets S3 aumentará o armazenamento usado.

Conceitos básicosAWS Storage Gateway

Esta seção fornece instruções para começar a usarAWS. Você precisa de uma AWS conta antes de começar a usarAWS 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 AWSRegiões 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

- AcessoAWS Storage Gateway- Saiba como se inscrever AWS e criar uma AWS conta.
- AcessoAWS Storage Gateway: saiba como criar um usuário do IAM com privilégios administrativos para sua conta da AWS.
- AcessoAWS Storage Gateway- Saiba como acessar AWS Storage Gateway por meio do console do Storage Gateway ou programaticamente usando os AWS SDKs.
- Regiões da AWSque suportam Storage Gateway- Saiba quais AWS regiões você pode usar para armazenar seus dados ao ativar seu gateway no Storage Gateway.

Inscreva-se para umConta da AWS

Para começarAWS, você precisa de umConta da AWS. Para obter informações sobre como criar umConta da AWS, consulte Introdução a um Conta da AWS no Guia de AWS Gerenciamento de contas referência.

AcessoAWS 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, criar, gerenciar e excluir compartilhamentos 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 na 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 os AWS SDKs para desenvolver aplicativos que interajam com o Storage Gateway. Os AWS SDKs para Java, .NET e PHP encapsulam a API subjacente do Storage Gateway para simplificar as tarefas de programação. Para obter informações sobre como 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 AWSque 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, comoAWS 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.

- 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 Gatewayendpoints 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 o Gateway de Arquivos do Amazon S3 (Gateway de Arquivos do S3), você deve atender aos seguintes pré-requisitos:

- 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.

Para acessar informações sobre as práticas recomendadas para a performance do Gateway de Arquivos, consulte Orientação básica de desempenho para o S3 File Gateway Gateway.

Requisitos de hardware para VMs locais

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.

Para acessar mais informações, consulte Maximizar o throughput do Gateway de Arquivos do S3. Para obter informações sobre como o hardware afeta o desempenho da VM do gateway, consulte Cotas para compartilhamentos de arquivos.

Requisitos para tipos de instância do Amazon EC2

Ao implantar seu gateway no Amazon Elastic Compute Cloud (Amazon EC2), o tamanho da instância deve ser pelo menos **`xlarge`** para que 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. ARM-based instâncias que usam processadores Graviton não são suportadas.

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

Recomendado para tipos de Gateway de Arquivos

- General-purpose família de instâncias — tipo 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.
- Compute-optimized família de instâncias — 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.
- Memory-optimized família de instâncias — 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.
- Storage-optimized família de instâncias — 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.
> As gravações da aplicação são armazenadas no cache de maneira síncrona e, depois, é feito upload delas de modo assíncrono no armazenamento durável no Amazon S3. Se o armazenamento temporário for perdido porque uma instância foi interrompida antes da conclusão do upload, os dados que ainda residem no cache e ainda não foram gravados no Amazon Simple Storage Service (Amazon S3) poderão ser perdidos. Antes de interromper a instância que hospeda o gateway, verifique se a `CachePercentDirty` CloudWatch métrica é `0`. Para obter informações sobre o armazenamento temporário, consulte Usar o armazenamento temporário com gateways do EC2. Para acessar informações sobre métricas de monitoramento para seu Storage Gateway, consulte Monitorando seu gateway de arquivos S3, gateway de .
> Se você tiver mais de 5 milhões de objetos em seu bucket do S3 e estiver usando um volume EBS gp2, é necessário um volume mínimo de EBS raiz de 350 GiB para um desempenho aceitável do seu gateway durante a inicialização. Newly-created As instâncias do Amazon EC2 File Gateway usam volumes raiz gp3 por padrão, que não têm esse requisito. Para acessar informações sobre como aumentar o tamanho do volume, consulte Modificar um volume do EBS usando volumes elásticos (console).

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.

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

Requisitos de rede e firewall

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

Os requisitos de largura de banda 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

O Gateway de Arquivos do S3 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 clientes NFS ou SMB, endpoints da VPC ou Microsoft Active Directory.

Para o Gateway de Arquivos do S3, só é necessário usar o Microsoft Active Directory quando você deseja permitir que os usuários do domínio acessem um compartilhamento de arquivos do Server Message Block (SMB). 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 Gateway de Arquivos do S3

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Navegador da web	Seu navegador da web	VM do Storage Gateway	TCP HTTP	80	✓	✓	✓	Usado por sistemas locais para recuperar a chave de ativação do Storage Gateway. A porta 80 só é usada durante a ativação de um dispositivo do Storage Gateway. Uma VM do Storage Gateway não exige que a porta

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
								80 seja publicamente acessível. O nível necessário de acesso à porta 80 depende da configuração da rede. Se você ativar o gateway pelo Console de Gerenciamento do Storage Gateway, o host pelo qual se conecta ao console deverá ter

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
								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)
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. *Exigido somente para SMB.

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	NetBIOS UDP	137	✓	✓	✓*	Serviço de nome *Exigido somente para SMBv1.
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	NetBIOS UDP	138	✓	✓	✓*	Serviço de datagrama *Exigido somente para SMBv1.
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	TCP e UDP LDAP	389	✓	✓	✓*	Conexão do cliente do Directory System Agent (DSA) *Exigido somente para SMB.

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 Kerberos	88	✓	✓	✓*	Kerberos *Exigido somente para SMB.
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	Mapeador de Environment/Endpontos de computação distribuída da TCP () DCE/ EMAP	135	✓	✓	✓*	RPC *Exigido somente para SMB.

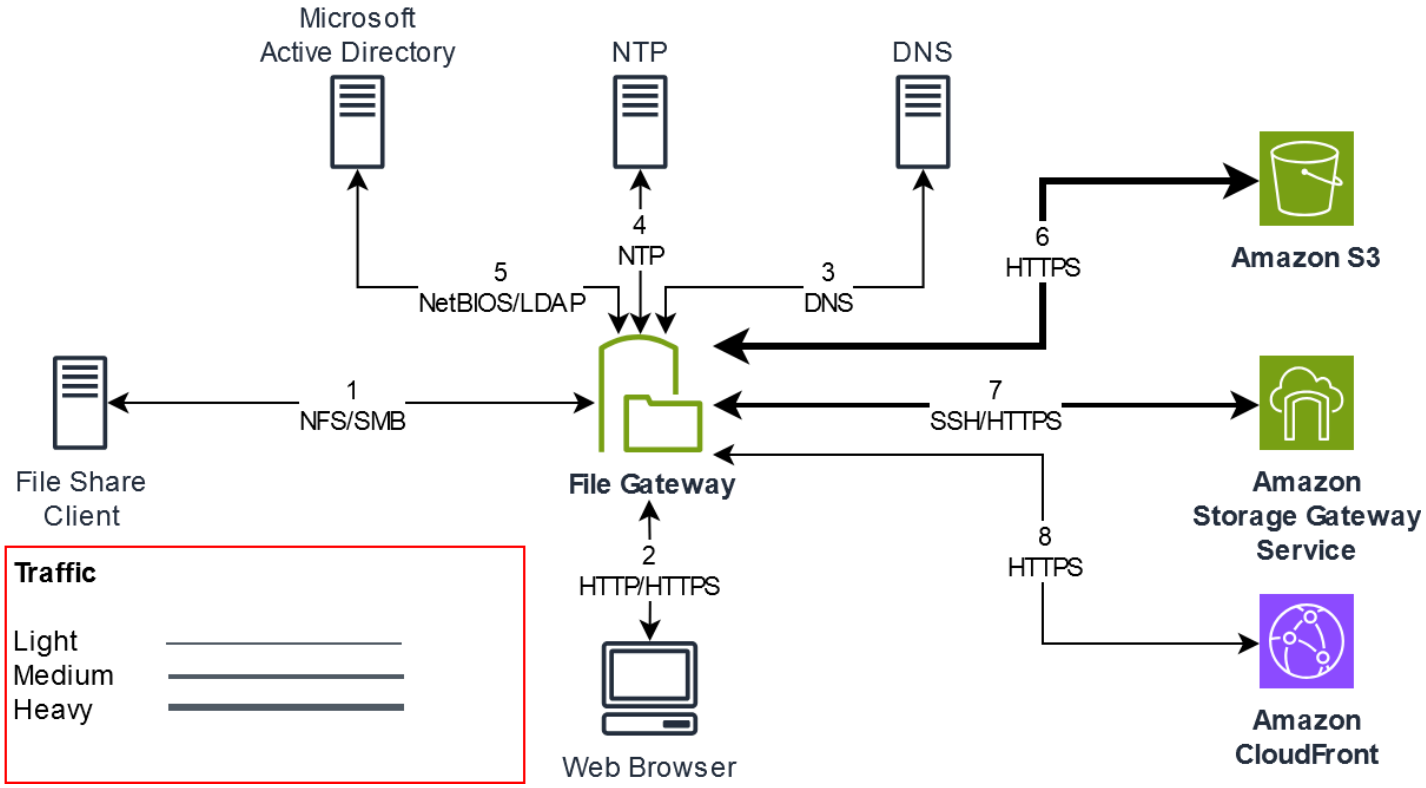
Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Microsoft Active Directory	VM do Storage Gateway	Servidor do Active Directory	Mapeador de Environment/Endpoints de computação distribuída TCP () DCE/EMAP	49152-65535	✓	✓	✓*	RPC Como alternativa, se o controlador de domínio AD usar portas RPC dedicadas, abra-as em vez disso. *Exigido somente para SMB.

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Cliente de compartilhamento de arquivo	Cliente NFS	VM do Storage Gateway	Dados TCP ou UDP NFSv3	111	✓	✓	✓*	Transferência de dados de compartilhamento de arquivo (apenas para NFS v3) *Exigido somente para NFS.
Cliente de compartilhamento de arquivo	Cliente NFS	VM do Storage Gateway	TCP ou UDP NFS	2049	✓	✓	✓*	Compartilhamento de arquivos e transferência de dados *Exigido somente para NFS v3 e v4.

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Cliente de compartilhamento de arquivo	Cliente NFS	VM do Storage Gateway	TCP ou UDP NFSv3	20048	✓	✓	✓*	Compartilhamento de arquivos e transferência de dados *Exigido somente para NFSv3.
Cliente de compartilhamento de arquivo	Cliente SMB	VM do Storage Gateway	TCP ou UDP SMBv2	139	✓	✓	✓*	Serviço de sessão de transferência de dados de compartilhamento de arquivos. *Exigido somente para SMB.

Elemento de rede	De	Para	Protocolo	Porta	Entrada	Saída	Obrigatório	Observações
Amazon S3	VM do Storage Gateway	Endpoints de serviço do Amazon S3	TCP HTTPS	443	✓	✓	✓	Para comunicação da VM do Storage Gateway com o endpoint do AWS serviço. Para obter informações sobre endpoints de serviço, consulte Permitir o acesso ao AWS Storage Gateway por meio de firewalls e roteadores.

A ilustração a seguir mostra o fluxo de tráfego de rede para uma implantação básica do Gateway de Arquivos do S3.



Requisitos de rede e firewall para o Storage Gateway Hardware Appliance

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

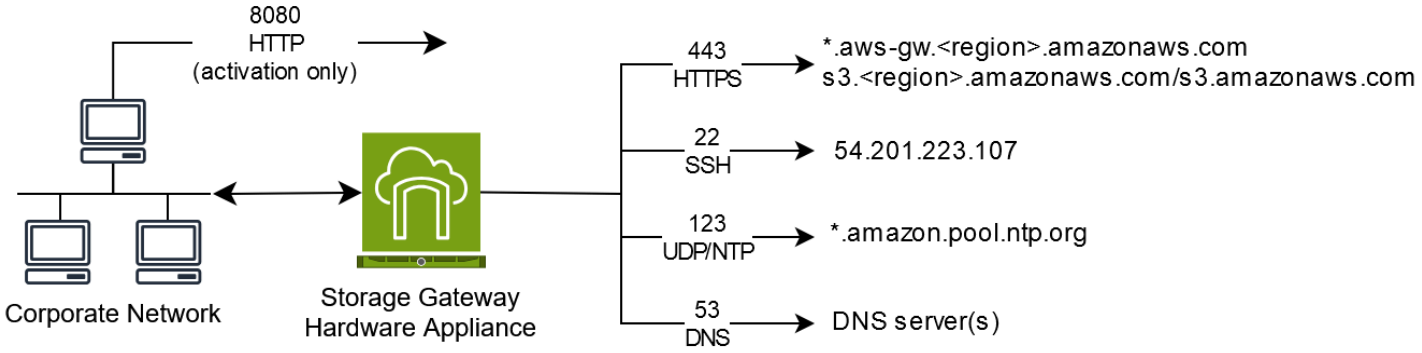
- Acesso à internet: em uma rede sempre disponível de conexão com a Internet por meio de uma interface de rede no servidor.
- DNS services: serviços DNS para comunicação entre o dispositivo de hardware e o servidor DNS.
- Sincronização de horário: um serviço Amazon NTP de horário configurado automaticamente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

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

1. iDRAC
2. `em1`

3. em2
4. em3
5. em4

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



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

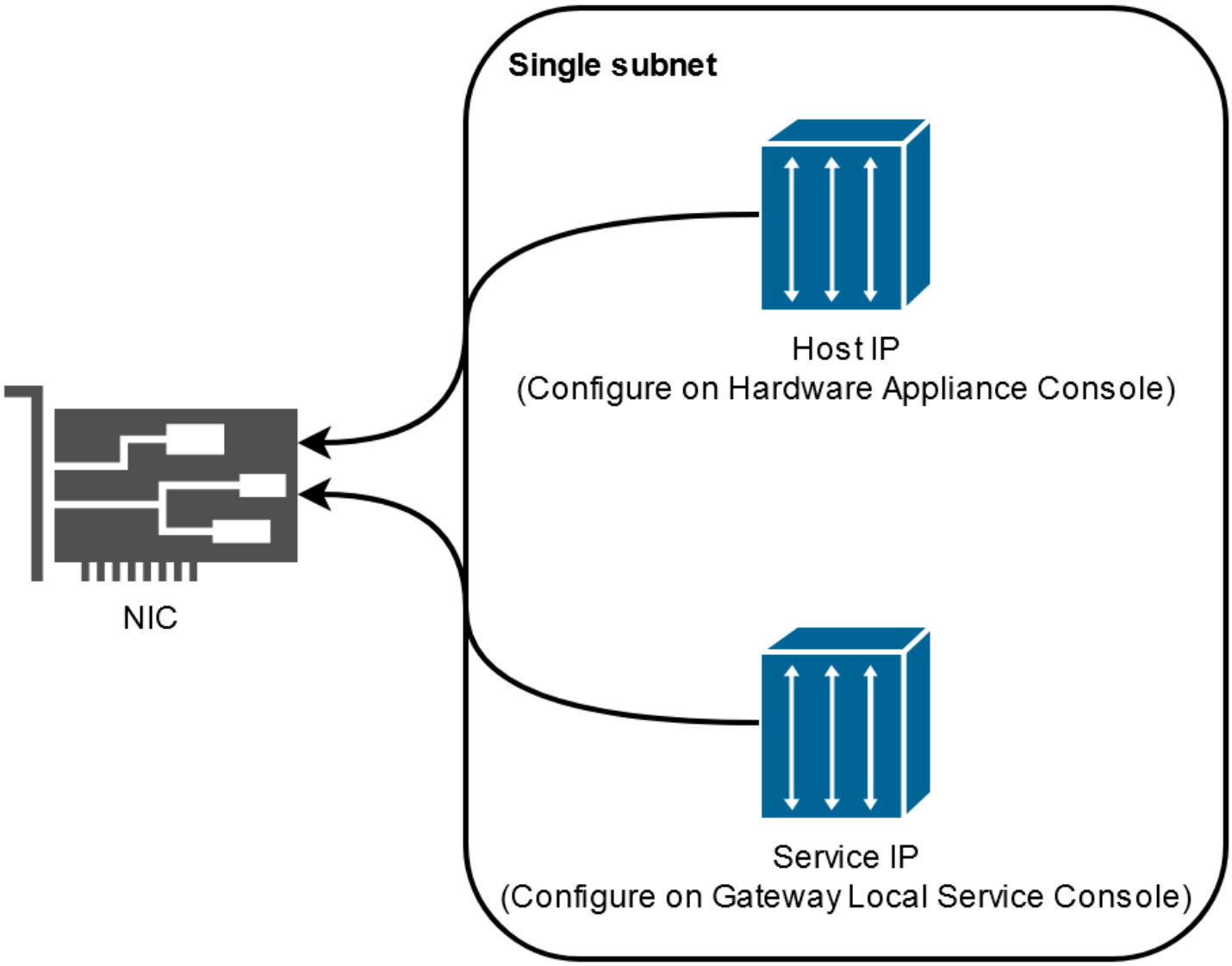
Protocolo	Porta	Direction	Fonte	Destino	Usage
SSH	22	Saída	Equipamento de hardware	`54.201.223.107`	Canal de suporte
DNS	53	Saída	Equipamento de hardware	Servidores DNS	Resolução de nome
UDP/NTP	123	Saída	Equipamento de hardware	`*.amazon.pool.ntp.org`	Sincronização de horário
HTTPS	443	Saída	Equipamento 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 Usar o AWS Dispositivo de hardware do 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 tráfego IPv4 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
```

Dual-stack endpoints

Esses endpoints oferecem suporte a tráfego IPv4 e IPv6 entre o dispositivo de gateway e a AWS.

O endpoint de serviço de pilha dupla a seguir é exigido por todos os gateways para operações de head-bucket.

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

Os endpoints de serviço de pilha dupla a seguir são exigidos por todos os gateways para operações de caminho de controle (ativação, ambiente de gerenciamento, proxy) e caminho de dados (plano de dados).

```
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
```

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

```
storagegateway.region.api.aws:443
```

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

```
storagegateway.us-west-2.api.aws:443
```

Endpoints de serviço do Amazon S3

O Gateway de Arquivos do Amazon S3 exige os três tipos de endpoints a seguir para se conectar ao serviço Amazon S3:

Endpoint de serviço do Amazon S3

> **Note**
>
> Somente para esse endpoint, não `s3` substitua por `s3-fips` para FIPS-compliant implantações.

```
s3.amazonaws.com
```

Endpoints regionais do Amazon S3

```
s3.region.amazonaws.com (Standard)
s3.dualstack.region.amazonaws.com (Dual-stack)
```

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

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

O exemplo a seguir mostra endpoints regionais padrão e de pilha dupla do FIPS-compliant Amazon S3 na região Oeste dos EUA (Norte da Califórnia) (). `us-west-1`

```
s3-fips.us-west-1.amazonaws.com
s3-fips.dualstack.us-west-1.amazonaws.com
```

Os exemplos a seguir mostram os endpoints regionais padrão e de pilha dupla do Amazon S3 usados pelas regiões: AWS GovCloud (US)

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

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

> **Note**
>
> Se seu gateway não puder determinar Região da AWS onde seu bucket do Amazon S3 está localizado, esse endpoint de serviço assume como padrão. `s3.us-east-1.amazonaws.com` Recomendamos que você permita o acesso à região Leste dos EUA (Norte da Virgínia`us-east-1`) (), além de Regiões da AWS onde seu gateway está ativado e onde seu bucket do Amazon S3 está localizado.

Endpoints de bucket do Amazon S3

```
bucket-name.s3.region.amazonaws.com (Standard)
bucket-name.s3.dualstack.region.amazonaws.com (Dual-stack)
```

Os exemplos a seguir mostram endpoints de bucket do Amazon S3 padrão e de pilha dupla para um bucket nomeado *amzn-s3-demo-bucket* na região do Leste dos EUA (Ohio) (`us-east-2`).

```
amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com (Standard)
amzn-s3-demo-bucket.s3.dualstack.us-east-2.amazonaws.com (Dual-stack)
```

Os exemplos a seguir mostram endpoints de bucket FIPS-compliant Amazon S3 padrão e de pilha dupla para um bucket chamado *amzn-s3-demo-bucket1* na Região (). AWS GovCloud (US-East) `us-gov-east-1`

```
amzn-s3-demo-bucket1.s3-fips.us-gov-east-1.amazonaws.com (FIPS)
amzn-s3-demo-bucket1.s3-fips.dualstack.us-gov-east-1.amazonaws.com (FIPS dual-stack)
```

Além dos endpoints de serviço do Storage Gateway e do Amazon S3, as VMs do Storage Gateway também exigem 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.

Para obter informações sobre quais portas abrir para seu gateway, consulte Requisitos de porta.

Hipervisores compatíveis e requisitos de host

Você pode executar o Storage Gateway 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:

- Hypervisor VMware ESXi (versões 7.0 ou 8.0): para configurar o VMware vSphere, você também precisa de um cliente VMware vSphere para se conectar ao host.
- Microsoft Hyper-V Hypervisor (2019, 2022 ou 2025) — Para essa configuração, você precisa de um Microsoft Hyper-V Manager em um computador cliente Microsoft Windows para se conectar ao host.
- Linux Kernel-based Virtual Machine (KVM) — Uma tecnologia de virtualização gratuita e de código aberto. O KVM está incluído em todas as versões do Linux versão 2.6.20 e mais 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 arquivo aws-storage-gateway.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 KVM-based virtualização 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 Implantar um host padrão do Amazon EC2 para o Gateway de Arquivos do S3.
- 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 NFS e SMB aceitos pelo Gateway de Arquivos

O Gateway de Arquivos oferece suporte aos seguintes clientes:

Versão do sistema operacional	Versão do kernel	Protocolos compatíveis
Amazon Linux 2023	6,1 LITROS	NFSv4.1, NFSv3
Amazon Linux 2	5,10 LITROS	NFSv4.1, NFSv3
RHEL 9	5.14	NFSv4.1, NFSv3
RHEL 8.10	4.18	NFSv4.1, NFSv3
SUSE 15	6.4	NFSv4.1, NFSv3
Ubuntu 24.04 LTS	6,8 LITROS	NFSv4.1, NFSv3
Ubuntu 22.04 LTS	5,15 LITROS	NFSv4.1, NFSv3
Microsoft Windows Server 2025		SMBv2, SMBv3, NFSv3
Microsoft Windows Server 2022		SMBv2, SMBv3, NFSv3
Microsoft Windows 11		SMBv2, SMBv3, NFSv3

Versão do sistema operacional	Versão do kernel	Protocolos compatíveis
Microsoft Windows 10		SMBv2, SMBv3, NFSv3

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

Operações de sistema de arquivos aceitas pelo Gateway de Arquivos

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

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

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

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 funciona como um armazenamento on-premises duradouro para dados com upload pendente para o Amazon S3. 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 S3, pense na quantidade de disco de cache a ser alocada. O Gateway de Arquivos do S3 usa um algoritmo usado menos recentemente para remover automaticamente os dados do cache. O cache em um Gateway de Arquivos do S3 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 determinada workload, é importante observar que você sempre pode adicionar disco de cache ao gateway (até as cotas atuais no Gateway de Arquivos do S3), mas não é possível diminuir o cache de 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 workloads mudam com o tempo, e o Gateway de Arquivos do S3 fornece 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 armazenamento de dados no VMware. Ao implantar a VM do gateway, você escolhe um armazenamento de dados para armazenar os arquivos da VM. Ao provisionar um disco local (por exemplo, para uso como armazenamento em cache), você tem a opção de armazenar o disco virtual no mesmo armazenamento de dados que a VM ou 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 válido quando o backup é uma configuração de RAID menos eficiente, 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/home.
3. No painel de navegação, selecione Gateways da .
4. Procure seu gateway e selecione-o na lista.
5. No menu Ações, selecione Configurar armazenamento 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

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

Os discos temporários fornecem armazenamento ao nível do bloco temporário para instâncias do Amazon EC2. Os discos temporários são ideais para armazenamento temporário de dados alterados com frequência, como aqueles no em um armazenamento em cache do gateway. 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.

Os dados que as aplicações gravam no gateway são armazenados de forma síncrona em cache nos discos temporários e, depois, carregados de forma assíncrona para armazenamento durável no Amazon S3. Se a instância do Amazon EC2 for interrompida depois que os dados forem gravados no armazenamento temporário, mas antes que ocorra um upload assíncrono, qualquer dado que ainda não tenha sido carregado para o Amazon S3 poderá ser perdido. Você pode evitar essa perda de dados seguindo as etapas antes de reiniciar ou interromper a instância do EC2 que hospeda seu gateway.

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

Essas etapas que compõem o procedimento a seguir são específicas de Gateways de Arquivos.

Como evitar a perda de dados em Gateways de Arquivos que usam discos temporários

1. Interrompa todos os processos que estão gravando no Amazon S3.
2. Inscreva-se para receber notificações de CloudWatch eventos. Para mais informações, consulte Receber notificação sobre operações de arquivo.
3. Chame a NotifyWhenUploaded API para ser notificado quando os dados gravados, até a perda do armazenamento temporário, forem armazenados de forma duradoura no Amazon S3.
4. Você vai receber o ID da notificação depois que a API concluir o processo.

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

Usar o AWS Dispositivo de hardware do 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. É possível configurar o dispositivo de hardware como um Gateway de Arquivos do S3, um Gateway de Arquivos do FSx, um Gateway de Fitas ou um Gateway de Volumes. 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 locais em Regiões da AWS que 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 AWS Dispositivo de hardware do 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 AWS Dispositivo de hardware do Storage Gateway

Configurando seu AWS Dispositivo de hardware do 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 dispositivo é ativado, você pode iniciar um Gateway de Arquivos do S3, um Gateway de Arquivos do FSx, um Gateway de Fitas ou um Gateway de Volumes pelo console do Storage Gateway.

Para instalar e configurar o dispositivo de hardware

1. Rack-mount o aparelho e conecte as conexões de alimentação e 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 (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 AWS Dispositivo de hardware do Storage Gateway.

4. Crie um gateway no dispositivo de hardware. Para obter mais informações, consulte Como criar um gateway.

   Você configura gateways em seu dispositivo de hardware da mesma forma que configura gateways no VMware ESXi, Hyper-V Microsoft, Kernel-based Linux Virtual Machine (KVM) ou Amazon EC2.

Aumento do armazenamento em cache utilizável

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

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

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

Opções da placa da interface de rede

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

- Configuração de 10 G-Base-T NIC:
  - Use cabos CAT6 para 10G ou CAT5(e) para 1G
- Configuração de NIC 10G DA/SFP +:
  - Use cabos de conexão direta de cobre Twinax de até cinco metros
  - Dell/Intel módulos ópticos SFP+ compatíveis (SR ou LR)
  - SFP/SFP+ transceptor de cobre para 1 ou 10 G-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). DAC de cobre Twinax, módulo óptico SFP+ (compatível com Intel) ou transceptor SFP para cobre. Base-T
- Teclado e monitor, ou uma solução de switch de teclado, vídeo e mouse (KVM).

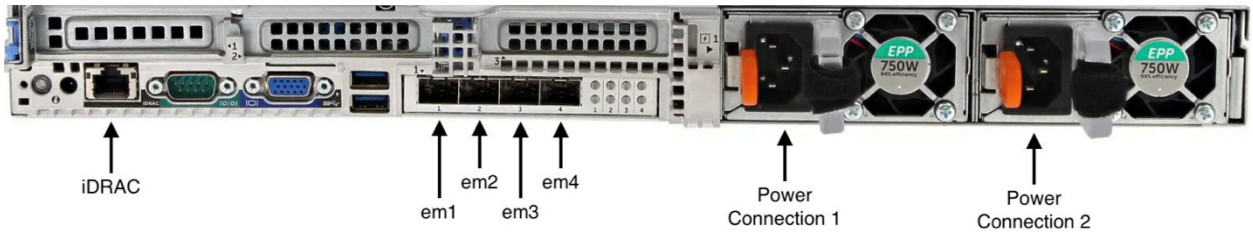
> **Note**
>
> Antes de executar o procedimento a seguir, verifique se você atende a todos os requisitos para o Storage Gateway Hardware Appliance como descrito em Requisitos de rede e firewall para o Storage Gateway Hardware Appliance.

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.

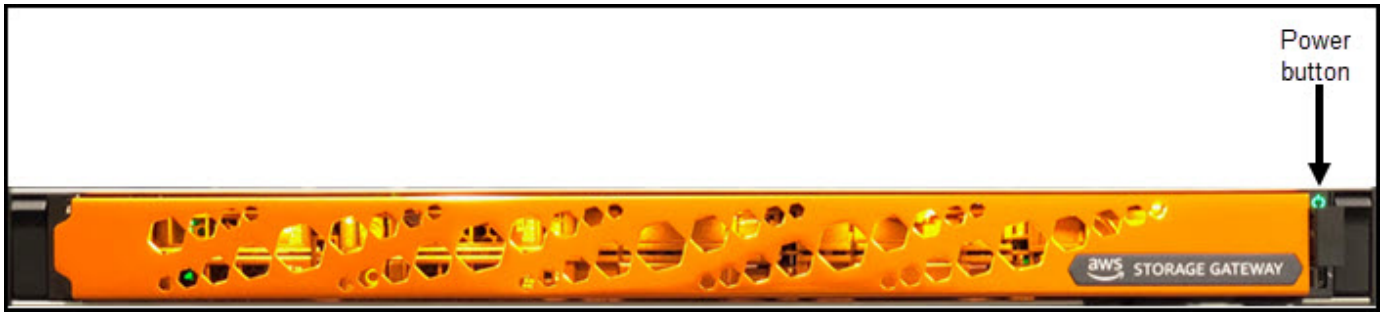


parte traseira do dispositivo um de hardware com etiquetas de rede e conector de alimentação.

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 endereço IPv4 atribuído pelo servidor Protocolo de Configuração Dinâmica de Host (DHCP) para a porta de rede física.

Anote este endereço para uso posterior na etapa de ativação.

- Escolha Estático e pressione `Enter` para configurar um endereço IPv4 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 AWS Dispositivo de hardware do Storage Gateway

Ativando seu AWS Dispositivo de hardware do 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 AWS Dispositivo de hardware do Storage Gateway

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

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

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

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

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

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

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

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

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.

É possível criar um Gateway de Arquivos do S3, um Gateway de Arquivos do FSx, um Gateway de Fitas ou um Gateway de Volumes no Dispositivo de Hardware do AWS Storage Gateway durante a 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/home.

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:

   - HTTP/SOCKS Configuração de proxy
   - 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 Configurar o Gateway de Arquivos do Amazon S3.

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/home.
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 AWS Dispositivo de hardware do 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 equipamento 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 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

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 .

Criar e ativar um Gateway de Arquivos para o Amazon S3

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

Tópicos

Configurar um Gateway de Arquivos do Amazon S3

Como configurar um novo Gateway de Arquivos do S3

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 Gateway de Arquivos do Amazon S3.
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.
      - Nutanix AHV — Baixe, implante e configure a máquina virtual gateway usando a Máquina Virtual Baseada em Kernel Linux (KVM). A mesma imagem funciona para ambientes de hipervisor Linux KVM e Nutanix AHV.

- 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 S3 File Gateway a AWS

Para conectar um novo S3 File Gateway ao AWS

1. Conclua o procedimento descrito em Configurar um Gateway de Arquivos do Amazon S3, caso ainda não tenha feito isso. Ao terminar, escolha Avançar para abrir a AWS página Connect to no AWS Storage Gateway console.
2. 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. Para obter mais informações, consulte Como obter o endereço IP do gateway.
   - 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.

3. Na seção Opções de endpoint, faça o seguinte:

   a. Para Endpoint de serviço, escolha o tipo de endpoint que 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.

  > **Note**
  >
  > Para especificar um endpoint da VPC que pertença a uma Conta da AWS que não seja a que você está usando atualmente para criar seu gateway, você deve fornecer o nome DNS ou o endereço IP.

b. Em Versão IP, escolha a versão do protocolo e o endpoint que seu gateway usará para se comunicar com a AWS.

> **Note**
>
> O endereço IP do gateway deve corresponder à versão de IP especificada aqui. Os endpoints de pilha dupla IPv4 aceitam IPv6 conexões, mas eles só se comunicam com seu gateway usando a versão IP selecionada.

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

Analisar as configurações e ativar o Gateway de Arquivos do Amazon S3

Como analisar as configurações e ativar um novo Gateway de Arquivos do S3

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

   - Configurar um Gateway de Arquivos do Amazon S3
   - Conecte seu Amazon S3 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.

Configurar o Gateway de Arquivos do Amazon S3

Como realizar a primeira configuração em um novo Gateway de Arquivos do S3

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

   - Configurar um Gateway de Arquivos do Amazon S3
   - Conecte seu Amazon S3 File Gateway a AWS
   - Analisar as configurações e ativar o Gateway de Arquivos do Amazon S3

   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 Compreendendo os CloudWatch alarmes.

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

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

5. (Opcional) Na seção Tags, escolha Adicionar nova tag e, 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 você criou o gateway, deverá criar um compartilhamento de arquivos a ser usado por ele. Para receber instruções, consulte Criar um compartilhamento de arquivos.

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 Conectar seu Amazon S3 File Gateway para AWS conectar

Para configurar seu Gateway de Arquivos do S3 para transferir dados por meio da VPC, você deve criar um endpoint da VPC separado para o Amazon S3 e, depois, especificar esse endpoint da VPC ao criar compartilhamentos de arquivos para o gateway.

> **Note**
>
> Você deve ativar o gateway na mesma região em que criou o endpoint da VPC para o Storage Gateway, e o armazenamento do Amazon S3 que você configura para o compartilhamento de arquivos deve estar na mesma região em que você criou o endpoint da VPC para o Amazon S3.

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 S3 File Gateway Gateway.

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

> **Important**
>
> Para configurar seu Gateway de Arquivos do S3 para transferir dados por meio da VPC, você deve criar um endpoint da VPC separado para o Amazon S3 e, depois, especificar esse endpoint da VPC ao criar compartilhamentos de arquivos para o gateway. Para fazer isso, siga as mesmas etapas mostradas acima, mas escolha `com.amazonaws.region.s3` Nome do serviço e selecione a tabela de rotas à qual você deseja associar o endpoint do S3 em vez do subnet/security grupo. Para receber instruções, consulte Criar um endpoint de gateway.

Criar um compartilhamento de arquivos

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

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

Ao criar um compartilhamento de arquivos SMB, você pode usar um dos três modos de autenticação:

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

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

Um Gateway de Arquivo pode hospedar um ou mais compartilhamentos de arquivos de tipos diferentes. Você pode ter vários compartilhamentos de arquivos NFS e SMB em um Gateway de Arquivos.

> **Important**
>
> Para criar um compartilhamento de arquivos, um gateway de arquivos exige que você ative AWS Security Token Service (AWS STS). Se AWS STS não estiver ativado no Região da

AWS local em que você criou seu File Gateway, ative-o. Para obter informações sobre como ativarAWS STS, consulte Ativação e desativação AWS Security Token Service em uma AWS região no Guia do AWS Identity and Access Management usuário.

Tópicos

Evitar custos imprevistos no upload de dados do gateway

Quando um arquivo é gravado no Gateway de Arquivos por um cliente NFS, o Gateway de Arquivos faz upload dos dados do arquivo para o Amazon S3 seguidos por seus metadados. O upload dos dados do arquivo cria um objeto do S3, e o upload dos metadados atualiza os metadados do objeto do S3. Esse processo cria uma versão adicional do objeto. Se o versionamento do S3 estiver ativado, as duas versões serão armazenadas.

Se você alterar os metadados de um arquivo armazenado no seu Gateway de Arquivos, um novo objeto do S3 será criado e substituirá o objeto do S3 existente. Esse comportamento é diferente da edição de um arquivo em um sistema de arquivos, em que a edição de um arquivo não gera a criação de outro arquivo. Teste todas as operações de arquivo que você planeja usar com o AWS Storage Gateway para entender como cada operação de arquivo interage com o armazenamento do Amazon S3.

Considere cuidadosamente o uso do controle de versão e Cross-Region replicação (CRR) do S3 no Amazon S3 ao fazer o upload de dados do seu gateway de arquivos. O upload de arquivos do seu gateway de arquivos para o Amazon S3 quando o controle de versão do S3 está ativado geralmente resulta em mais de uma versão de um objeto do S3.

Certos fluxos de trabalho envolvendo arquivos grandes e padrões de gravação de arquivos, como uploads de arquivos que são executados em várias etapas, podem aumentar o número de versões de objetos do S3 armazenadas. Se o cache do Gateway de Arquivos precisar liberar espaço devido às altas taxas de gravação de arquivos, várias versões de objetos do S3 poderão ser criadas.

Esses cenários aumentarão o armazenamento do S3 se o versionamento do S3 estiver ativado e aumentarão os custos de transferência associados à CRR. Teste todas as operações de arquivo que você planeja usar com o Storage Gateway para entender como cada operação de arquivo interage com o armazenamento do Amazon S3.

O uso do utilitário Rsync com seu Gateway de Arquivos gera a criação de arquivos temporários no cache e a criação de objetos do S3 temporários no Amazon S3. Essa situação resulta em cobranças de exclusão antecipada na classe de armazenamento S3 Standard-Infrequent Access (S3 Standard-IA).

Criptografar objetos armazenados pelo gateway de arquivos no Amazon S3

O Gateway de Arquivos do S3 oferece suporte aos seguintes métodos de criptografia do lado do servidor para os dados que ele armazena no Amazon S3:

- SSE-S3— Por padrão, todos os novos objetos enviados para os buckets do Amazon S3 usam criptografia do lado do servidor com chaves gerenciadas do Amazon S3. Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 no Guia do usuário do Amazon Simple Storage Service.
- SSE-KMS— Você pode configurar seu compartilhamento de arquivos para usar criptografia do lado do servidor com chaves gerenciadas AWS Key Management Service (AWS KMS). AWS KMSé um serviço que combina hardware e software seguros e altamente disponíveis para fornecer um sistema de gerenciamento de chaves dimensionado para a nuvem. Para obter mais informações, consulte O que é o AWS Key Management Service? no Guia do AWS Key Management Service desenvolvedor.
- DSSE-KMS— a criptografia Dual-layer do lado do servidor com AWS KMS chaves aplica duas camadas de criptografia aos objetos quando eles são enviados para o Amazon S3. Isso ajuda a cumprir os padrões de conformidade referentes à criptografia de várias camadas. Para obter mais informações, consulte Usando criptografia de camada dupla no lado do servidor com chaves AWS KMS no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Há custos adicionais pelo uso DSSE-KMS e pelas AWS KMS chaves. Para obter mais informações, consulte Preços do AWS KMS.

É possível especificar um método de criptografia ao criar um compartilhamento de arquivos usando o console do Storage Gateway ou a API do Storage Gateway. Em relação a procedimentos do console, consulte Criar um compartilhamento de arquivos NFS com configuração personalizada ou Criar um compartilhamento de arquivos SMB com configuração personalizada. Para obter informações sobre os comandos de API correspondentes, consulte CreateNFSFileShareou CreateSMBFileSharena Referência da API do AWS Storage Gateway.

É possível também atualizar as configurações de criptografia de um compartilhamento de arquivos existente usando o console do Storage Gateway ou a API do Storage Gateway. Para o procedimento do console, consulte Alterar o método de criptografia do lado do servidor para um compartilhamento de arquivos existente. Para obter informações sobre os comandos de API correspondentes, consulte UpdateNFSFileShareou UpdateSMBFileSharena Referência da API do AWS Storage Gateway.

> **Note**
>
> Depois de atualizar o método de criptografia, o gateway usa o novo método para todos os novos objetos criados no Amazon S3 e para qualquer objeto armazenado que ele atualize ou modifique no futuro. Os objetos existentes do Amazon S3 só receberão o novo método de criptografia se forem atualizados ou modificados pelo gateway.

> **Important**
>
> Seu compartilhamento de arquivos deve usar o mesmo tipo de criptografia que do bucket do Amazon S3 em que ele armazena seus dados.
> Se você configurar seu gateway de arquivos para usar SSE-KMS ou DSSE-KMS para criptografia, deverá adicionar manualmente`kms:Encrypt`,`kms:Decrypt`,`kms:ReEncrypt*`,`kms:GenerateDataKey`, e `kms:DescribeKey` permissões à função do IAM associada ao compartilhamento de arquivos. Para obter mais informações, consulte Como usar Identity-Based políticas (políticas do IAM) para o Storage Gateway.

Criar um compartilhamento de arquivos NFS

O protocolo NFS (Network File System) é um protocolo de compartilhamento de arquivos com monitoramento de estado para sistemas baseados em Unix. Quando um cliente habilitado para

NFS e um servidor NFS se comunicam, o cliente solicita um arquivo ou diretório do servidor usando chamadas de procedimento remoto (RPC). O servidor verifica se o arquivo ou diretório está disponível e se o cliente tem as permissões de acesso necessárias. Depois, o servidor monta o arquivo ou diretório remotamente no cliente e compartilha o acesso por meio de uma conexão virtual. Para operações de cliente, o NFS torna o uso do arquivo do servidor remoto semelhante ao acesso a um arquivo local.

> **Note**
>
> O protocolo NFS oferece suporte a até 16 grupos por usuário. Os usuários podem ter problemas ao montar compartilhamentos de arquivos NFS se pertencerem a mais de 16 grupos. Para evitar problemas de montagem, assegure-se de que os usuários sejam membros de 16 grupos ou menos ao acessar compartilhamentos de arquivos NFS.

Os tópicos a seguir explicam vários métodos para criar um compartilhamento de arquivos NFS para seu Gateway de Arquivos:

Sumário

Criar um compartilhamento de arquivos NFS usando a configuração padrão

Esta seção explica como criar um compartilhamento de arquivos do Network File System (NFS) usando configurações padrão pré-configuradas. Use esse método para implantações básicas, uso pessoal, testes ou como uma forma de implantar rapidamente vários compartilhamentos de arquivos que você planeja editar e personalizar posteriormente. Para ver uma lista das configurações padrão para compartilhamentos de arquivos que você cria usando esse procedimento, consulte Configurações padrão para compartilhamentos de arquivos NFS. Se você precisar de um controle mais granular ou quiser usar configurações avançadas para seu compartilhamento de arquivos, consulte Criar um compartilhamento de arquivos NFS com uma configuração personalizada.

> **Note**
>
> Se você precisar conectar seu compartilhamento de arquivos ao Amazon S3 por meio de uma nuvem privada virtual (VPC), deverá seguir o procedimento de configuração personalizado. Não é possível editar configurações de VPC para um compartilhamento de arquivos depois de criá-lo.

> **Important**
>
> Usar o versionamento do S3, a replicação entre regiões ou o utilitário Rsync ao fazer upload de dados de um Gateway de Arquivos pode ter implicações de custo significativas. Para acessar mais informações, consulte Evitar custos imprevistos ao fazer upload de dados do Gateway de Arquivos.

Como criar um compartilhamento de arquivos NFS usando a configuração padrão:

1. Abra o console do AWS Storage Gateway em https://console.aws.amazon.com/storagegateway/casa/ e escolha Compartilhamentos de arquivos no painel de navegação esquerdo.
2. Escolha Create file share (Criar compartilhamento de arquivos).
3. Em Gateway, escolha o Gateway de Arquivos do Amazon S3 na lista suspensa.
4. Em Protocolo de compartilhamento de arquivos, escolha NFS.
5. Em Bucket do S3, siga um destes procedimentos:

   - Escolha um bucket do Amazon S3 existente na sua conta na lista suspensa.
   - Escolha Um bucket em outra conta na lista suspensa e insira o nome do bucket em Nome do bucket entre contas.
   - Escolha Criar bucket do S3 e, depois, selecione a Região da AWS onde o endpoint do Amazon S3 para seu novo bucket está localizado e insira um nome exclusivo do bucket do S3. Selecione Criar bucket do S3 quando terminar.

     Para acessar mais informações sobre como um bucket, consulte Como criar um bucket do S3 no Guia do usuário do Amazon S3.

> **Note**
>
> O Gateway de Arquivos do S3 não oferecem suporte a buckets do Amazon S3 com pontos (`.`) no nome do bucket.
> Confirme se o nome do bucket está de acordo com as regras de nomenclatura de bucket no Amazon S3. Para obter mais informações, consulte as Regras para nomear buckets no Manual do usuário do Amazon Simple Storage Service.

6. Analise as configurações em Configuração padrão e escolha Criar compartilhamento de arquivos para criar seu compartilhamento de arquivos NFS usando a configuração padrão.

Depois que seu compartilhamento de arquivos NFS for criado, você poderá ver suas configurações no console do AWS Storage Gateway na guia Detalhes do compartilhamento de arquivos. Para acessar informações sobre como montar seu compartilhamento de arquivos, consulte Montar seu compartilhamento de arquivos NFS em seu cliente.

Configurações padrão para compartilhamentos de arquivos NFS

As configurações a seguir se aplicam a todos os novos compartilhamentos de arquivos NFS criados usando a configuração padrão. Depois de criar um compartilhamento de arquivos, você pode selecioná-lo na página Compartilhamentos de arquivos no console do AWS Storage Gateway para ver detalhes sobre sua configuração.

> **Important**
>
> A configuração padrão do compartilhamento de arquivos NFS fornece controle total de arquivos e permissões de acesso ao proprietário do bucket do S3 que está mapeado para o compartilhamento de arquivos, mesmo que o bucket seja de propriedade de uma conta diferente. AWS Para acessar mais informações sobre como usar seu compartilhamento de arquivos para acessar objetos em um bucket de propriedade de outra conta, consulte Usar um compartilhamento de arquivos para acesso entre contas.

Configuração	Valor padrão	Observações
Localização do Amazon S3	O compartilhamento de arquivos se conecta diretamente ao bucket do Amazon S3 e tem o mesmo nome que do bucket. Seu gateway usa esse bucket para armazenar e recuperar arquivos.	O nome não inclui prefixo.
AWS PrivateLink para S3	O compartilhamento de arquivos não se conecta ao Amazon S3 por meio de um endpoint em sua nuvem privada virtual (VPC).	
Notificação de upload de arquivos	Desativado	
Classe de armazenamento para novos objetos	Amazon S3 Standard	Isso permite armazenar os dados de objetos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Para acessar mais informações sobre a classe de armazenamento Amazon S3 Standard, consulte Classes de armazenamento para objetos acessados com frequência no Guia do usuário do Amazon Simple Storage Service.
Criptografia	Criptografia do lado do servidor com chaves gerenciadas pelo S3 (SSE-S3)	Todos os objetos do Amazon S3 dos quais seu Gateway de Arquivos do S3 faz upload,

Configuração	Valor padrão	Observações
		atualiza ou modifica são criptografados por padrão com criptografia do lado do servidor usando chaves gerenciadas pelo Amazon S3.
Metadados do objeto	Adivinhar o tipo MIME	Isso permite ao Storage Gateway adivinhar o tipo Multipurpose Internet Mail Extension (MIME) dos objetos cujo upload foi feito com base nas extensões de arquivo. Essa opção exige que as Listas de Controle de Acesso (ACLs) estejam ativadas para o bucket do Amazon S3 associado ao seu compartil hamento de arquivos. Se ACLs são desativado, o compartilhamento de arquivos não pode acessar o bucket do Amazon S3 e permanece no estado Indisponível indefinid amente.
Habilitar pagamentos pelo solicitante	Desativado	Para obter mais informaçõ es, consulte Buckets de pagamento pelo solicitante.
Logs de auditoria	Desativado	O registro em um Amazon CloudWatch grupo é desativad o por padrão.

Configuração	Valor padrão	Observações
Acessar o bucket do S3	Criar um perfil do IAM	A opção padrão permite que o Gateway de Arquivos acesse um novo perfil e política de acesso do IAM em seu nome. Todos os clientes NFS têm acesso permitido. Para acessar informações sobre clientes NFS aceitos, consulte Clientes NFS e SMB aceitos pelo Gateway de Arquivos.
Opções de montagem	• Nível de extermínio: extermínio de raiz • Exportar como: leitura e gravação	O valor padrão do nível de extermínio significa que acesso para o controle remoto o superusuário (raiz) é associado ao Identificador de Usuário (UID) (65534) e ao Identificador de Grupo (GID) (65534).
Padrões de metadados de arquivo	• Permissões de diretório: 0777 • Permissões de arquivo: 0666 • Identificador de usuário (UID): 65534 • Identificador de grupo (GID): 65534	

Criar um compartilhamento de arquivos NFS com configuração personalizada

Use o procedimento a seguir para criar um compartilhamento de arquivos do Network File System (NFS) com configuração personalizada. Para criar um compartilhamento de arquivos NFS usando as configurações padrão, consulte Criar um compartilhamento de arquivos NFS usando a configuração padrão.

> **Important**
>
> Usar o versionamento do S3, a replicação entre regiões ou o utilitário Rsync ao fazer upload de dados de um Gateway de Arquivos pode ter implicações de custo significativas. Para acessar mais informações, consulte Evitar custos imprevistos ao fazer upload de dados do Gateway de Arquivos.

Como criar um compartilhamento de arquivos NFS com configurações personalizadas

1. Abra o console do AWS Storage Gateway em https://console.aws.amazon.com/storagegateway/casa/ e escolha Compartilhamentos de arquivos no painel de navegação esquerdo.
2. Escolha Create file share (Criar compartilhamento de arquivos).
3. Escolha Personalizar configuração. Você pode ignorar os outros campos desta página por enquanto. Será solicitado que você defina as configurações de gateway, protocolo e armazenamento nas etapas subsequentes.
4. Em Gateway, escolha o Gateway de Arquivos do Amazon S3 para o novo compartilhamento de arquivos na lista suspensa.
5. Para o grupo de CloudWatch registros, escolha uma das seguintes opções na lista suspensa:
   - Para desativar o registro em log desse compartilhamento de arquivos, escolha Desativar registro em log.
   - Para criar automaticamente um grupo de logs para esse compartilhamento de arquivos, escolha Criado pelo Storage Gateway.
   - Para enviar notificações de integridade e recursos desse compartilhamento de arquivos a um grupo de logs existente, escolha o grupo desejado na lista.

Para acessar mais informações sobre logs de auditoria, consulte Noções básicas dos logs de auditoria do Gateway de Arquivos do S3.

6. (Opcional) Em Tags: opcional, escolha Adicionar nova tag e insira uma chave e um valor para o seu compartilhamento de arquivos.

   Tag é um par de chave-valor que diferencia maiúsculas de minúsculas e ajuda você a categorizar os recursos do Storage Gateway. Adicionar tags pode facilitar a filtragem e a pesquisa do seu compartilhamento de arquivos. Repita essa etapa para adicionar até cinquenta tags.

   Quando terminar, escolha Próximo.

7. Em Bucket do S3, faça o seguinte para especificar onde seu compartilhamento de arquivos armazenará e recuperará arquivos:

   - Para conectar o compartilhamento de arquivos diretamente a um bucket do S3 existente em sua conta da Amazon Web Services, escolha o nome do bucket na lista suspensa.
   - Para conectar o compartilhamento de arquivos a um bucket existente do S3 pertencente a uma conta da Amazon Web Services diferente da que você usa para criar o compartilhamento de arquivos, escolha Um bucket em outra conta na lista suspensa e insira o nome do bucket entre contas.
   - Para conectar o compartilhamento de arquivos a um novo bucket do S3, escolha Criar um bucket do S3 e, depois, escolha a região onde o endpoint do Amazon S3 para seu novo bucket está localizado e insira um nome exclusivo do bucket do S3. Selecione Criar bucket do S3 quando terminar. Para acessar mais informações sobre como criar buckets, consulte Como criar um bucket do S3 no Guia do usuário do console do Amazon S3.
   - Para conectar o compartilhamento de arquivos a um bucket do S3 usando um nome de ponto de acesso, escolha o nome do ponto de acesso Amazon S3 na lista suspensa e insira o nome do ponto de acesso. Se você precisar criar um ponto de acesso, poderá optar por Criar um ponto de acesso do S3. Para receber mais instruções, consulte Criar um ponto de acesso no Guia do usuário do Amazon S3. Para acessar mais informações sobre pontos de acesso, consulte Gerenciar o acesso a dados com o recurso Pontos de Acesso Amazon S3 e Delegar o controle de acesso a pontos de acesso no Guia do usuário do Amazon S3.
   - Para conectar o compartilhamento de arquivos a um bucket do S3 usando um alias de ponto de acesso, escolha o alias do ponto de acesso Amazon S3 na lista suspensa e insira o alias do ponto de acesso. Se você precisar criar um ponto de acesso, poderá optar por Criar um

ponto de acesso do S3. Para receber mais instruções, consulte Criar um ponto de acesso no Guia do usuário do Amazon S3. Para acessar mais informações sobre aliases de ponto de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso no Guia do usuário do Amazon S3.

> **Note**
>
> Cada compartilhamento de arquivo só pode se conectar a um bucket do S3, mas vários compartilhamentos de arquivos podem se conectar ao mesmo bucket. Se você conectar mais de um compartilhamento de arquivos ao mesmo bucket, deverá configurar cada compartilhamento de arquivo para usar um prefixo de bucket do S3 exclusivo e não sobreposto para evitar conflitos. read/write
> O Gateway de Arquivos do S3 não oferecem suporte a buckets do Amazon S3 com pontos (`.`) no nome do bucket.
> Confirme se o nome do bucket está de acordo com as regras de nomenclatura de bucket no Amazon S3. Para obter mais informações, consulte as Regras para nomear buckets no Manual do usuário do Amazon Simple Storage Service.

8. (Opcional) Em Prefixo do bucket do S3, insira um prefixo para seu compartilhamento de arquivos a ser aplicado aos objetos que ele cria no Amazon S3. Os prefixos são uma maneira de organizar seus dados no S3, de forma semelhante aos diretórios em estruturas de arquivos tradicionais. Para acessar mais informações, consulte Organizar objetos usando prefixos no Guia de usuário do Amazon S3.

> **Note**
>
> - Se você conectar mais de um compartilhamento de arquivos ao mesmo bucket, deverá configurar cada compartilhamento de arquivo para usar um prefixo exclusivo e não sobreposto para evitar conflitos. read/write
> - O prefixo deve terminar com uma barra (/).
> - Depois que o compartilhamento de arquivos é criado, o prefixo não pode ser modificado nem excluído.

9. Em Região, escolha Região da AWS onde o endpoint S3 do seu bucket está localizado na lista suspensa. Esse campo aparece somente quando você especifica um ponto de acesso ou um bucket em outra conta para o bucket do S3.

10. Em Classe de armazenamento para novos objetos, escolha uma classe de armazenamento na lista suspensa. Para acessar mais informações sobre classes de armazenamento, consulte Usar as classes de armazenamento com um Gateway de Arquivos.
11. Em Perfil do IAM, faça o seguinte para configurar um perfil do IAM para seu compartilhamento de arquivos:

    - Para criar automaticamente um perfil do IAM com as permissões necessárias para que seu compartilhamento de arquivos funcione corretamente, escolha Criado pelo Storage Gateway na lista suspensa.
    - Para usar um perfil do IAM existente, escolha o nome do perfil na lista suspensa.
    - Para criar um perfil do IAM, escolha Criar um perfil. Para obter mais instruções, consulte Criação de uma função para delegar permissões a um AWS serviço no Guia do AWS Identity and Access Management usuário.

    Para acessar mais informações sobre como os perfis do IAM controlam o acesso entre seu compartilhamento de arquivos e o bucket do S3, consulte Conceder acesso a um bucket do Amazon S3.
12. Para Link privado, faça o seguinte somente se precisar configurar seu compartilhamento de arquivos para se comunicar AWS usando um endpoint privado em uma Virtual Private Cloud (VPC). Caso contrário, ignore essa etapa. Para obter mais informações, consulte O que é AWS PrivateLink? no AWS PrivateLink Guia.

    a. Selecione Usar endpoint da VPC.

    b. Em Identificar endpoints da VPC por, realize um dos seguintes procedimentos:

        - Selecione ID da endpoint da VPC e, depois, escolha o endpoint que você deseja usar na lista suspensa Endpoint da VPC.
        - Selecione o nome DNS e, depois, insira o nome DNS do endpoint que você deseja usar.
13. Em Criptografia, escolha o tipo de criptografia do lado do servidor que o compartilhamento de arquivos usará para os dados que ele armazena no Amazon S3:

    - Para usar a criptografia no lado do servidor, gerenciada com o Amazon S3 (SSE-S3), escolha Chaves gerenciadas com o S3 (SSE-S3).

      Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

- Para usar a criptografia do lado do servidor gerenciada com o AWS Key Management Service (SSE-KMS), escolha Chaves gerenciadas pelo KMS (SSE-KMS). Em Chave KMS primária, escolha uma chave AWS KMS existente ou escolha Criar uma nova chave KMS para criar uma nova chave KMS no console AWS Key Management Service ().AWS KMS

  Para obter mais informações sobre AWS KMS, consulte O que é o AWS Key Management Service? no Guia do AWS Key Management Service desenvolvedor.

- Para usar a criptografia de camada dupla do lado do servidor gerenciada com o AWS Key Management Service (DSSE-KMS), escolha Criptografia do lado do servidor de camada dupla com chaves (DSSE-KMS). AWS Key Management Service Em Chave KMS primária, escolha uma chave AWS KMS existente ou escolha Criar uma nova chave KMS para criar uma nova chave KMS no console AWS Key Management Service ().AWS KMS

  Para obter mais informações sobre o DSSE-KMS, consulte Usando criptografia de duas camadas no lado do servidor com AWS KMS chaves no Guia do usuário do Amazon Simple Storage Service.

  > **Note**
  >
  > Há cobranças adicionais pelo uso do DSSE-KMS e das chaves. AWS KMS Para obter mais informações, consulte Preços do AWS KMS.
  > Para especificar uma AWS KMS chave com um alias que não esteja listado ou para usar uma AWS KMS chave de uma AWS conta diferente, você deve usar o. AWS Command Line Interface As chaves do KMS assimétricas não são aceitas. Para obter mais informações, consulte Create NFSFile Share na Referência da API do AWS Storage Gateway.

> **Important**
>
> Seu compartilhamento de arquivos deve usar o mesmo tipo de criptografia que do bucket do Amazon S3 em que ele armazena seus dados.

14. Em Adivinhar tipos MIME, selecione Adivinhar tipo de mídia MIME para permitir que o Storage Gateway adivinhe o tipo de mídia para objetos enviados com base em suas extensões de arquivo.

15. Em Nome do compartilhamento de arquivos, insira um nome para seu compartilhamento de arquivos.

    > **Note**
    >
    > Um nome de compartilhamento de arquivo NFS válido só pode conter os seguintes caracteres: `a-z`, `A-Z`, `0-9`, `-`, `.` e `_`.

16. Em Eventos de upload, selecione Registrar um evento quando um arquivo for carregado com sucesso pelo gateway se quiser que seu gateway registre eventos de CloudWatch log ao carregar arquivos com sucesso no Amazon S3. O Atraso na notificação controla o atraso mínimo entre a operação de gravação mais recente do cliente e a geração da notificação de log `ObjectUploaded`. Como os clientes podem fazer muitas gravações pequenas em arquivos em pouco tempo, recomendamos definir esse parâmetro como o maior tempo possível a fim de evitar a geração de várias notificações para o mesmo arquivo em rápida sucessão. Para acessar mais informações, consulte Receber notificação de upload de arquivos.

    > **Note**
    >
    > Essa configuração não tem efeito no momento do upload do objeto para o S3, somente no momento da notificação.
    > Essa configuração não serve para especificar a hora exata em que a notificação será enviada. Em alguns casos, o gateway pode exigir mais do que o tempo de atraso especificado para gerar e enviar notificações.

    Quando terminar, escolha Próximo.

17.

18. Em Protocolo de compartilhamento de arquivos, escolha NFS.

19. Em Acesso de cliente, siga um destes procedimentos para especificar quais clientes NFS podem acessar seu compartilhamento de arquivos:

    - Para aceitar todas as conexões de entrada de clientes, selecione Todos os clientes NFS.
    - Para aceitar conexões de clientes de entrada somente de endereços IP específicos, selecione Clientes NFS específicos e escolha Adicionar um cliente. Em Clientes permitidos, especifique um endereço IP ou bloco CIDR válido a partir do qual aceitar conexões. Se você precisar especificar endereços IP adicionais, escolha Adicionar outro cliente.

> **Note**
>
> Recomendamos configurar a limitação do acesso ao seu compartilhamento de arquivos usando a opção Clientes NFS específicos. Se você não alterar, qualquer cliente em sua rede poderá acessar o compartilhamento de arquivos.

20. Em Tipo de acesso, selecione uma das seguintes opções:

    - Para permitir que os clientes leiam e gravem arquivos no compartilhamento de arquivos, selecione Leitura/gravação.
    - Para permitir que os clientes leiam arquivos, mas não gravem no compartilhamento de arquivos, selecione Somente leitura.

    > **Note**
    >
    > Para compartilhamentos de arquivos montados em um cliente Microsoft Windows, se você selecionar Somente leitura, provavelmente uma mensagem de erro será exibida. Ela indica que um erro inesperado está impedindo que a pasta seja criada. Você pode ignorar a mensagem.

21. Para Nível de acesso, escolha uma das seguinte opções:

    - Extermínio de raiz (padrão): o acesso para o superusuário remoto (raiz) é mapeado para o UID (65534) e o GID (65534).
    - Todo extermínio: todo o acesso de usuário é mapeado para o ID de usuário (UID) (65534) e o ID de grupo (GID) (65534).
    - Sem extermínio de raiz: o superusuário remoto (raiz) recebe acesso como raiz.

22. (Opcional) Em Atualização automática do cache do S3, escolha Definir intervalo de atualização do cache e defina o tempo em minutos ou dias para atualizar o cache do compartilhamento de arquivos usando tempo de vida (TTL). TTL é o intervalo desde a última atualização. Depois de decorrido o intervalo de TTL, o acesso a um diretório faz com que o Gateway de Arquivos atualize o conteúdo desse diretório pelo bucket do Amazon S3.

> **Note**
>
> Definir esse valor como menos de trinta minutos pode afetar negativamente a performance do gateway em situações em que grandes números de objetos do Amazon S3 são frequentemente criados ou excluídos.

23. Em Padrões de metadados de arquivo, selecione Alterar metadados padrão para objetos do S3 que não foram criados ou modificados pelo seu gateway se você quiser que o gateway aplique metadados de arquivo (incluindo permissões Unix) a objetos preexistentes que ele descobre no seu bucket do S3. Especifique as permissões de diretório, permissões de arquivo, ID de usuário e ID de grupo que você deseja aplicar nos campos correspondentes.
24. Em Propriedade e permissões do arquivo, selecione Conceder ao proprietário do bucket do S3 a propriedade total dos arquivos criados pelo gateway, incluindo permissões de leitura, gravação, edição e exclusão, se você quiser que a AWS conta proprietária do bucket do S3 tenha controle total de todos os objetos gravados no bucket pelo seu compartilhamento de arquivos.

    Quando terminar, escolha Próximo.
25. Analise a configuração de compartilhamento de arquivos. Escolha Editar para modificar as configurações de qualquer seção que você deseje alterar. Quando terminar, escolha Create (Criar).

Depois que seu compartilhamento de arquivos NFS for criado, você poderá ver suas configurações no console do AWS Storage Gateway na guia Detalhes do compartilhamento de arquivos. Para receber instruções sobre como montar seu compartilhamento de arquivos, consulte Montar seu compartilhamento de arquivos NFS em seu cliente.

Criar um compartilhamento de arquivos SMB

O protocolo Server Message Block (SMB) está profundamente integrado ao pacote de produtos Microsoft Windows e continua sendo o protocolo padrão de compartilhamento de arquivos para sistemas operacionais Windows. O processo de comunicação cliente-servidor é semelhante ao NFS em alto nível, mas há diferenças em alguns detalhes e mecanismos operacionais. Por exemplo, no SMB, os sistemas de arquivos não são montados no cliente SMB local. Em vez disso, um compartilhamento de rede hospedado no servidor SMB é acessado por meio de um caminho de rede.

Os tópicos nesta seção explicam vários métodos para criar um compartilhamento de arquivos SMB para seu Gateway de Arquivos.

Sumário

Criar um compartilhamento de arquivos SMB usando a configuração padrão

Esta seção explica como criar um compartilhamento de arquivos do protocolo Server Message Block (SMB) usando configurações padrão predefinidas. Use esse método para implantações básicas, uso pessoal, testes ou como uma forma de implantar rapidamente vários compartilhamentos de arquivos que você planeja editar e personalizar posteriormente. Para ver uma lista das configurações padrão para compartilhamentos de arquivos que você cria usando esse procedimento, consulte Configurações padrão para compartilhamentos de arquivos SMB. Se você precisar de um controle mais granular ou quiser usar configurações avançadas para seu compartilhamento de arquivos, consulte Criar um compartilhamento de arquivos SMB com uma configuração personalizada.

> **Note**
>
> Se você precisar conectar seu compartilhamento de arquivos ao Amazon S3 por meio de uma nuvem privada virtual (VPC), deverá seguir o procedimento de configuração personalizado. Não é possível editar configurações de VPC para um compartilhamento de arquivos depois de criá-lo.

> **Important**
>
> Usar o versionamento do S3, a replicação entre regiões ou o utilitário Rsync ao fazer upload de dados de um Gateway de Arquivos pode ter implicações de custo significativas. Para acessar mais informações, consulte Evitar custos imprevistos ao fazer upload de dados do Gateway de Arquivos.

Pré-requisitos

Antes de criar o compartilhamento de arquivos, faça o seguinte:

- Configure as definições de segurança SMB para o Gateway de Arquivos. Para receber instruções, consulte Definir um nível de segurança para seu gateway.
- Configurar o Microsoft Active Directory ou um acesso de convidado para a autenticação. Para receber instruções, consulte Usar o Active Directory para autenticar usuários ou Conceder acesso de convidado ao seu compartilhamento de arquivos.
- Certifique-se de que as portas necessárias estejam abertas em seu grupo de segurança. Para acessar mais informações, consulte Requisitos de porta.

Para criar um compartilhamento de arquivos SMB usando a configuração padrão:

1. Abra o console do AWS Storage Gateway em https://console.aws.amazon.com/storagegateway/casa/ e escolha Compartilhamentos de arquivos no painel de navegação esquerdo.
2. Escolha Create file share (Criar compartilhamento de arquivos).
3. Em Gateway, escolha o Gateway de Arquivos do Amazon S3 na lista suspensa.
4. Em Protocolo de compartilhamento de arquivos, escolha SMB.
5. Em Bucket do S3, siga um destes procedimentos:

   - Escolha um bucket do Amazon S3 existente na sua conta na lista suspensa.
   - Escolha Um bucket em outra conta na lista suspensa e insira o nome do bucket em Nome do bucket entre contas.
   - Escolha Criar bucket do S3 e, depois, selecione a Região da AWS onde o endpoint do Amazon S3 para seu novo bucket está localizado e insira um nome exclusivo do bucket do S3. Selecione Criar bucket do S3 quando terminar.

     Para acessar mais informações sobre como um bucket, consulte Como criar um bucket do S3 no Guia do usuário do Amazon S3.

> **Note**
>
> O Gateway de Arquivos do S3 não oferecem suporte a buckets do Amazon S3 com pontos (`.`) no nome do bucket.

Confirme se o nome do bucket está de acordo com as regras de nomenclatura de bucket no Amazon S3. Para obter mais informações, consulte as Regras para nomear buckets no Manual do usuário do Amazon Simple Storage Service.

6. Autenticação do usuário, escolha o método de autenticação desejado na lista suspensa:

   - Para usar o Microsoft Active Directory corporativo ou AWS Managed Microsoft AD para autenticar o acesso do usuário ao seu compartilhamento de arquivos SMB, escolha Active Directory. Seu gateway deve estar associado a um domínio para usar esse método. Para acessar mais informações, consulte Usar o Active Directory para autenticar usuários.

     > **Note**
     >
     > 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 AWS Managed Microsoft AD o grupo de segurança à instância `_workspaceMembers` 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.

     Se Status de associação indicar que seu gateway já está associado a um domínio do Active Directory, vá para a próxima etapa. Caso contrário, faça o seguinte:

     1. Selecione Configurar.
     2. Em Domínio, insira o nome do domínio do Active Directory ao qual você deseja associar o gateway.
     3. Digite o nome de usuário e a senha que o gateway usará para ingressar no domínio.
     4. (Opcional) Em Unidade organizacional (UO), insira a UO designada que seu Active Directory usa para novos objetos de computador.
     5. (Opcional) Em Controladores de domínio (DC), insira o nome do DC por meio do qual seu gateway se conectará ao Active Directory. Você pode deixar esse campo em branco para permitir que o DNS selecione automaticamente um DC.
     6. Escolha Ingressar no Active Directory.

> **Note**
>
> A associação a um domínio cria uma conta do Active Directory no contêiner padrão (que não é uma unidade organizacional) 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, você precisará 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.

- Para conceder acesso protegido por senha a qualquer pessoa que forneça a senha de convidado configurada, escolha Acesso de convidado. Seu Gateway de Arquivos não precisa fazer parte de um domínio do Microsoft Active Directory para usar esse método. Escolha Configurar para especificar sua senha de convidado e selecione Salvar.

7. Analise as configurações em Configuração padrão e escolha Criar compartilhamento de arquivos para criar seu compartilhamento de arquivos SMB usando a configuração padrão.

Depois que seu compartilhamento de arquivos SMB for criado, você poderá ver suas configurações no console do AWS Storage Gateway na guia Detalhes do compartilhamento de arquivos. Para acessar informações sobre como montar seu compartilhamento de arquivos, consulte Montar seu compartilhamento de arquivos SMB em seu cliente.

Configurações padrão para compartilhamentos de arquivos SMB

As configurações a seguir se aplicam a todos os novos compartilhamentos de arquivos SMB criados usando a configuração padrão. Depois de criar um compartilhamento de arquivos, você pode selecioná-lo na página Compartilhamentos de arquivos no console do AWS Storage Gateway para ver detalhes sobre sua configuração.

> **Important**
>
> A configuração padrão de compartilhamento de arquivos SMB fornece controle total de arquivos e permissões de acesso ao proprietário do bucket do S3 que está associado ao compartilhamento de arquivos, mesmo que o bucket seja de propriedade de uma conta diferente da Amazon Web Services. Para acessar mais informações sobre como usar seu

compartilhamento de arquivos para acessar objetos em um bucket que pertence a outra conta, consulte Usar um compartilhamento de arquivos para acesso entre contas.

Configuração	Valor padrão	Observações
Localização do Amazon S3	O compartilhamento de arquivos se conecta diretamente ao bucket do Amazon S3 e tem o mesmo nome que do bucket. Seu gateway usa esse bucket para armazenar e recuperar arquivos.	O nome não inclui prefixo.
AWS PrivateLink para S3	O compartilhamento de arquivos não se conecta ao Amazon S3 por meio de um endpoint em sua nuvem privada virtual (VPC).	
Notificação de upload de arquivos	Desativado	
Classe de armazenamento para novos objetos	Amazon S3 Standard	Isso permite armazenar os dados de objetos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Para acessar mais informações sobre a classe de armazenamento Amazon S3 Standard, consulte Classes de armazenamento para objetos acessados com frequência no Guia do usuário do Amazon Simple Storage Service.

Configuração	Valor padrão	Observações
Criptografia	Criptografia do lado do servidor com chaves gerenciadas pelo S3 (SSE-S3)	Todos os objetos do Amazon S3 dos quais seu Gateway de Arquivos do S3 faz upload, atualiza ou modifica são criptografados por padrão com criptografia do lado do servidor usando chaves gerenciadas pelo Amazon S3.
Metadados do objeto	Adivinhar o tipo MIME	Isso permite ao Storage Gateway adivinhar o tipo Multipurpose Internet Mail Extension (MIME) dos objetos cujo upload foi feito com base nas extensões de arquivo. Essa opção exige que as listas de controle de acesso (ACLs) estejam ativadas para o bucket do Amazon S3 associado ao seu compartil hamento de arquivos. Se ACLs são desativado, o compartilhamento de arquivos não pode acessar o bucket do Amazon S3 e permanece no estado Indisponível indefinid amente.

Configuração	Valor padrão	Observações
Enumeração baseada em acesso	Não ativada	Os arquivos e pastas no compartilhamento de arquivos são visíveis para todos os usuários durante a enumeração do diretório. A enumeração baseada em acesso é um sistema que filtra a enumeração de arquivos e pastas em um compartilhamento de arquivos SMB com base no acesso do compartilhamento listas de controle (ACLs).
Habilitar pagamentos pelo solicitante	Desativado	Para obter mais informações, consulte Buckets de pagamento pelo solicitante.
Bloqueio oportunista	Ativado	Permite que o compartilhamento de arquivos use o bloqueio oportunista para otimizar a estratégia de armazenamento em buffer de arquivos. Na maioria dos casos, a ativação do bloqueio oportunista melhora a performance, particularmente no que diz respeito aos menus de contexto do Windows.
Logs de auditoria	Desativado	O registro em um Amazon CloudWatch grupo é desativado por padrão.

Configuração	Valor padrão	Observações
Forçar distinção entre maiúsculas e minúsculas	Desativado	Permite que o cliente controle a distinção entre maiúsculas e minúsculas.
Acessar o bucket do S3	Criar um perfil do IAM	A opção padrão permite que o Gateway de Arquivos acesse um novo perfil e política de acesso do IAM em seu nome.

Criar um compartilhamento de arquivos SMB com configuração personalizada

Use o procedimento a seguir para criar um compartilhamento de arquivos Server Message Block (SMB) com configuração personalizada. Para criar um compartilhamento de arquivos SMB usando as configurações padrão, consulte Criar um compartilhamento de arquivos SMB usando a configuração padrão.

> **Important**
>
> Usar o versionamento do S3, a replicação entre regiões ou o utilitário Rsync ao fazer upload de dados de um Gateway de Arquivos pode ter implicações de custo significativas. Para acessar mais informações, consulte Evitar custos imprevistos ao fazer upload de dados do Gateway de Arquivos.

Pré-requisitos

Antes de criar o compartilhamento de arquivos, faça o seguinte:

- Configure as definições de segurança SMB para o Gateway de Arquivos. Para receber instruções, consulte Definir um nível de segurança para seu gateway.
- Configurar o Microsoft Active Directory ou um acesso de convidado para a autenticação. Para receber instruções, consulte Usar o Active Directory para autenticar usuários ou Conceder acesso de convidado ao seu compartilhamento de arquivos.

- Certifique-se de que as portas necessárias estejam abertas em seu grupo de segurança. Para acessar mais informações, consulte Requisitos de porta.

Como criar um compartilhamento de arquivos SMB com configurações personalizadas

1. Abra o console do AWS Storage Gateway em https://console.aws.amazon.com/storagegateway/casa/ e escolha Compartilhamentos de arquivos no painel de navegação esquerdo.
2. Escolha Create file share (Criar compartilhamento de arquivos).
3. Escolha Personalizar configuração. Você pode ignorar os outros campos desta página por enquanto. Será solicitado que você defina as configurações de gateway, protocolo e armazenamento nas etapas subsequentes.
4. Em Gateway, escolha o Gateway de Arquivos do Amazon S3 na lista suspensa.
5. Para o grupo de CloudWatch registros, escolha uma das seguintes opções na lista suspensa:

   - Para desativar o registro em log desse compartilhamento de arquivos, escolha Desativar registro em log.
   - Para criar automaticamente um grupo de logs para esse compartilhamento de arquivos, escolha Criado pelo Storage Gateway.
   - Para enviar notificações de integridade e recursos desse compartilhamento de arquivos a um grupo de logs existente, escolha o grupo desejado na lista.

   Para acessar mais informações sobre logs de auditoria, consulte Noções básicas dos logs de auditoria do Gateway de Arquivos do S3.
6. (Opcional) Em Tags: opcional, escolha Adicionar nova tag e insira uma chave e um valor para o seu compartilhamento de arquivos. Tag é um par de chave-valor que diferencia maiúsculas de minúsculas e ajuda você a categorizar os recursos do Storage Gateway. Adicionar tags pode facilitar a filtragem e a pesquisa do seu compartilhamento de arquivos. Repita essa etapa para adicionar até cinquenta tags.

   Quando terminar, escolha Próximo.
7. Em Bucket do S3, faça o seguinte para especificar onde armazenar e recuperar arquivos:

   - Para conectar o compartilhamento de arquivos diretamente a um bucket do S3 existente em sua conta da Amazon Web Services, escolha o nome do bucket na lista suspensa.

- Para conectar o compartilhamento de arquivos a um bucket existente do S3 pertencente a uma conta da Amazon Web Services diferente da que você usa para criar o compartilhamento de arquivos, escolha Um bucket em outra conta na lista suspensa e insira o nome do bucket entre contas.
- Para conectar o compartilhamento de arquivos a um novo bucket do S3, escolha Criar um bucket do S3 e, depois, escolha a região onde o endpoint do Amazon S3 para seu novo bucket está localizado e insira um nome exclusivo do bucket do S3. Selecione Criar bucket do S3 quando terminar. Para acessar mais informações sobre como criar buckets, consulte Como criar um bucket do S3 no Guia do usuário do console do Amazon S3.
- Para conectar o compartilhamento de arquivos a um bucket do S3 usando um nome de ponto de acesso, escolha o nome do ponto de acesso Amazon S3 na lista suspensa e insira o nome do ponto de acesso. Se você precisar criar um ponto de acesso, poderá optar por Criar um ponto de acesso do S3. Para receber mais instruções, consulte Criar um ponto de acesso no Guia do usuário do Amazon S3. Para acessar mais informações sobre pontos de acesso, consulte Gerenciar o acesso a dados com o recurso Pontos de Acesso Amazon S3 e Delegar o controle de acesso a pontos de acesso no Guia do usuário do Amazon S3.
- Para conectar o compartilhamento de arquivos a um bucket do S3 usando um alias de ponto de acesso, escolha o alias do ponto de acesso Amazon S3 na lista suspensa e insira o alias do ponto de acesso. Se você precisar criar um ponto de acesso, poderá optar por Criar um ponto de acesso do S3. Para receber mais instruções, consulte Criar um ponto de acesso no Guia do usuário do Amazon S3. Para acessar mais informações sobre aliases de ponto de acesso, consulte Usar um alias em estilo de bucket para seu ponto de acesso no Guia do usuário do Amazon S3.

> **Note**
>
> Cada compartilhamento de arquivo só pode se conectar a um bucket do S3, mas vários compartilhamentos de arquivos podem se conectar ao mesmo bucket. Se você conectar mais de um compartilhamento de arquivos ao mesmo bucket, deverá configurar cada compartilhamento de arquivo para usar um prefixo de bucket do S3 exclusivo e não sobreposto para evitar conflitos. read/write
> O Gateway de Arquivos do S3 não oferecem suporte a buckets do Amazon S3 com pontos (`.`) no nome do bucket.

Confirme se o nome do bucket está de acordo com as regras de nomenclatura de bucket no Amazon S3. Para obter mais informações, consulte as Regras para nomear buckets no Manual do usuário do Amazon Simple Storage Service.

8. (Opcional) Em Prefixo do bucket do S3, insira um prefixo para seu compartilhamento de arquivos a ser aplicado aos objetos que ele cria no Amazon S3. Os prefixos são uma maneira de organizar seus dados no S3, de forma semelhante aos diretórios em estruturas de arquivos tradicionais. Para acessar mais informações, consulte Organizar objetos usando prefixos no Guia de usuário do Amazon S3.

   Note

   - Se você conectar mais de um compartilhamento de arquivos ao mesmo bucket, deverá configurar cada compartilhamento de arquivo para usar um prefixo exclusivo e não sobreposto para evitar conflitos. read/write
   - O prefixo deve terminar com uma barra (/).
   - Depois que o compartilhamento de arquivos é criado, o prefixo não pode ser modificado nem excluído.

9. Em Região, escolha Região da AWS onde o endpoint S3 do seu bucket está localizado na lista suspensa. Esse campo aparece somente quando você especifica um ponto de acesso ou um bucket em outra conta para o bucket do S3.
10. Em Classe de armazenamento para novos objetos, escolha uma classe de armazenamento na lista suspensa. Para acessar mais informações sobre classes de armazenamento, consulte Usar as classes de armazenamento com um Gateway de Arquivos.
11. Em Perfil do IAM, faça o seguinte para configurar um perfil do IAM para seu compartilhamento de arquivos:

    - Para criar automaticamente um perfil do IAM com as permissões necessárias para que seu compartilhamento de arquivos funcione corretamente, escolha Criado pelo Storage Gateway na lista suspensa.
    - Para usar um perfil do IAM existente, escolha o nome do perfil na lista suspensa.
    - Para criar um perfil do IAM, escolha Criar um perfil. Para obter mais instruções, consulte Criação de uma função para delegar permissões a um AWS serviço no Guia do AWS Identity and Access Management usuário.

Para acessar mais informações sobre como os perfis do IAM controlam o acesso entre seu compartilhamento de arquivos e o bucket do S3, consulte Conceder acesso a um bucket do Amazon S3.

12. Para Link privado, faça o seguinte somente se precisar configurar seu compartilhamento de arquivos para se comunicar AWS usando um endpoint privado em uma Virtual Private Cloud (VPC). Caso contrário, ignore essa etapa. Para obter mais informações, consulte O que é AWS PrivateLink? no AWS PrivateLink Guia.

    a. Selecione Usar endpoint da VPC.

    b. Em Identificar endpoints da VPC por, realize um dos seguintes procedimentos:

    - Selecione ID da endpoint da VPC e, depois, escolha o endpoint que você deseja usar na lista suspensa Endpoint da VPC.
    - Selecione o nome DNS e, depois, insira o nome DNS do endpoint que você deseja usar.

13. Em Criptografia, escolha o tipo de chaves de criptografia a serem usadas para criptografar objetos que o Gateway de Arquivos armazena no Amazon S3:

    - Para usar a criptografia no lado do servidor, gerenciada com o Amazon S3 (SSE-S3), escolha Chaves gerenciadas com o S3 (SSE-S3).

      Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

    - Para usar a criptografia do lado do servidor gerenciada com o AWS Key Management Service (SSE-KMS), escolha Chaves gerenciadas pelo KMS (SSE-KMS). Em Chave KMS primária, escolha uma chave AWS KMS existente ou escolha Criar uma nova chave KMS para criar uma nova chave KMS no console AWS Key Management Service ().AWS KMS

      Para obter mais informações sobre AWS KMS, consulte O que é o AWS Key Management Service? no Guia do AWS Key Management Service desenvolvedor.

    - Para usar a criptografia de camada dupla do lado do servidor gerenciada com o AWS Key Management Service (DSSE-KMS), escolha Criptografia do lado do servidor de camada dupla com chaves (DSSE-KMS). AWS Key Management Service Em Chave KMS primária, escolha uma chave AWS KMS existente ou escolha Criar uma nova chave KMS para criar uma nova chave KMS no console AWS Key Management Service ().AWS KMS

Para obter mais informações sobre o DSSE-KMS, consulte Usando criptografia de duas camadas no lado do servidor com AWS KMS chaves no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Há custos adicionais pelo uso do DSSE-KMS e das chaves. AWS KMS Para obter mais informações, consulte Preços do AWS KMS.
> Para especificar uma AWS KMS chave com um alias que não esteja listado ou para usar uma AWS KMS chave de uma AWS conta diferente, você deve usar o. AWS Command Line Interface As chaves do KMS assimétricas não são aceitas. Para obter mais informações, consulte Create SMBFile Share na Referência da API do AWS Storage Gateway.

> **Important**
>
> Seu compartilhamento de arquivos deve usar o mesmo tipo de criptografia que do bucket do Amazon S3 em que ele armazena seus dados.

14. Em Adivinhar tipos MIME, selecione Adivinhar tipo de mídia MIME para permitir que o Storage Gateway adivinhe o tipo de Internet Mail Extension (MIME) para objetos enviados com base em suas extensões de arquivo.
15. Em Nome do compartilhamento de arquivos, insira um nome para seu compartilhamento de arquivos.

> **Note**
>
> Um nome de compartilhamento de arquivos SMB válido não pode conter os seguintes caracteres: `[,],#,;,<,>,:,",\,/,|,?,*,+` ou caracteres de controle ASCII `1-31`.

16. Em Eventos de upload, selecione Registrar um evento quando um arquivo for carregado com sucesso pelo gateway se quiser que seu gateway registre eventos de CloudWatch log ao carregar arquivos com sucesso no Amazon S3. O Atraso na notificação controla o atraso entre a operação de gravação mais recente do cliente e a geração da notificação de log `ObjectUploaded`. Como os clientes podem fazer muitas gravações pequenas em arquivos em pouco tempo, recomendamos definir esse parâmetro como o maior tempo possível a fim de

evitar a geração de várias notificações para o mesmo arquivo em rápida sucessão. Para acessar mais informações, consulte Receber notificação de upload de arquivos.

> **Note**
>
> Essa configuração não tem efeito no momento do upload do objeto para o S3, somente no momento da notificação.
> Essa configuração não serve para especificar a hora exata em que a notificação será enviada. Em alguns casos, o gateway pode exigir mais do que o tempo de atraso especificado para gerar e enviar notificações.

Quando terminar, escolha Próximo.

17. Em Protocolo de compartilhamento de arquivos, escolha SMB.
18. Em Autenticação do usuário, escolha o método de autenticação desejado na lista suspensa:

    - Para usar o Microsoft Active Directory corporativo ou AWS Managed Microsoft AD para autenticar o acesso do usuário ao seu compartilhamento de arquivos SMB, escolha Active Directory. Seu gateway deve estar associado a um domínio para usar esse método. Para acessar mais informações, consulte Usar o Active Directory para autenticar usuários.

      > **Note**
      >
      > 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 AWS Managed Microsoft AD o grupo de segurança à instância `_workspaceMembers` 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.

      Se Status de associação indicar que seu gateway já está associado a um domínio do Active Directory, vá para a próxima etapa. Caso contrário, faça o seguinte:

      1. Selecione Configurar.

2. Em Domínio, insira o nome do domínio do Active Directory ao qual você deseja associar o gateway.
3. Digite o nome de usuário e a senha que o gateway usará para ingressar no domínio.
4. (Opcional) Em Unidade organizacional (UO), insira a UO designada que seu Active Directory usa para novos objetos de computador.
5. (Opcional) Em Controladores de domínio (DC), insira o nome do DC por meio do qual seu gateway se conectará ao Active Directory. Você pode deixar esse campo em branco para permitir que o DNS selecione automaticamente um DC.
6. Escolha Ingressar no Active Directory.

> **Note**
>
> A associação a um domínio cria uma conta do Active Directory no contêiner padrão (que não é uma unidade organizacional) 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, você precisará 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.

- Para conceder acesso protegido por senha a qualquer pessoa que forneça a senha de convidado configurada, escolha Acesso de convidado. Seu Gateway de Arquivos não precisa fazer parte de um domínio do Microsoft Active Directory para usar esse método. Escolha Configurar para especificar sua senha de convidado e selecione Salvar.

19. Em Acesso de usuário, siga um destes procedimentos para especificar quais clientes SMB podem acessar seu compartilhamento de arquivos:

    - Para conceder acesso a todos os usuários que se autenticaram com êxito por meio do Active Directory, selecione Todos os usuários autenticados pelo AD.
    - Para permitir ou negar acesso a usuários ou grupos específicos, escolha Usuários ou grupos específicos autenticados pelo AD e faça o seguinte:
        - Em Usuários e grupos permitidos, escolha Adicionar usuário permitido ou Adicionar grupo permitido e insira um usuário ou grupo do Active Directory ao qual você deseja permitir o acesso ao compartilhamento de arquivos. Repita esse processo para permitir quantos usuários e grupos forem necessários.

- Em Usuários e grupos negados, escolha Adicionar usuário negado ou Adicionar grupo negado e insira um usuário ou grupo do Active Directory ao qual você deseja negar o acesso ao compartilhamento de arquivos. Repita esse processo para negar quantos usuários e grupos forem necessários.

> **Note**
>
> A seção Acesso ao compartilhamento de arquivos para usuários e grupos será exibida somente se a autenticação do usuário estiver definida como Active Directory.
> Ao especificar usuários ou grupos, não inclua o domínio. O nome de domínio é inferido pela associação do gateway no Active Directory específico no qual ele ingressou.

20. (Opcional) Em Usuários administradores, insira uma lista separada por vírgulas de usuários e grupos do Active Directory. Os usuários administradores recebem privilégios para atualizar as listas de controle de acesso (ACLs) em todos os arquivos e pastas no compartilhamento de arquivos. Grupos devem receber um prefixo como o caractere `@`, por exemplo `@group1`.
21. Em Tipo de acesso, selecione uma das seguintes opções:

    - Para permitir que os clientes leiam e gravem arquivos no compartilhamento de arquivos, selecione Leitura/gravação.
    - Para permitir que os clientes leiam arquivos, mas não gravem no compartilhamento de arquivos, selecione Somente leitura.

    > **Note**
    >
    > Para compartilhamentos de arquivos montados em um cliente Microsoft Windows, se você selecionar Somente leitura, provavelmente uma mensagem de erro será exibida. Ela indica que um erro inesperado está impedindo que a pasta seja criada. Você pode ignorar a mensagem.

22. Em Controle de acesso a arquivos e diretórios, escolha uma das seguintes opções:

    - Selecione Lista de controles de acesso do Windows para definir permissões detalhadas em arquivos e pastas no seu compartilhamento de arquivos SMB. Para obter mais informações, consulte Usando o Microsoft Windows ACLs para controlar o acesso a um compartilhamento de arquivos SMB.

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

23. Em Enumeração baseada em acesso, faça o seguinte:

- Para tornar os arquivos e pastas no compartilhamento visíveis somente para usuários com acesso de leitura, selecione Ocultar arquivos e diretórios nos quais o usuário não tenha permissão.
- Para tornar os arquivos e pastas no compartilhamento visíveis para todos os usuários durante a enumeração do diretório, não marque a caixa de seleção.

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

24. Para ver as opções de acesso ao arquivo, selecione uma das seguintes opções:

- Para otimizar a estratégia de armazenamento em buffer de arquivos do compartilhamento de arquivos usando bloqueio oportunista, selecione Bloqueio oportunista. Na maioria dos casos, a ativação do bloqueio oportunista melhora a performance, particularmente no que diz respeito aos menus de contexto do Windows.
- Para permitir que o gateway, em vez do cliente SMB, controle a distinção entre maiúsculas e minúsculas no nome do arquivo, selecione Forçar distinção entre maiúsculas e minúsculas.
- Para desativar as duas configurações, selecione Nenhuma.

> **Note**
>
> Para evitar conflitos de acesso a arquivos, essas configurações são mutuamente exclusivas e não podem ser ativadas ao mesmo tempo.

25. (Opcional) Em Atualização automática do cache do S3, escolha Definir intervalo de atualização do cache e defina o tempo em minutos ou dias para atualizar o cache do compartilhamento de arquivos usando tempo de vida (TTL). TTL é o intervalo desde a última atualização. Depois de decorrido o intervalo de TTL, o acesso a um diretório faz com que o Gateway de Arquivos atualize o conteúdo desse diretório pelo bucket do Amazon S3.

> **Note**
>
> Definir esse valor como menos de trinta minutos pode afetar negativamente a performance do gateway em situações em que grandes números de objetos do Amazon S3 são frequentemente criados ou excluídos.

26. Em Propriedade e permissões do arquivo, selecione Conceder ao proprietário do bucket do S3 a propriedade total dos arquivos criados pelo gateway, incluindo permissões de leitura, gravação, edição e exclusão, se você quiser que a AWS conta proprietária do bucket do S3 tenha controle total de todos os objetos gravados no bucket pelo seu compartilhamento de arquivos.

    Quando terminar, escolha Próximo.
27. Analise a configuração de compartilhamento de arquivos. Escolha Editar para modificar as configurações de qualquer seção que você deseje alterar. Quando terminar, escolha Create (Criar).

Depois que seu compartilhamento de arquivos SMB for criado, você poderá ver suas configurações no console do AWS Storage Gateway na guia Detalhes do compartilhamento de arquivos. Para receber instruções sobre como montar seu compartilhamento de arquivos, consulte Montar seu compartilhamento de arquivos SMB em seu cliente.

Copiar um compartilhamento de arquivos

> **Note**
>
> O recurso de compartilhamento de cópia de arquivos está disponível somente por meio do console do Storage Gateway. Não há comando de AWS CLI ou ação de API correspondente para esse recurso.

Você pode usar o console do Storage Gateway para copiar um compartilhamento de arquivos NFS ou SMB existente para um gateway diferente. A cópia de um compartilhamento de arquivos cria um novo compartilhamento de arquivos no gateway de destino que aponta para o mesmo bucket do Amazon S3 que o compartilhamento de arquivos de origem, preservando a maioria das configurações do compartilhamento original. O objetivo principal é auxiliar nas migrações de gateway, permitindo que você mova um compartilhamento de arquivos para um gateway substituto

sem recriar manualmente sua configuração. Depois de verificar se o compartilhamento de arquivos copiados está funcionando corretamente no novo gateway, você deve excluir o compartilhamento de arquivos original do gateway de origem.

Considerações

Antes de copiar um compartilhamento de arquivos, considere o seguinte:

- O gateway de destino deve estar em um estado Ativo.
- Os gateways de origem e destino devem ser gateways do Amazon S3 File Gateway. Você não pode copiar compartilhamentos de arquivos entre diferentes tipos de gateway.
- O compartilhamento de arquivos copiados aponta para o mesmo bucket do Amazon S3 da origem. Não recomendamos manter os dois compartilhamentos de arquivos ativamente por um longo período. Gravar no mesmo bucket do Amazon S3 a partir de vários gateways simultaneamente pode levar a inconsistências de dados, conflitos de cache e comportamento inesperado. Depois de confirmar que o compartilhamento de arquivos copiados está funcionando corretamente, exclua o compartilhamento de arquivos de origem.
- A operação de cópia preserva o protocolo de compartilhamento de arquivos (NFS ou SMB). Você não pode alterar o tipo de protocolo durante a cópia.
- Se o compartilhamento do arquivo de origem usar uma função do IAM para acesso ao bucket do Amazon S3, você pode escolher usar a mesma função para o compartilhamento de arquivos copiados, selecionar uma função existente diferente ou fazer com que o console crie uma nova função automaticamente.
- Se o compartilhamento do arquivo de origem tiver o monitoramento de grupos de CloudWatch registros configurado, você poderá optar por usar o mesmo grupo de registros, selecionar um grupo de registros diferente ou fazer com que o console crie um novo grupo de registros automaticamente.
- Se você estiver copiando um compartilhamento de arquivos SMB entre gateways associados a diferentes domínios do Active Directory ou entre um gateway usando a autenticação do Active Directory e outro usando acesso de convidado, revise suas configurações de acesso SMB após a conclusão da cópia para garantir que as permissões de acesso estejam configuradas corretamente.
- Se os gateways de origem e destino tiverem configurações de VPC diferentes (por exemplo, um gateway é ativado em uma VPC e o outro não), o compartilhamento de arquivos copiados usa a configuração de rede do gateway de destino.

> **Important**
>
> Ao copiar um compartilhamento de arquivos SMB, as listas de controle de acesso (ACLs) no nível raiz não são copiadas para o novo compartilhamento de arquivos. O compartilhamento de arquivos copiados é criado com ACLs raiz padrão. Se você configurou ACLs raiz personalizadas no compartilhamento de arquivos de origem, deverá reconfigurá-las manualmente no compartilhamento de arquivos copiados após a conclusão da cópia.

Copiar um compartilhamento de arquivos para outro gateway

Para copiar um compartilhamento de arquivos usando o console do Storage Gateway

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, escolha Compartilhamentos de arquivos.
3. Selecione o compartilhamento de arquivos que você deseja copiar.
4. No menu Ações, escolha Copiar compartilhamento de arquivos para outro gateway.
5. Em Gateway, selecione o gateway de destino em que você deseja criar a cópia.
6. Para a função do IAM, escolha uma das seguintes opções:
   - Use a mesma função do IAM — usa a mesma função do IAM que o compartilhamento do arquivo de origem. Escolha essa opção se o gateway de destino precisar usar as mesmas permissões para acessar o bucket do Amazon S3.
   - Selecione uma função do IAM existente — Escolha uma função do IAM diferente na lista. Certifique-se de que a função conceda as permissões necessárias do Amazon S3.
   - Auto-generate uma nova função do IAM — O console cria uma nova função do IAM com as permissões necessárias para o bucket do Amazon S3.
7. Para Grupo de registros, escolha uma das seguintes opções:
   - Use o mesmo grupo de registros — envia registros de saúde para o mesmo grupo de CloudWatch registros do compartilhamento do arquivo de origem.
   - Selecionar um grupo de registros existente — Escolha um grupo de CloudWatch registros diferente na lista.
   - Auto-generate um novo grupo de registros — O console cria um novo grupo de CloudWatch registros para o compartilhamento de arquivos copiados.

8. Escolha Copiar compartilhamento de arquivos.

O novo compartilhamento de arquivos aparece na lista de compartilhamentos de arquivos com o status Criando. Depois que o compartilhamento estiver disponível, você poderá montá-lo em seus clientes usando o mesmo protocolo do compartilhamento de origem.

Configurações preservadas durante a cópia

Quando você copia um compartilhamento de arquivos, as seguintes configurações são transferidas do compartilhamento do arquivo de origem para a nova cópia:

- Nome e prefixo do bucket Amazon S3
- Classe de armazenamento
- Configurações de criptografia de objetos (SSE-S3 SSE-KMS, ou DSSE-KMS)
- Protocolo de compartilhamento de arquivos (NFS ou SMB)
- Configurações de atualização do cache
- Configurações do Squash e acesso ao cliente (compartilhamentos de arquivos NFS)
- Configurações de acesso SMB, incluindo método de autenticação, visibilidade do compartilhamento de arquivos e enumeração baseada em acesso (compartilhamentos de arquivos SMB)
- Usuários e grupos permitidos e negados (compartilhamentos de arquivos SMB)

As configurações a seguir não são copiadas e usam a configuração ou os padrões do gateway de destino:

- Configuração de rede de gateway (endpoint VPC, endpoint público)
- Associação ao domínio do Active Directory (usa a configuração AD do gateway de destino)
- Limites de taxa de largura de banda (usa os limites do gateway de destino)
- Root-level ACLs (compartilhamentos de arquivos SMB — o compartilhamento copiado é criado com ACLs raiz padrão)

Montar e usar seu compartilhamento de arquivos

Os tópicos desta seção fornecem instruções sobre como montar seu compartilhamento de arquivos em seu cliente, usar seu compartilhamento de arquivos, testar seu gateway de arquivos e limpar recursos que não são mais necessários, como gateways, instâncias do Amazon EC2 ou VMs locais que você pode criar para fins de teste. Para acessar mais informações sobre clientes de Network File System (NFS) e Service Message Block (SMB) aceitos, consulte Clientes NFS e SMB aceitos pelo Gateway de Arquivos.

> **Note**
>
> Console de gerenciamento da AWS Também fornece exemplos de comandos que você pode usar para montar seu compartilhamento de arquivos.

Tópicos

- Montar seu compartilhamento de arquivos NFS no cliente: saiba como montar o compartilhamento de arquivos NFS em uma unidade no cliente e associe-lo ao bucket do Amazon S3.
- Montar o compartilhamento de arquivos SMB no cliente: saiba como montar seu compartilhamento de arquivos SMB e associar a uma unidade acessível por seu cliente.
- Usar compartilhamentos de arquivos em buckets com objetos preexistentes: saiba como exportar um compartilhamento de arquivos em um bucket do Amazon S3 com objetos criados fora do Gateway de Arquivos usando NFS ou SMB.
- Testar seu Gateway de Arquivos do S3: saiba como testar seu gateway copiando arquivos e pastas para sua unidade associada e verificando se eles aparecem automaticamente no bucket do Amazon S3.

Montar seu compartilhamento de arquivos NFS no cliente

Use o procedimento a seguir para montar seu compartilhamento de arquivos NFS em uma unidade no cliente e associá-lo ao seu bucket do Amazon S3.

Como montar um compartilhamento de arquivos e associá-lo a um bucket do Amazon S3

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

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

     ```
     sudo mount -t nfs -o nolock,hard [GatewayVMIPAddress]:/[FileShareName] [ClientMountPath]
     ```

   - Para clientes Windows, digite o comando a seguir no prompt (cmd.exe).

     ```
     mount -o nolock -o mtype=hard [GatewayVMIPAddress]:/[FileShareName] [WindowsDriveLetter]
     ```

   Por exemplo, suponha que em um cliente Windows seu endereço IP da VM seja 123.123.1.2 e o nome do compartilhamento de arquivos seja `test-fileshare`. Suponha também que você deseja mapear para a unidade T. Nesse caso, o comando tem a seguinte aparência.

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

   > **Note**
   >
   > Ao montar compartilhamentos de arquivos, esteja ciente do seguinte:
   >
   > - Por padrão, o Windows usa uma montagem flexível para compartilhamentos NFS. As montagens flexíveis expiram mais facilmente quando há problemas de conexão. É recomendável usar uma montagem de disco rígido para workloads críticas porque é mais segura e preserva melhor os dados. Para usar uma montagem rígida, verifique se o comando usa a chave `-o mtype=hard`.
   > - O Gateway de Arquivos do S3 não oferece suporte ao bloqueio de arquivos NFS. Sempre use a opção `-o nolock` de desativar o bloqueio de arquivos ao montar compartilhamentos de arquivos NFS.
   > - Pode acontecer de uma pasta e um objeto existirem em um bucket do Amazon S3 e terem o mesmo nome. Neste caso, se o nome do objeto não contiver uma barra no final, apenas a pasta ficará visível no Gateway de Arquivos. Por exemplo, se o bucket

contiver um objeto chamado `test` ou `test/` e uma pasta chamada `test/test1`, apenas `test/` e `test/test1` estarão visíveis no Gateway de Arquivos.

- É provável que você precise montar novamente o compartilhamento de arquivos ao reinicializar seu cliente.
- Se você estiver usando clientes Windows, verifique suas opções `mount` após a montagem executando o comando `mount` sem opções. A resposta deve confirmar que o compartilhamento de arquivos foi montado usando as opções mais recentes que você forneceu. Ela também deve confirmar que você não está usando entradas antigas em cache, que levam pelo menos 60 segundos para desaparecer.

Próxima etapa

[Testar seu Gateway de Arquivos do S3]

Montar o compartilhamento de arquivos SMB no cliente

Use um dos procedimentos a seguir para 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. A seguir, você pode encontrar algumas opções adicionais para testar.

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

- Prompt de comando (`cmdkey` e `net use`): use o prompt de comando para montar seu compartilhamento de arquivos. Armazene suas credenciais com `cmdkey`, depois, monte a unidade com `net use` e inclua as opções `/persistent:yes` e `/savecred` se quiser que a conexão persista durante as reinicializações do sistema. Os comandos específicos serão diferentes dependendo se você deseja montar a unidade para acesso ao Microsoft Active Directory (AD) ou acesso de usuário convidado. São fornecidos exemplos abaixo.
- Explorador de Arquivos (Map Network Drive): use o Explorador de Arquivos do Windows para montar seu compartilhamento de arquivos. Defina as configurações para especificar se você deseja que a conexão persista nas reinicializações do sistema e solicite as credenciais da rede.
- PowerShell script — Crie um PowerShell script personalizado para montar seu compartilhamento de arquivos. Dependendo dos parâmetros especificados no script, a conexão pode ser persistente

nas reinicializações do sistema e o compartilhamento pode ficar visível ou invisível para o sistema operacional enquanto montado.

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

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

1. Assegure-se de que o usuário do Microsoft AD tenha as permissões necessárias para o compartilhamento de arquivos SMB antes de montá-lo no sistema do usuário.
2. Digite o seguinte no prompt de comando para montar o compartilhamento de arquivos:

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

Para montar o compartilhamento de arquivos SMB com uma combinação específica de credenciais de login usando o prompt de comando:

1. Assegure-se de que você tenha acesso ao compartilhamento de arquivos SMB antes de montá-lo no sistema.
2. Digite o seguinte no prompt de comando para salvar as credenciais do usuário no Gerenciador de Credenciais do Windows:

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

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

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

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

   cmdkey /add:*GatewayIPAddress* /user:*DomainName*\smbguest /pass:*Password*
3. No prompt de comando, digite o seguinte.

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

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

Para montar um compartilhamento de arquivos SMB usando Windows File Explorer

1. Pressione a tecla Windows e digite **File Explorer** na caixa Pesquisa do Windows ou pressione **Win+E**.
2. No painel de navegação, escolha Este PC. Depois, na guia Computador, escolha Associar unidade de rede.
3. Na caixa de diálogo Mapear unidade de rede, escolha uma letra de unidade em Unidade.
4. Para Pasta, digite ***[File Gateway IP]**[SMB File Share Name]*** ou selecione Procurar para escolher seu compartilhamento de arquivos SMB na caixa de diálogo.

5. (Opcional) Selecione Reconectar ao entrar se quiser que seu ponto de montagem persista após reinicializações.
6. (Opcional) Selecione Conectar usando credenciais diferentes se você deseja que um usuário insira o logon do Microsoft AD ou uma conta de usuário e senha de convidado.
7. Escolha Finalizar para concluir o ponto de montagem.

> **Note**
>
> Todos os arquivos ou diretórios que comecem com um caractere de ponto (`.`) serão marcados como ocultos no Windows. Para tornar esses arquivos e diretórios visíveis, marque a caixa de seleção Itens ocultos na guia Visualizar no Explorador de Arquivos do Windows.

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

Para modificar suas propriedades de compartilhamento de arquivos SMB

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. No painel de navegação, escolha File Shares (Compartilhamentos de arquivos).
3. Na página File Share (Compartilhamento de arquivos), marque a caixa de seleção próxima ao compartilhamento de arquivos SMB que você deseja modificar.
4. Em Ações, escolha a ação desejada:
   - Escolha Edit file share settings (Editar configurações de compartilhamento de arquivos) para modificar o acesso do compartilhamento.
   - Escolha Editar allowed/denied usuários para adicionar ou excluir usuários e grupos e, em seguida, digite os usuários e grupos permitidos e negados nas caixas Usuários permitidos, Usuários negados, Grupos permitidos e Grupos negados. Use os botões Add Entry (Adicionar entrada) para criar novos direitos de acesso e o botão (X) para remover acesso.

> **Note**
>
> Os grupos devem ser prefixados com o caractere `@`. Os formatos aceitáveis são: `DOMAIN\User1`, `user1`, `@group1` e `@DOMAIN\group1`.

5. Ao terminar, escolha Salvar.

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

   Você pode ativar as Listas de Controle de Acesso (ACLs) no compartilhamento de arquivos SMB. Para obter informações sobre como ativar ACLs, consulteUsar ACLs do Windows para limitar o acesso a compartilhamentos de arquivos SMB.

Próxima etapa

Testar seu Gateway de Arquivos do S3

Usar compartilhamentos de arquivos em buckets com objetos preexistentes

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

Você pode fazer upload de objetos em um bucket do S3 a qualquer momento. Para que o compartilhamento de arquivos exiba esses objetos adicionados recentemente como arquivos, é necessário atualizar o bucket do S3. Para obter mais informações, consulte the section called “Atualizar o cache de objetos do bucket do Amazon S3”.

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

Para atribuir padrões de metadados a objetos acessados usando NFS, consulte Editar padrões de metadados no Gerenciar um Gateway de Arquivos do Amazon S3.

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

Testar seu Gateway de Arquivos do S3

Use o procedimento a seguir para testar seu gateway copiando arquivos e pastas para sua unidade associada e verificando se eles aparecem automaticamente no bucket do Amazon S3.

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

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

   Você pode ver o compartilhamento de arquivos que você criou na guia Compartilhamentos de arquivos no AWS Storage Gateway Management Console.

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

> **Note**
>
> Os Gateways de Arquivos não aceitam a criação de links físicos ou simbólicos em um compartilhamento de arquivos.

Lembre-se do seguinte sobre a forma como os Gateways de Arquivos trabalham com o S3:

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

Gerenciar um Gateway de Arquivos do Amazon S3

Os tópicos desta seção fornecem informações sobre como gerenciar recursos do Gateway de Arquivos do Amazon S3. O gerenciamento do gateway inclui a concessão de permissões para que o gateway acesse compartilhamentos de arquivos e buckets do Amazon S3, edição de informações e configurações para gateways e compartilhamentos de arquivos, exclusão de compartilhamentos de arquivos, atualização de objetos em cache e compreensão dos indicadores de status operacional para gateways e compartilhamentos de arquivos.

Tópicos

- Editar informações básicas do gateway- Aprenda a 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.
- Conceder acesso e permissões- Saiba como usar as funções do IAM para fornecer ao seu gateway permissões de acesso para buckets do Amazon S3 e endpoints do Amazon VPC, evitar certos problemas de segurança e conectar compartilhamentos de arquivos a buckets entre contas. AWS
- Excluir um compartilhamento de arquivos: aprenda a excluir um compartilhamento de arquivos usando o console do Storage Gateway.
- Editar configurações de SMB do gateway: aprenda a editar configurações de SMB ao nível do gateway que controlam a estratégia de segurança, a autenticação do Active Directory, o acesso de convidado, as permissões de grupos locais e a visibilidade de compartilhamentos de arquivos para os compartilhamentos SMB em um gateway.
- Editar configurações do compartilhamento de arquivos SMB: aprenda a editar configurações para definir nome, registro em log, atualização de cache, classe de armazenamento, exportação de arquivos e muito mais para um compartilhamento de arquivos SMB.
- Limitar acesso ao compartilhamento de arquivos SMB: aprenda a adicionar usuários ou grupos permitidos ou negados para limitar o acesso a um compartilhamento de arquivos SMB.
- Editar configurações do compartilhamento de arquivos NFS: aprenda a editar configurações para definir nome, registro em log, atualização de cache, classe de armazenamento, exportação de arquivos e muito mais para um compartilhamento de arquivos NFS.
- Editar padrões de metadados do compartilhamento de arquivos NFS: aprenda a editar valores de metadados padrão que incluem permissões do Unix para arquivos e pastas em compartilhamentos de arquivos NFS.

- Limitar acesso ao compartilhamento de arquivos NFS: aprenda a limitar o acesso a clientes de endereços IP ou intervalos de IP específicos para um compartilhamento de arquivos NFS.
- Atualizar o cache de objetos do bucket do Amazon S3: aprenda a atualizar o cache de objetos do bucket do S3 para um compartilhamento de arquivos e configurar um cronograma de atualização automática do cache.
- Usar o bloqueio de objetos do S3: saiba como o Gateway de Arquivos do Amazon S3 funciona com o recurso Bloqueio de Objetos do S3.
- Status do compartilhamento de arquivos: aprenda a visualizar e interpretar o status de um compartilhamento de arquivos.
- Status do gateway: aprenda a visualizar e interpretar o status de um gateway.
- Gerenciar a largura de banda de um Gateway de Arquivos do Amazon S3- Saiba como limitar a taxa de transferência de upload do seu gateway para controlar AWS a quantidade de largura de banda de rede que o gateway usa.

Editar informações básicas de um Gateway de Arquivos do S3

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.

Conceder acesso e permissões para compartilhamentos de arquivos e buckets

Depois que seu S3 File Gateway estiver ativado e em execução, você poderá adicionar compartilhamentos de arquivos adicionais e conceder acesso aos buckets do Amazon S3, incluindo buckets Contas da AWS diferentes dos seus gateways e compartilhamentos de arquivos. As seções a seguir descrevem como usar perfis do IAM para fornecer ao gateway permissões de acesso a buckets do Amazon S3 e endpoints da VPC, evitar certos problemas de segurança e conectar compartilhamentos de arquivos a buckets entre Contas da AWS.

Para obter informações sobre como criar um compartilhamento de arquivos, consulte Criar um compartilhamento de arquivos.

Esta seção contém os seguintes tópicos, que fornecem informações adicionais sobre como conceder acesso e permissões para compartilhamentos de arquivos e buckets do Amazon S3:

Tópicos

- Conceder acesso a um bucket do Amazon S3: aprenda a conceder acesso para um Gateway de Arquivos fazer upload de arquivos em um bucket do Amazon S3 e realizar ações em qualquer ponto de acesso ou endpoint do Amazon Virtual Private Cloud (Amazon VPC) que ele usa para se conectar ao bucket.
- Prevenção contra o ataque do “substituto confuso” em todos os serviços: aprenda a evitar um problema de segurança comum em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executar a ação.

- Usar um compartilhamento de arquivos para acesso entre contas: aprenda a conceder acesso para uma conta da Amazon Web Services e para os usuários dessa conta acessarem recursos que pertencem a outra conta da Amazon Web Services.

Conceder acesso a um bucket do Amazon S3

Quando você cria um compartilhamento de arquivos, o Gateway de Arquivos precisa de acesso para fazer upload de arquivos no bucket do Amazon S3 e para realizar ações em quaisquer pontos de acesso ou endpoints da nuvem privada virtual (VPC) que ele usa para se conectar ao bucket. Para conceder esse acesso, seu File Gateway assume uma função AWS Identity and Access Management (IAM) associada a uma política do IAM que concede esse acesso.

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

Você pode criar o perfil e a política de acesso por conta própria, ou o Gateway de Arquivos pode criá-los para você. Se o Gateway de Arquivos criar a política para você, ela terá uma lista de ações do S3. Para obter informações sobre perfis e permissões, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

O exemplo de política de confiança a seguir permite que o Gateway de Arquivos assuma um perfil do IAM.

JSON

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

```
}
```

> **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

Se não quiser que o Gateway de Arquivos crie uma política em seu nome, você pode criar sua própria política e anexá-la ao compartilhamento de arquivos. Para obter mais informações sobre como fazer isso, consulte Criar um compartilhamento de arquivos.

O exemplo de política a seguir permite que o Gateway de Arquivos realize todas as ações do Amazon S3 listadas na política. A primeira parte da declaração permite que todas as ações listadas sejam executadas no bucket do S3 chamado `amzn-s3-demo-bucket`. A segunda parte permite as ações listadas em todos os objetos no `amzn-s3-demo-bucket`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
```

```
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Effect": "Allow"
        }
    ]
}
```

O exemplo de política a seguir é semelhante ao anterior, mas permite que o Gateway de Arquivos execute as ações necessárias para acessar um bucket por meio de um ponto de acesso.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
```

```
            "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Se você precisar conectar o compartilhamento de arquivos a um bucket do S3 por meio de um endpoint da VPC, consulte Políticas de endpoint para o Amazon S3 no Guia do usuário do AWS PrivateLink .

> **Note**
>
> Para buckets criptografados, o compartilhamento de arquivos deve usar a chave na conta do bucket do S3 de destino.

> **Note**
>
> Se o seu gateway de arquivos usa SSE-KMS ou DSSE-KMS para criptografia, certifique-se de que a função do IAM associada ao compartilhamento de arquivos inclua as permissões kms:encrypt, kms:decrypt, kms: *, kms: e kms:. ReEncrypt GenerateDataKey DescribeKey Para acessar mais informações, consulte Usar políticas baseadas em identidade (políticas do IAM) para o Storage Gateway.

Prevenção contra o ataque do “substituto confuso” em todos os serviços

O problema "confused deputy" é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executar a ação. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter

permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount`global `aws:SourceArn`e as chaves de contexto nas políticas de recursos para limitar as permissões que AWS Storage Gateway concedem outro serviço ao recurso. Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta `aws:SourceArn` no valor deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

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

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

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` no Storage Gateway para evitar o problema de "confused deputy" (representante enganado).

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Sid": "ConfusedDeputyPreventionExamplePolicy",
       "Effect": "Allow",
       "Principal": {
         "Service": "storagegateway.amazonaws.com"
       },
       "Action": "sts:AssumeRole",
       "Condition": {
         "StringEquals": {
           "aws:SourceAccount": "444455556666"
         },
         "ArnLike": {
```

```
          "aws:SourceArn": "arn:aws:storagegateway:us-
east-1:444455556666:gateway/sgw-123456DA"
        }
      }
    }
  ]
}
```

Usar um compartilhamento de arquivos para acesso entre contas

O acesso entre contas é quando uma conta da Amazon Web Services e os usuários dela recebem acesso a recursos que pertencem a outra conta da Amazon Web Services. Com os Gateways de Arquivos, você pode usar um compartilhamento de arquivos em uma conta da Amazon Web Services para acessar objetos em um bucket do Amazon S3 que pertence a outra conta da Amazon Web Services.

Como usar um compartilhamento de arquivos pertencente a uma conta da Amazon Web Services para acessar um bucket do S3 em outra conta da Amazon Web Services

1. Verifique se o proprietário do bucket do S3 concedeu à conta da Amazon Web Services acesso ao bucket do S3 que você precisa acessar e aos objetos desse bucket. Para obter informações sobre como conceder esse acesso, consulte Exemplo 2: Proprietário do bucket concedendo permissões de bucket entre contas no Guia do usuário do Amazon Simple Storage Service. Para obter uma lista das permissões necessárias, consulte Conceder acesso a um bucket do Amazon S3.
2. Verifique se a função do IAM usada por seu compartilhamento de arquivos para acessar o bucket do S3 inclui as permissões de operações como `s3:GetObjectAcl` e `s3:PutObjectAcl`. Além disso, certifique-se de que a função do IAM inclui uma política de confiança que permite que a sua conta assuma essa função do IAM. Para um exemplo de uma política de confiança desse tipo, consulte Conceder acesso a um bucket do Amazon S3.

   Se seu compartilhamento de arquivo usar uma função existente para acessar o bucket do S3, você deve incluir permissões para operações `s3:GetObjectAcl` e `s3:PutObjectAcl`. Uma função também precisa de uma política de confiança que permita à sua conta assumir essa função. Para um exemplo de uma política de confiança desse tipo, consulte Conceder acesso a um bucket do Amazon S3.

3. Escolha arquivos do Gateway acessíveis ao proprietário do bucket do S3 ao criar seu compartilhamento de arquivos ou editar as configurações de compartilhamento de arquivos em casa. https://console.aws.amazon.com/storagegateway/

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

> **Important**
>
> Certifique-se de configurar as políticas corretamente para conceder o acesso entre contas para a conta usada por seu compartilhamento de arquivos. Se não fizer isso, as atualizações nos arquivos por meio de aplicações on-premises não serão propagadas para o bucket do Amazon S3 em que você está trabalhando.

Recursos

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

Diretrizes para usar as opções de política de acesso disponíveis no Guia do usuário do Amazon Simple Storage Service

Visão geral da lista de controle de acesso (ACL) no Guia do usuário do Amazon Simple Storage Service

Excluir um compartilhamento de arquivos

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

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

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

Para excluir um compartilhamento de arquivos

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Compartilhamentos de arquivos e selecione um ou mais compartilhamentos de arquivos para excluir.
3. Para Actions, escolha Delete file share. Uma caixa de diálogo de confirmação é exibida.
4. Verifique se você deseja excluir os compartilhamentos de arquivos especificados, digite a palavra excluir na caixa de confirmação e escolha Excluir.

Em alguns casos, talvez você queira excluir o compartilhamento de arquivos antes que todos os dados gravados em arquivos no compartilhamento de arquivos do NFS (Sistema de arquivos em rede) sejam carregados. Por exemplo, talvez você queira descartar intencionalmente dados que foram gravados, mas cujo upload ainda não foi feito, ou o bucket do Amazon S3 que armazena o compartilhamento de arquivos pode já ter sido excluído, o que significa que não é mais possível fazer upload dos dados especificados.

Nesses casos, você pode excluir à força o compartilhamento de arquivos usando a operação Console de gerenciamento da AWS ou a `DeleteFileShare` API. Essa operação interrompe o processo de upload de dados. Quando fizer isso, o compartilhamento de arquivos entrará no status FORCE_DELETING. Para excluir à força um compartilhamento de arquivos usando o console do Storage Gateway, consulte o procedimento a seguir.

Para excluir à força um compartilhamento de arquivos

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Na página da lista de Compartilhamentos de arquivos, escolha o compartilhamento de arquivos que você sinalizou para exclusão no procedimento acima para ver seus detalhes. Depois de alguns segundos, uma mensagem de notificação de exclusão aparece na guia Detalhes.
3. Na mensagem que aparece na guia Detalhes, verifique o ID do compartilhamento de arquivos que deseja excluir à força, selecione a caixa de confirmação e escolha Forçar exclusão agora.

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

> Quando você exclui um compartilhamento de arquivos à força, as partes de arquivos parcialmente transferidos por meio de uploads fragmentados podem permanecer no Amazon S3, onde podem gerar cobranças de armazenamento. Recomendamos que você configure uma regra de ciclo de vida de bucket do Amazon S3 para excluir essas partes de arquivo automaticamente. Para obter mais informações, consulte Práticas recomendadas: gerenciar uploads fragmentados.

Você também pode usar a operação da DeleteFileShareAPI para excluir à força o compartilhamento de arquivos. A exclusão de um compartilhamento de arquivos usando a API exige a permissão de política do IAM `storagegateway:DeleteFileShare`.

Editar as configurações de SMB para um gateway

As configurações de SMB ao nível do gateway permitem que você configure a estratégia de segurança, a autenticação do Active Directory, o acesso de convidado, as permissões de grupos locais e a visibilidade de compartilhamentos de arquivos para os compartilhamentos SMB em um gateway.

Como editar as configurações de SMB ao nível do gateway

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, selecione Editar configurações do SMB e escolha as configurações que deseja editar.

Esta seção contém os tópicos a seguir, que fornecem informações e procedimentos adicionais relacionados à configuração de cada uma das configurações de SMB para o gateway.

Tópicos

- Definir nível de segurança do gateway: aprenda a definir um nível de segurança para especificar os requisitos de conexão, como assinatura e criptografia do Server Message Block (SMB), e se deve permitir conexões de clientes SMB versão 1.
- Configurar a autenticação do Active Directory- Saiba como configurar seu Active Directory corporativo ou Microsoft AD AWS gerenciado para acesso autenticado pelo usuário ao seu compartilhamento de arquivos SMB.

- Fornecer acesso de convidado: aprenda a configurar o gateway para permitir o acesso de convidado a qualquer usuário que forneça o nome de usuário e a senha corretos da conta de convidado.
- Configurar grupos locais: aprenda a configurar grupos locais para conceder aos usuários do Active Directory permissões especiais de compartilhamento de arquivos.
- Definir a visibilidade do compartilhamento de arquivos: saiba como especificar se os compartilhamentos em um gateway ficam visíveis ao listar compartilhamentos para usuários.

Definir um nível de segurança para o gateway

Usando um Gateway de Arquivos do S3, você pode especificar um nível de segurança para seu gateway. Ao especificar esse nível de segurança, é possível definir se o gateway exigirá uma assinatura do Server Message Block (SMB) ou criptografia do SMB, ou se você deseja permitir o SMB versão 1.

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 estratégia de segurança mais alto pode afetar o desempenho do gateway.

- Impor AES256 criptografia — Se você escolher essa opção, o S3 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 lidam com dados sensíveis. Ela funciona com todos os clientes SMB atuais no Microsoft Windows.

- Impor criptografia — Se você escolher essa opção, o S3 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 lidam com dados sensíveis. Ela funciona com todos os clientes SMB atuais no Microsoft Windows.
- Impor assinatura — Se você escolher essa opção, o S3 File Gateway só permitirá conexões de SMBv2 ou SMBv3 clientes que tenham a assinatura ativada. Essa opção funciona com todos os clientes SMB atuais no Microsoft Windows.
- Cliente negociado: se você escolher essa opção, as solicitações serão estabelecidas com base no que for negociado pelo cliente. Essa opção é recomendada quando você quer maximizar a compatibilidade entre diferentes clientes em seu ambiente.

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

5. Escolha Salvar.

Usar o Active Directory para autenticar usuários

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

> **Note**
>
> 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.

Você também pode ativar listas de controle de acesso (ACLs) no compartilhamento de arquivos SMB. Para obter informações sobre como ativar ACLs, consulteUsar ACLs do Windows para limitar o acesso a compartilhamentos de arquivos SMB.

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.

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

1. No console do Storage Gateway, escolha o compartilhamento de arquivos ao qual deseja limitar o acesso.
2. No menu suspenso Ações, escolha Editar configurações de acesso a compartilhamentos de arquivos.
3. Na seção Acesso ao compartilhamento de arquivos para usuários e grupos, escolha suas configurações.

   Em Usuários e grupos permitidos, escolha Adicionar usuário permitido ou Adicionar grupo permitido e insira um usuário ou grupo do AD ao qual deseja permitir o acesso ao compartilhamento de arquivos. Repita esse processo para permitir quantos usuários e grupos forem necessários.

   Em Usuários e grupos negados, escolha Adicionar usuário negado ou Adicionar grupo negado e insira um usuário ou grupo do AD ao qual deseja negar o acesso ao compartilhamento de arquivos. Repita esse processo para negar quantos usuários e grupos forem necessários.

   > **Note**
   >
   > A seção Acesso ao compartilhamento de arquivos para usuários e grupos será exibida somente se a opção Active Directory estiver selecionada.
   > Os grupos devem ser prefixados com o caractere `@`. Os formatos aceitáveis são: `DOMAIN\User1`, `user1`, `@group1` e `@DOMAIN\group1`.
   > Se você configurar as listas de Usuários e Grupos Permitidos e Negados, o Windows ACLs não concederá nenhum acesso que substitua essas listas.

As listas de usuários e grupos permitidos e negados são avaliadas anteriormente ACLs e controlam quais usuários podem montar ou acessar o compartilhamento de arquivos. Se algum usuário ou grupo for colocado na lista Permitidos, a lista será considerada ativa e somente esses usuários poderão montar o compartilhamento de arquivos. Depois que um usuário montar um compartilhamento de arquivos, ACLs forneça uma proteção mais granular que controle quais arquivos ou pastas específicos o usuário pode acessar. Para obter mais informações, consulte Ativando o Windows ACLs em um novo compartilhamento de arquivos SMB.

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

Fornecer acesso de convidado ao compartilhamento de arquivos

Você pode configurar o Gateway de Arquivos do S3 para permitir o acesso de convidado a qualquer usuário que forneça o nome de usuário e a senha corretos da conta de convidado. Se você quiser que esse seja o único método pelo qual os usuários possam acessar o Gateway de Arquivos, não precisará associar o gateway a um domínio do Microsoft Active Directory. Também pode usar esse método de acesso de convidado para criar compartilhamentos de arquivos em um Gateway de Arquivos do S3 que seja membro de um domínio do Active Directory.

Quando você configura um compartilhamento de arquivos para usar o método de autenticação Acesso de convidado, o nome de usuário de acesso de convidado é `smbguest`. Antes de criar um compartilhamento de arquivos usando o acesso de convidado, é necessário alterar a senha padrão do usuário `smbguest`.

Você pode usar o procedimento a seguir para alterar a senha do usuário convidado `smbguest`.

Para alterar a senha de acesso convidado

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Gateways no painel de navegação no lado esquerdo da página do console e selecione o Nome do gateway ao qual deseja fornecer acesso de convidado.
3. No menu suspenso Ações, escolha Editar configurações do SMB e selecione Configurações de acesso de convidado.
4. Em Senha de convidado, insira a senha de acesso de convidado que deseja definir e selecione Salvar alterações.

Configurar grupos locais para o gateway

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

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

> **Note**
>
> É necessário adicionar pelo menos um usuário ou grupo de administradores do gateway antes de poder associar o gateway a um domínio do Active Directory.

Como atribuir administradores do gateway

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 Grupo local.
4. Na seção Configurações de Grupo local, escolha suas configurações. Esta seção só é exibida para compartilhamentos de arquivos que usam o Active Directory.

   Em Administradores do gateway, adicione usuários e grupos do Active Directory aos quais deseja conceder permissões locais de administrador do gateway. Adicione um usuário ou grupo por linha, inclusive o nome do domínio. Por exemplo, .**`corp\Domain Admins`** Para criar linhas adicionais, escolha Adicionar novo administrador do gateway.

   > **Note**
   >
   > A edição dos administradores do gateway desconecta e reconecta todos os compartilhamentos de arquivos SMB.

5. Escolha Salvar alterações e selecione Continuar para confirmar a mensagem de aviso exibida.

Definir a visibilidade do compartilhamento de arquivos

A visibilidade do compartilhamento de arquivos controla se os compartilhamentos em um gateway ficam visíveis ao listar compartilhamentos para usuários, como em uma visualização de rede ou lista de navegação. Se os compartilhamentos de arquivos em um gateway estiverem visíveis, os clientes poderão descobri-los facilmente usando um navegador de arquivos se souberem o endereço IP ou nome DNS do gateway. Se os compartilhamentos de arquivos não estiverem visíveis, os clientes precisarão saber o nome do compartilhamento, além do IP ou nome DNS do gateway, para poderem descobri-los.

> **Note**
>
> Essa configuração não é um método eficaz para proteger o acesso aos compartilhamentos de arquivos em sua implantação. Por segurança, recomendamos que você configure permissões para limitar o acesso a usuários e grupos específicos. Para obter instruções, consulte Limitar o acesso de usuários e grupos a um compartilhamento de arquivos SMB.

Como definir a visibilidade do compartilhamento de arquivos

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 visibilidade de compartilhamentos de arquivos.
4. Em Status de visibilidade, marque a caixa de seleção se quiser que os compartilhamentos nesse gateway apareçam quando o gateway listar compartilhamentos para os usuários. Deixe a caixa de seleção desmarcada se não quiser que os compartilhamentos nesse gateway apareçam quando o gateway listar compartilhamentos para os usuários.

Editar as configurações de um compartilhamento de arquivos SMB

Você pode editar as seguintes configurações de um compartilhamento de arquivos SMB existente:

- Nome do compartilhamento de arquivos: escolha um nome para o compartilhamento de arquivos.
- Logs de auditoria: ative ou desative os logs de auditoria.
- Lista de grupos de logs existente: escolha um grupo de logs existente para os logs de auditoria.

- Tempo de atualização do cache de arquivos que não são do gateway: especifique o intervalo em que deseja atualizar o cache do compartilhamento de arquivos.

> **Note**
>
> Definir esse valor como menos de 30 minutos pode afetar negativamente o desempenho do gateway em situações em que grandes números de objetos do Amazon S3 são criados ou excluídos com frequência.

- Tempo de configuração de eventos de upload: especifique o número de segundos a esperar após o último momento em que um cliente gravou em um arquivo antes de gerar uma notificação `ObjectUploaded`.
- Classe de armazenamento para novos objetos: escolha uma classe de armazenamento para novos objetos criados no bucket do Amazon S3.
- Adivinhar tipo MIME: escolha se deseja que o Storage Gateway adivinhe o tipo MIME dos objetos enviados com base nas extensões de arquivo.
- Arquivos do gateway acessíveis ao proprietário do bucket do S3 - escolha se deseja tornar os arquivos no gateway acessíveis à AWS conta proprietária do bucket do Amazon S3 que está vinculado ao compartilhamento de arquivos
- Habilitar pagamentos pelo solicitante: escolha se deseja exigir que as contas que leiam ou solicitam dados do compartilhamento de arquivos paguem taxas de acesso, em vez do proprietário do bucket.
- Exportar como: escolha se os arquivos são exportados no estado de leitura/gravação ou somente leitura.
- Acesso a arquivos e diretórios controlado por - escolha se deseja usar as permissões Windows ACLs ou POSIX para controlar o acesso a arquivos e diretórios
- Bloqueio oportunista (oplock): escolha se deseja permitir que o compartilhamento de arquivos use o bloqueio oportunista para otimizar a estratégia de armazenamento em buffer de arquivos.
- Forçar distinção entre maiúsculas e minúsculas: escolha se o cliente ou o gateway controla a distinção entre maiúsculas e minúsculas para nomes de arquivos e diretórios.

> **Note**
>
> Se o compartilhamento de arquivos atualmente tiver a distinção Force maiúsculas e minúsculas ativada, desativá-la poderá tornar inacessíveis arquivos com nomes idênticos, mas com maiúsculas e minúsculas diferentes (por exemplo, file.txt, File.txt). Somente

uma versão permanecerá acessível para clientes que não diferenciem maiúsculas de minúsculas.

- Enumeração baseada em acesso para arquivos e diretórios: escolha se deseja tornar os arquivos e pastas no compartilhamento visíveis para todos os usuários durante a enumeração de diretórios ou somente para usuários com acesso de leitura.

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

Para editar as configurações de compartilhamento de arquivos

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha File shares e, em seguida, o compartilhamento de arquivos que deseja atualizar.
3. Em Actions, escolha Edit file share settings.
4. Edite as configurações que desejar alterar.
5. Escolha Salvar.

Limitar o acesso de usuários e grupos a um compartilhamento de arquivos SMB

Recomendamos adicionar usuários ou grupos permitidos ou negados para limitar o acesso ao compartilhamento de arquivos. Caso contrário, o compartilhamento de arquivos estará disponível para todos os usuários autenticados.

Como editar as configurações de acesso SMB

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Compartilhamentos de arquivos e selecione o compartilhamento de arquivos SMB que deseja editar.
3. Em Ações, escolha Editar configurações de acesso ao compartilhamento.

4. Na seção Acesso ao compartilhamento de arquivos para usuários e grupos, escolha suas configurações.

   Em Usuários e grupos permitidos, escolha Adicionar usuário permitido ou Adicionar grupo permitido e insira um usuário ou grupo do AD ao qual deseja permitir o acesso ao compartilhamento de arquivos. Repita esse processo para permitir quantos usuários e grupos forem necessários. Qualquer usuário que não esteja na lista Usuários e grupos permitidos terá o acesso negado.

   Em Usuários e grupos negados, escolha Adicionar usuário negado ou Adicionar grupo negado e insira um usuário ou grupo do AD ao qual deseja negar o acesso ao compartilhamento de arquivos. Repita esse processo para negar quantos usuários e grupos forem necessários. Se a lista Usuários e grupos permitidos estiver vazia, todos os usuários terão acesso, exceto aqueles na lista Usuários e grupos negados.

   > **Note**
   >
   > Insira somente o nome do usuário ou grupo do AD. O nome do domínio é inferido pela associação do gateway no AD específico no qual o gateway ingressou.
   > Se você não especificar nenhum usuário ou grupo permitido ou negado, qualquer usuário do AD autenticado poderá exportar o compartilhamento de arquivos.

Alterar o método de criptografia do lado do servidor para um compartilhamento de arquivos existente

O procedimento a seguir descreve como alterar o método de criptografia do lado do servidor para um compartilhamento de arquivos NFS ou SMB existente usando o console do Storage Gateway. Para realizar essa ação usando a API do Storage Gateway, consulte Atualizar NFSFile compartilhamento ou Atualizar SMBFile compartilhamento na Referência da API do AWS Storage Gateway.

> **Note**
>
> A atualização do método de criptografia aplica o novo método aos objetos existentes armazenados nos buckets do Amazon S3 após a atualização.
> Se você configurar o Gateway de Arquivos para usar criptografia SSE-KMS, deverá adicionar manualmente as permissões `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt*`,

`kms:GenerateDataKey` e `kms:DescribeKey` ao perfil do IAM associado ao compartilhamento de arquivos. Para obter mais informações, consulte Usar políticas baseadas em identidade (políticas do IAM) para o Storage Gateway.

Como alterar o método de criptografia do lado do servidor para um compartilhamento de arquivos NFS ou SMB

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Compartilhamentos de arquivos e selecione o compartilhamento para o qual deseja alterar o método de criptografia.
3. Em Ações, escolha Editar configurações de acesso ao compartilhamento.
4. Em Criptografia, selecione o tipo de criptografia que deseja usar para arquivos em repouso no Amazon S3:

   - Para usar a criptografia do lado do servidor gerenciada com o Amazon S3 (SSE-S3), escolha Chaves gerenciadas pelo S3 (SSE-S3). Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 no Guia do usuário do Amazon Simple Storage Service.
   - Para usar a criptografia do lado do servidor gerenciada com o AWS Key Management Service (SSE-KMS), escolha Chaves gerenciadas pelo KMS (SSE-KMS). Em Chave KMS primária, escolha uma chave AWS KMS existente ou escolha Criar uma nova chave KMS para criar uma nova chave KMS no console AWS Key Management Service ().AWS KMS

     Para obter mais informações sobre AWS KMS, consulte O que é o AWS Key Management Service? no Guia do AWS Key Management Service desenvolvedor.
   - Para usar a criptografia de camada dupla do lado do servidor gerenciada com o AWS Key Management Service (DSSE-KMS), escolha Criptografia do lado do servidor de camada dupla com chaves (DSSE-KMS). AWS Key Management Service Em Chave KMS primária, escolha uma chave AWS KMS existente ou escolha Criar uma nova chave KMS para criar uma nova chave KMS no console AWS Key Management Service ().AWS KMS

     Para obter mais informações sobre o DSSE-KMS, consulte Usando criptografia de camada dupla no lado do servidor com AWS KMS chaves no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Há custos adicionais pelo uso do DSSE-KMS e das chaves. AWS KMS Para obter mais informações, consulte Preços do AWS KMS.
> Para especificar uma AWS KMS chave com um alias que não esteja listado ou para usar uma AWS KMS chave de uma AWS conta diferente, você deve usar o. AWS Command Line Interface As chaves do KMS assimétricas não são aceitas. Para obter mais informações, consulte Create SMBFile Share na Referência da API do AWS Storage Gateway.

5. Quando concluir, escolha Salvar alterações.

Editar as configurações de um compartilhamento de arquivos NFS

Use o procedimento a seguir para editar as configurações de um compartilhamento de arquivos NFS existente depois de criá-lo.

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

Para editar as configurações de compartilhamento de arquivos

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha File shares e, em seguida, o compartilhamento de arquivos que deseja atualizar.
3. Em Actions, escolha Edit file share settings.
4. Em Nome do compartilhamento de arquivos, insira um nome para o compartilhamento.
5. Em Logs de auditoria, escolha uma das seguintes opções:

   - Para criar um grupo de logs para esse compartilhamento de arquivos, selecione Criar um novo grupo de logs.

- Para enviar notificações de integridade e recursos desse compartilhamento de arquivos a um grupo de logs existente, escolha Usar um grupo de logs existente e selecione o grupo desejado na lista.
- Para desativar o registro em log desse compartilhamento de arquivos, escolha Desativar registro em log.

Para obter mais informações sobre logs de auditoria, consulte Noções básicas sobre os logs de auditoria do Gateway de Arquivos do S3.

6. Em Tempo de atualização do cache de arquivos que não são do gateway, escolha Definir intervalo de atualização e defina o tempo em Minutos ou Dias para atualizar o cache do compartilhamento de arquivos usando tempo de vida (TTL). TTL é o intervalo desde a última atualização. Depois de decorrido o intervalo de TTL, o acesso a um diretório faz com que o Gateway de Arquivos atualize o conteúdo desse diretório pelo bucket do Amazon S3.

   > **Note**
   >
   > Definir esse valor como menos de 30 minutos pode afetar negativamente o desempenho do gateway em situações em que grandes números de objetos do Amazon S3 são criados ou excluídos com frequência.

7. Em Tempo de configuração de eventos de upload, escolha Definir tempo de ajuste e insira o tempo de ajuste em segundos. O Tempo de ajuste controla o atraso mínimo entre a operação de gravação mais recente do cliente e a geração da notificação de log `ObjectUploaded`. Como os clientes podem fazer muitas gravações pequenas em arquivos em pouco tempo, recomendamos definir esse parâmetro como o maior tempo possível a fim de evitar a geração de várias notificações para o mesmo arquivo em rápida sucessão. Para obter mais informações, consulte Receber notificação de upload de arquivos.
8. Em Classe de armazenamento para novos objetos, escolha uma classe de armazenamento na lista suspensa. Para obter mais informações sobre as classes de armazenamento, consulte Usar classes de armazenamento com um Gateway de Arquivos.
9. Em Metadados de objetos, faça o seguinte:

   a. Selecione Adivinhar tipo MIME se quiser permitir que o Storage Gateway adivinhe o tipo de mídia para objetos enviados com base em suas extensões de arquivo.

b. Selecione os arquivos do Gateway acessíveis ao proprietário do bucket do S3, se quiser que a AWS conta proprietária do bucket do S3 tenha propriedade total dos arquivos criados pelo gateway, incluindo permissões de leitura, gravação, edição e exclusão.

10. Selecione Habilitar pagamentos pelo solicitante se quiser que o solicitante do arquivo, e não o proprietário do bucket, pague pelo custo da solicitação de dados e do download do bucket do S3.

11.

12. Em Nível de acesso, escolha uma das seguintes opções:

    - Extermínio de raiz (padrão): o acesso para o superusuário remoto (raiz) é mapeado para o UID (65534) e o GID (65534).
    - Todo extermínio: todo o acesso de usuário é mapeado para o ID de usuário (UID) (65534) e o ID de grupo (GID) (65534).
    - Sem extermínio de raiz: o superusuário remoto (raiz) recebe acesso como raiz.

13. Em Exportar como, selecione uma das seguintes opções:

    - Para permitir que os clientes leiam e gravem arquivos no compartilhamento de arquivos, selecione Leitura/gravação.
    - Para permitir que os clientes leiam arquivos, mas não gravem no compartilhamento de arquivos, selecione Somente leitura.

    > **Note**
    >
    > Para compartilhamentos de arquivos montados em um cliente Microsoft Windows, se você selecionar Somente leitura, provavelmente uma mensagem de erro será exibida. Ela indica que um erro inesperado está impedindo que a pasta seja criada. Você pode ignorar a mensagem.

14. Quando terminar de editar as configurações, escolha Salvar alterações.

Editar os padrões de metadados para um compartilhamento de arquivos NFS

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

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

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

Para editar padrões de metadados

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha File shares e, em seguida, o compartilhamento de arquivos que deseja atualizar.

3. Em Actions, escolha Edit file metadata defaults.
4. Na caixa de diálogo Edit file metadata defaults, forneça as informações de metadados e escolha Save.

Limitar o acesso de clientes a um compartilhamento de arquivos NFS

Recomendamos editar as configurações de acesso de clientes NFS para definir uma lista de endereços IP de clientes específicos ou intervalos de blocos CIDR para clientes NFS que têm permissão para se conectar ao compartilhamento de arquivos NFS. Se você optar por não limitar o acesso, qualquer cliente na sua rede poderá acessar o compartilhamento de arquivos.

Como limitar o acesso de clientes a um compartilhamento de arquivos NFS

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Compartilhamentos de arquivos no painel de navegação no lado esquerdo da página do console, depois selecione o ID do compartilhamento de arquivos que deseja editar.
3. No menu suspenso Ações, escolha Editar configurações de acesso a compartilhamentos de arquivos.

   A seção Acessar objeto exibe uma lista de endereços IP e blocos CIDR que atualmente têm permissão para se conectar ao compartilhamento de arquivos NFS. Se o acesso não estiver limitado no momento, você verá uma entrada em Clientes permitidos para o bloco CIDR 0.0.0.0/0, que indica que todos os IPv4 endereços possíveis podem se conectar.
4. Em Clientes permitidos, à direita do bloco CIDR 0.0.0.0/0, escolha Remover.
5. Escolha Adicionar cliente e forneça um endereço IP ou intervalo de endereços em notação CIDR para os clientes que deseja permitir.
6. Repita a etapa anterior para adicionar mais endereços IP ou intervalos, conforme necessário. Se cometer um erro ou precisar revogar o acesso, você poderá escolher Remover à direita do endereço IP ou intervalo que deseja excluir da lista.
7. Quando concluir, escolha Salvar alterações.

Atualizar o cache de objetos do bucket do Amazon S3

À medida que seu cliente NFS ou SMB executa operações no sistema de arquivos, o gateway mantém um inventário dos objetos no cache de objetos do Amazon S3 associado ao compartilhamento de arquivos. O gateway usa esse inventário armazenado em cache para reduzir a latência e a frequência das solicitações do Amazon S3. Essa operação não importa arquivos para o armazenamento em cache do Gateway de Arquivos do S3. Ela atualiza apenas o inventário armazenado em cache para refletir as alterações no inventário dos objetos que estão no cache do bucket do Amazon S3.

Para atualizar o cache de objetos do bucket do S3 para o compartilhamento de arquivos, selecione o método mais adequado ao seu caso de uso na lista a seguir e conclua o procedimento correspondente abaixo.

> **Note**
>
> Independentemente do método usado, listar um diretório pela primeira vez o inicializa, o que faz com que o gateway liste o conteúdo de metadados do diretório do Amazon S3. O tempo necessário para inicializar um diretório é proporcional ao número de entradas nele.

Tópicos

Configurar um cronograma de atualização automática do cache usando o console do Storage Gateway

O procedimento a seguir configura um cronograma de atualização automática do cache com base em um valor de tempo de vida (TTL) especificado por você. Antes de configurar um cronograma de atualização do cache baseado em TTL, considere o seguinte:

- O TTL é medido como o intervalo desde a última atualização do cache para determinado diretório.
- A atualização do cache baseada em TTL ocorre somente quando determinado diretório é acessado após a expiração do período de TTL especificado.
- A atualização não é recursiva. Ela ocorre somente nos diretórios específicos que estão sendo acessados.
- A atualização gera custos de API do Amazon S3 somente em diretórios que não foram sincronizados desde a expiração do TTL.
  - Os diretórios só são sincronizados se forem acessados por atividade NFS ou SMB.
  - A sincronização não ocorre com mais frequência do que o período de TTL especificado.
- A configuração da atualização do cache baseada em TTL é recomendada somente se você atualizar com frequência o conteúdo do seu bucket do Amazon S3 diretamente, fora do fluxo de trabalho entre o gateway e o bucket do Amazon S3.
- As operações NFS e SMB que acessam diretórios expirados TTLs serão bloqueadas enquanto o gateway atualiza o conteúdo do diretório.

> **Note**
>
> Como a atualização do cache pode bloquear as operações de acesso ao diretório, recomendamos configurar o maior período de TTL que for prático para sua implantação.

Como configurar um cronograma de atualização automática do cache usando o console do Storage Gateway

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Compartilhamentos de arquivos.
3. Escolha o compartilhamento de arquivos para o qual deseja configurar o cronograma de atualização.
4. Em Actions, escolha Edit file share settings.
5. Em Atualização automática do cache do S3 depois de, marque a caixa de seleção e defina o tempo em dias, horas e minutos para atualizar o cache do compartilhamento de arquivos usando tempo de vida (TTL). TTL é o intervalo desde a última atualização após a qual o acesso ao diretório fará com que o Gateway de Arquivos atualize o conteúdo desse diretório pela primeira vez no bucket do Amazon S3.
6. Escolha Salvar alterações.

Configure um cronograma automatizado de atualização de cache usando AWS Lambda uma regra da Amazon CloudWatch

Para configurar um cronograma automatizado de atualização de cache usando AWS Lambda uma regra da Amazon CloudWatch

1. Identifique o bucket do S3 usado pelo Gateway de Arquivos do S3.
2. Verifique se a seção Evento está em branco. Ela será preenchida automaticamente mais tarde.
3. Crie um perfil do IAM e permita a relação de confiança para o Lambda `lambda.amazonaws.com`.
4. Use a política a seguir.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Crie uma função do Lambda usando o console do Lambda.
6. Use a função a seguir para sua tarefa do Lambda.

```
import json
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406474878:share/
share-E51FBS9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. Em Perfil de execução, escolha o perfil do IAM que você criou.
8. Opcional: adicione um gatilho para o Amazon S3 e selecione o evento ObjectCreatedou. ObjectRemoved

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

9. Crie uma CloudWatch regra no CloudWatch console e adicione uma agenda. Em geral, recomendamos uma frequência fixa de 30 minutos. No entanto, você pode usar de 1 a 2 horas em um grande bucket do S3.
10. Adicione um novo gatilho para CloudWatch eventos e escolha a regra que você acabou de criar.
11. Salve a configuração do Lambda. Escolha Testar.
12. Escolha S3 PUT e personalize o teste de acordo com seus requisitos.
13. O teste deve ser bem-sucedido. Caso contrário, modifique o JSON de acordo com seus requisitos e teste novamente.
14. Abra o console do Amazon S3 e verifique se o evento que você criou e o ARN da função do Lambda estão presentes.
15. Faça upload de um objeto para o seu bucket do S3 usando o console do Amazon S3 ou a AWS CLI.

    O CloudWatch console gera uma CloudWatch saída semelhante à seguinte.

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

A invocação do Lambda fornece uma saída semelhante à seguinte:

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

O compartilhamento NFS montado em seu cliente refletirá essa atualização.

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

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

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

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

Executar uma atualização manual do cache usando o console do Storage Gateway

Como executar uma atualização manual do cache usando o console do Storage Gateway

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/casa.
2. Escolha Compartilhamentos de arquivos e selecione o compartilhamento para o qual deseja executar a atualização.
3. Em Actions, escolha Refresh cache.

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

Executar uma atualização manual do cache usando a API do Storage Gateway

O procedimento a seguir executa uma atualização manual do cache usando a API do Storage Gateway. Antes de executar uma atualização de cache baseada em API, considere o seguinte:

- Você pode especificar uma atualização recursiva ou não recursiva.
- Uma atualização recursiva consome mais recursos e é mais cara.
- A atualização gera custos de API do Amazon S3 somente em relação aos diretórios que você envia como argumentos na solicitação e, se você especificar uma atualização recursiva, aos descendentes desses diretórios.
- A atualização é executada simultaneamente com outras operações enquanto o gateway está em uso.
  - As operações de NFS e SMB geralmente não ficam bloqueadas durante as atualizações, a menos que uma atualização esteja ativa para o diretório que está sendo acessado pela operação.
  - O gateway não consegue determinar se o conteúdo atual do cache está obsoleto e usa seu conteúdo atual para operações de NFS e SMB, independentemente da atualização.
  - Como a atualização de cache utiliza recursos de hardware virtual do gateway, o desempenho do gateway pode ser afetado negativamente enquanto a atualização está em andamento.
- Executar a atualização do cache baseada em API é recomendada somente se você atualizar o conteúdo do seu bucket do Amazon S3 diretamente, fora do fluxo de trabalho entre o gateway e o bucket do Amazon S3.

> **Note**
>
> Se você conhece os diretórios específicos em que está atualizando o conteúdo do Amazon S3 fora do fluxo de trabalho do gateway, recomendamos especificar esses diretórios na solicitação de atualização baseada em API para reduzir os custos de API do Amazon S3 e o impacto no desempenho do gateway.

Como executar uma atualização manual do cache usando a API do Storage Gateway

- Envie uma solicitação HTTP POST para invocar a operação `RefreshCache` com os parâmetros desejados por meio da API do Storage Gateway. Para obter mais informações, consulte RefreshCachena Referência da API do AWS Storage Gateway.

  > **Note**
  >
  > O envio da solicitação `RefreshCache` apenas inicia a operação de atualização do cache. Quando a atualização do cache termina, não significa necessariamente que o arquivo de atualização esteja concluída. Para saber se a operação de atualização do arquivo foi concluída antes de verificar se há novos arquivos no compartilhamento de arquivos do gateway, use a notificação `refresh-complete`. Para fazer isso, você pode se inscrever para ser notificado por meio de um CloudWatch evento da Amazon. Para obter mais informações, consulte Receber notificação sobre operações de arquivo.

Usar o recurso Bloqueio de Objetos do S3 com o Gateway de Arquivos do Amazon S3

O Gateway de Arquivos do Amazon S3 oferece suporte ao acesso a buckets do S3 que tenham o recurso Bloqueio de Objetos do Amazon S3 ativado. O recurso Bloqueio de Objetos do Amazon S3 permite armazenar objetos usando um modelo de “gravação única e várias leituras” (WORM). Ao usar o recurso Bloqueio de Objetos do Amazon S3, você pode impedir que um objeto no bucket do S3 seja excluído ou substituído. O recurso Bloqueio de Objetos do Amazon S3 funciona em conjunto com o versionamento de objetos para proteger seus dados.

Se você ativar o recurso Bloqueio de Objetos do Amazon S3, ainda poderá modificar o objeto. Por exemplo, ele poderá receber gravações, ser excluído ou renomeado por meio de um compartilhamento de arquivos em um Gateway de Arquivos do S3. Quando você modifica um objeto dessa forma, o Gateway de Arquivos do S3 coloca uma nova versão do objeto sem afetar a versão anterior (ou seja, o objeto bloqueado).

Por exemplo, se você usar a interface NFS ou SMB do Gateway de Arquivos do S3 para excluir um arquivo e o objeto do S3 correspondente estiver bloqueado, o gateway colocará um marcador de exclusão do S3 como a próxima versão do objeto e deixará a versão do objeto original no lugar. Da mesma forma, se um Gateway de Arquivos do S3 modificar o conteúdo ou os metadados de um

objeto bloqueado, uma nova versão do objeto será carregada com as alterações, mas a versão do objeto bloqueado original permanecerá inalterada.

Para obter mais informações sobre o recurso Bloqueio de Objetos do Amazon S3, consulte Bloquear objetos com o recurso Bloqueio de Objetos do S3 no Guia do usuário do Amazon Simple Storage Service.

Noções básicas sobre o status do compartilhamento de arquivos

Você pode visualizar rapidamente a integridade de um compartilhamento de arquivos observando seu status. Se o status indicar que o compartilhamento 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 compartilhamento de arquivos no console do Storage Gateway, na coluna Status. Um compartilhamento de arquivos que está funcionando corretamente mostra o status AVAILABLE. 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 compartilhamento de arquivos está configurado corretamente e disponível para uso. Esse é o status padrão de um compartilhamento de arquivos que está funcionando corretamente.
CRIANDO	O compartilhamento de arquivos ainda não foi totalmente criado e não está pronto para uso. O status CREATING é transitório. Nenhuma ação é necessária. Se o compartilhamento de arquivos ficar preso nesse status, provavelmente é porque a VM do gateway perdeu a AWS conexão com.
ATUALIZANDO	A configuração do compartilhamento de arquivos está sendo atualizad a no momento. O status UPDATING é transitório. Nenhuma ação é necessária. Se um compartilhamento 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 compartil hamento de arquivos não é excluído até que todos os dados sejam enviados para AWS. O status DELETING é transitório e nenhuma ação é necessária.
FORCE_DELETING	O compartilhamento de arquivos está sendo excluído à força. O compartilhamento de arquivos é excluído imediatamente e os dados não são enviados para AWS. O status FORCE_DELETING é transitório e nenhuma ação é necessária.
INDISPONÍVEL	O compartilhamento de arquivos encontra-se em um estado corrompid o. É necessário realizar uma ação. Algumas causas possíveis incluem erros de política de perfil ou mapeamento para um bucket do Amazon S3 que não existe. Quando o problema que provocou esse estado corrompido é resolvido, o compartilhamento de arquivos volta para o status AVAILABLE.

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.

Status	Significado
`OFFLINE`	Seu gateway pode estar sendo exibido como `OFFLINE` por um ou mais dos seguintes motivos: • 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.

Gerenciar a largura de banda de um Gateway de Arquivos do Amazon S3

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

Você pode configurar um bandwidth-rate-limit cronograma usando o Console de gerenciamento da AWS, um kit de desenvolvimento de AWS software (SDK) ou a AWS Storage Gateway API (consulte UpdateBandwidthRateLimitSchedulea referência da API do AWS Storage Gateway). Ao usar uma programação de limite de taxa de largura de banda, é possível configurar limites para serem alterados automaticamente ao longo do dia ou da semana. Para obter mais informações, consulte Visualize e edite a bandwidth-rate-limit programação do seu gateway usando o console do Storage Gateway.

Você pode monitorar a taxa de transferência de upload do seu gateway usando a `CloudBytesUploaded` métrica na guia Monitoramento no console do Storage Gateway ou na Amazon CloudWatch.

> **Note**
>
> Os limites de taxa de largura de banda se aplicam somente aos uploads de arquivos do Storage Gateway. Outras operações de gateway não são afetadas.
> A limitação da taxa de largura de banda funciona equilibrando o throughput de todos os arquivos cujo upload é feito, calculada com base na média por segundo. Embora seja possível que os uploads ultrapassem brevemente o limite da taxa de largura de banda por

um determinado micro ou milissegundo, isso normalmente não resulta em grandes picos por longos períodos.
Atualmente, não há suporte para a configuração de limites e horários de taxa de largura de banda para o tipo Amazon FSx File Gateway.

Tópicos

- Visualize e edite a bandwidth-rate-limit programação do seu gateway usando o console do Storage Gateway
- Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK para Java
- Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK para .NET
- Atualizando os limites de taxa de largura de banda do gateway usando o AWS Tools for Windows PowerShell

Visualize e edite a bandwidth-rate-limit programação do seu gateway usando o console do Storage Gateway

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

Como visualizar e editar a programação do limite da taxa de largura de banda

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.
3. Em Ações, escolha Editar programação do limite da taxa de largura de banda.

   A bandwidth-rate-limit programação atual do gateway é exibida na página Editar programação de limite de taxa de largura de banda. Por padrão, um gateway novo não tem nenhum limite de taxa de largura de banda definido.
4. (Opcional) Escolha Adicionar novo limite de taxa de largura de banda para adicionar um novo intervalo configurável à programação. Para cada intervalo adicionado, insira as seguintes informações:

   - Taxa de upload: insira o limite da taxa de upload, em megabits por segundo (Mbps). O valor mínimo é 100 Mbps.

- Dias da semana: selecione o dia ou dias da semana em que deseja que o intervalo seja aplicado. Você pode aplicar o intervalo em dias úteis (segunda a sexta-feira), fins de semana (sábado e domingo), todos os dias da semana ou em um dia específico por semana. Para aplicar o limite de taxa de largura de banda de maneira uniforme e constante em todos os dias e em todos os horários, escolha Sem programação.
- Hora de início: insira a hora de início do intervalo de largura de banda, usando o formato HH:MM e o fuso horário em relação ao UTC para o seu gateway.

> **Note**
>
> Seu bandwidth-rate-limit intervalo começa no início do minuto especificado aqui.

- Hora de término: insira a hora de término do intervalo de largura de banda, usando o formato HH:MM e o fuso horário em relação ao GMT para o seu gateway.

> **Important**
>
> O bandwidth-rate-limit intervalo termina no final do minuto especificado aqui. Para agendar um intervalo que termine no final de uma hora, insira **59**.
> Para programar intervalos contínuos consecutivos, fazendo a transição no início da hora, sem interrupção entre os intervalos, insira **59** para o minuto final do primeiro intervalo. Insira **00** para o minuto inicial do intervalo seguinte.

5. (Opcional) Repita a etapa anterior conforme necessário até que sua bandwidth-rate-limit programação seja concluída. Se precisar excluir um intervalo da sua agenda, escolha Remover.

> **Important**
>
> Bandwidth-rate-limitos intervalos não podem se sobrepor. A hora de início de um intervalo deve ocorrer após a hora de término de um intervalo anterior e antes da hora de início de um intervalo seguinte.

6. Ao concluir, escolha Salvar alterações.

Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK para Java

Ao atualizar os limites de taxa de largura de banda de forma programática, é possível ajustá-los automaticamente ao longo de um período, por exemplo, usando tarefas programadas. O exemplo a seguir demonstra como atualizar os limites de taxa de largura de banda de um gateway usando o AWS SDK para Java. Para usar o código de exemplo, você deve estar familiarizado com a execução de aplicativos em console Java. Para obter mais informações, consulte Conceitos básicos no Guia do desenvolvedor do AWS SDK para Java .

Example: Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK para Java

O exemplo de código Java a seguir atualiza os limites de taxa de largura de banda de um gateway. Para usar este exemplo de código, você deve fornecer o endpoint de serviço, o nome do recurso da Amazon (ARN) do gateway e o limite de upload. Para obter uma lista de endpoints de serviço da AWS com os quais é possível usar o Storage Gateway, consulte Endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.

```
   import java.io.IOException;

   import com.amazonaws.AmazonClientException;
   import com.amazonaws.auth.PropertiesCredentials;
   import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

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

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

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

       // The endpoint
```

```
        static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

        // Rates
        static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

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

            // Create a Storage Gateway client
            sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
            sgClient.setEndpoint(serviceURL);

            UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File Gateways

        }

        private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
            try
            {
                BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
```

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

Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK para .NET

Ao atualizar os limites de taxa de largura de banda de forma programática, é possível ajustá-los automaticamente ao longo de um período, por exemplo, usando tarefas programadas. O exemplo a seguir demonstra como atualizar os limites de taxa de largura de banda de um gateway usando o AWS Software Development Kit (SDK) para.NET. Para usar o código de exemplo, você deve estar familiarizado com a execução de aplicativos em console do .NET. Para obter mais informações, consulte Conceitos básicos no Guia do desenvolvedor do AWS SDK para .NET .

Example: Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK para .NET

O exemplo de código C# a seguir atualiza os limites de taxa de largura de banda de um gateway. Para usar este exemplo de código, você deve fornecer o endpoint de serviço, o nome do recurso da Amazon (ARN) do gateway e o limite de upload. Para obter uma lista de endpoints de serviço da AWS com os quais é possível usar o Storage Gateway, consulte Endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.

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

```
    namespace AWSStorageGateway
    {
        class UpdateBandwidthExample
        {
            static AmazonStorageGatewayClient sgClient;
            static AmazonStorageGatewayConfig sgConfig;

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

            // The endpoint
            static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";

            // Rates
            static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

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

                UpdateBandwidth(gatewayARN, uploadRate, null);

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

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
 BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
 BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
```

```
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                bandwidthRateLimitIntervals.Add(noScheduleInterval);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

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

Atualizando os limites de taxa de largura de banda do gateway usando o AWS Tools for Windows PowerShell

Ao atualizar os limites de taxa de largura de banda de forma programática, é possível ajustá-los automaticamente ao longo de um período, por exemplo, usando tarefas programadas. O exemplo a seguir demonstra como atualizar os limites de taxa de largura de banda de um gateway usando o AWS Tools for Windows PowerShell. Para usar o código de exemplo, você deve estar familiarizado com a execução de um PowerShell script. Para obter mais informações, consulte Conceitos básicos no Guia do usuário do Ferramentas da AWS para PowerShell .

Example: Atualizando os limites de taxa de largura de banda do gateway usando o AWS Tools for Windows PowerShell

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

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

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


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

    $UploadBandwidthRate = 100 * 1024 * 1024
    $gatewayARN = "*** provide gateway ARN ***"

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

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

    $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN
```

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

Como 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 arquivos S3, gateway de - 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 S3 File Gateway Gateway, consulte Entendendo as métricas do gateway Compreendendo as métricas do de compartilhamento de arquivos Compreendendo as métricas . 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.
- Compartilhamentos de arquivos indisponíveis: `FileSharesUnavailable` >= 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 Configurar seu Amazon S3 File Gateway File Gateway. 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 arquivos S3, gateway de

Você pode monitorar o gateway de arquivos do S3 FSx 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 S3 FSx File Gateway com grupos CloudWatch de registros
- Usando CloudWatch métricas da Amazon
- Receber notificação sobre operações de arquivo
- Noções básicas de métricas de gateway
- Noções básicas de métricas de compartilhamento de arquivos
- Compreendendo os registros de auditoria do S3 File Gateway FSx

Obtendo registros de integridade do S3 FSx File Gateway com grupos CloudWatch de registros

Você pode usar o Amazon CloudWatch Logs para obter informações sobre a integridade do seu gateway de arquivos do S3 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 logs para monitorar seu gateway e ser notificado quando o S3 File Gateway falhar ao fazer upload de arquivos para um bucket do Amazon S3. 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 CloudWatch registros ao ativar um gateway, consulteConfigurar o Gateway de Arquivos do Amazon S3. 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.

Veja a seguir um exemplo de erro relatado pelo Gateway de Arquivos do S3.

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/amzn-s3-demo-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

Esse erro significa que o Gateway de Arquivos do S3 não consegue fazer upload do objeto `myFolder/myFile.text` para o Amazon S3 porque ele mudou da classe de armazenamento Amazon S3 Standard para a classe de armazenamento S3 Glacier Deep Archive.

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

- `source: share-E1A2B34C` indica o compartilhamento de arquivos que encontrou esse erro.

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

Para obter informações sobre como solucionar os erros que podem ser relatados pelo S3 File Gateway , 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 S3 File Gateway Gateway

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 gateway de arquivos do S3 FSx 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 gateway de arquivos do S3 FSx com o qual trabalhar especificando as dimensões `GatewayId` e as`GatewayName` .

CloudWatch Namespace Amazon	Dimensão	Description
		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

Receber notificação sobre operações de arquivo

O Storage Gateway pode iniciar os seguintes CloudWatch eventos quando suas operações de arquivo forem concluídas:

- Você pode ser notificado quando o gateway terminar o upload assíncrono de seus arquivos do compartilhamento de arquivos para o Amazon S3. Use o parâmetro `NotificationPolicy` para solicitar uma notificação de upload de arquivo. Isso envia uma notificação para cada upload de arquivo concluído para o Amazon S3. Para obter mais informações, consulte Receber notificação do upload de arquivos.
- Você pode ser notificado quando o gateway terminar o upload assíncrono do conjunto de arquivos em uso do compartilhamento de arquivos para o Amazon S3. Use a operação da NotifyWhenUploadedAPI para solicitar uma notificação de upload de um conjunto de arquivos em funcionamento. Isso envia uma notificação quando é feito upload de todos os arquivos do conjunto de arquivos de trabalho para o Amazon S3. Para obter mais informações, consulte Receber notificação de upload do conjunto de arquivos em uso.

- Você pode ser notificado quando o gateway terminar de atualizar o cache para seu bucket do S3. Ao invocar a RefreshCacheoperação por meio do console ou da API do Storage Gateway, assine a notificação quando a operação for concluída. Para obter mais informações, consulte Receber notificação de atualização do cache.

Quando a operação de arquivo solicitada estiver concluída, o Storage Gateway enviará uma notificação por meio de CloudWatch Eventos. Você pode configurar CloudWatch Eventos para enviar a notificação por meio de destinos de eventos, como Amazon SNS, Amazon SQS ou uma função. AWS Lambda Por exemplo, você pode configurar um destino do Amazon SNS para enviar a notificação aos consumidores do Amazon SNS, como e-mails e mensagens de texto. Para obter informações sobre CloudWatch eventos, consulte O que são CloudWatch eventos?

Para configurar a notificação de CloudWatch eventos

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

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

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

```
}
```

Para obter informações sobre como usar as regras de CloudWatch eventos, consulte Criação de uma regra de CloudWatch eventos que é acionada em um evento no Guia do usuário do Amazon CloudWatch Events.

Receber notificação do upload de arquivos

Há dois casos de uso para os quais você pode utilizar a notificação de upload de arquivos:

- Para automatizar o processamento em nuvem do upload de arquivos, você pode chamar o parâmetro `NotificationPolicy` e receber um ID de notificação. A notificação que ocorre quando os arquivos dos quais é feito upload tem o mesmo ID de notificação que o dos exibidos pela API. Se você associar esse ID de notificação para monitorar a lista de arquivos dos quais está fazendo upload, você poderá iniciar o processamento do arquivo cujo upload foi feito para a AWS quando o evento com o mesmo ID for gerado.
- Para casos de uso de distribuição de conteúdo, você pode ter dois Gateways de Arquivos do S3 associados ao mesmo bucket do Amazon S3. O cliente de compartilhamento de arquivos do Gateway1 pode fazer upload de novos arquivos para o Amazon S3 e os arquivos são lidos por clientes de compartilhamento de arquivos no Gateway2. Será feito upload dos arquivos para o Amazon S3, mas eles não ficarão visíveis no Gateway2, pois este usa uma versão localmente armazenada em cache dos arquivos no Amazon S3. Para tornar os arquivos visíveis no Gateway2, é possível usar o parâmetro `NotificationPolicy` para solicitar que a notificação de upload de arquivos do Gateway1 envie uma notificação para você quando o upload estiver concluído. Em seguida, você pode usar CloudWatch Eventos para emitir automaticamente uma RefreshCachesolicitação para o compartilhamento de arquivos no Gateway2. Quando a RefreshCachesolicitação for concluída, o novo arquivo ficará visível no Gateway2.

Example Exemplo: notificação de upload de arquivos

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

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
```

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

Nomes de campos	Description
version	A versão atual da política do IAM.
id	O ID que identifica a política do IAM.
detail-type	Uma descrição do evento que iniciou a notificação enviada.
origem	O AWS serviço que é a fonte da solicitação e da notificação.
account	O ID da AWS conta da qual a solicitação e a notificação foram geradas.
horário	O horário em que a solicitação para fazer upload de arquivos para o Amazon S3 foi feita.
region	A AWS região de onde a solicitação e a notificação foram enviadas.

Nomes de campos	Description
recursos	Os recursos do Storage Gateway aos quais a política se aplica.
tamanho do objeto	O tamanho do objeto em bytes.
modification-time	A hora em que o cliente modificou o arquivo.
object-key	O caminho para a função .
event-type	Os CloudWatch eventos que iniciaram a notificação.
prefix	O nome do prefixo do bucket do S3.
nome-do-seu-bucket	O nome do bucket do S3.

Receber notificação de upload do conjunto de arquivos em uso

Há dois casos de uso para os quais você pode utilizar a notificação de upload do conjunto de arquivos de trabalho:

- Para automatizar o processamento em nuvem de arquivos cujo upload foi feito, você pode chamar a API `NotifyWhenUploaded` e receber um ID de notificação. A notificação que ocorre quando o conjunto de arquivos em uso do qual é feito upload tem o mesmo ID de notificação daquele exibido pela API. Se você mapear esse ID de notificação para rastrear a lista de arquivos que você está carregando, poderá iniciar o processamento do conjunto de trabalho de arquivos que são enviados AWS quando o evento com o mesmo ID for gerado.
- Para casos de uso de distribuição de conteúdo, você pode ter dois Gateways de Arquivos do S3 associados ao mesmo bucket do Amazon S3. O cliente de compartilhamento de arquivos do Gateway1 pode fazer upload de novos arquivos para o Amazon S3 e os arquivos são lidos por clientes de compartilhamento de arquivos no Gateway 2. Será feito upload dos arquivos para o Amazon S3, mas eles não ficarão visíveis no Gateway2, pois este usa uma versão localmente armazenada em cache dos arquivos no S3. Para tornar os arquivos visíveis no Gateway2, use a operação de NotifyWhenUploadedAPI para solicitar uma notificação de upload de arquivo do Gateway1, para notificá-lo quando o upload do conjunto de arquivos de trabalho estiver concluído. Em seguida, você pode usar os CloudWatch Eventos para emitir automaticamente

uma RefreshCachesolicitação para o compartilhamento de arquivos no Gateway2. Quando a RefreshCachesolicitação for concluída, os novos arquivos ficarão visíveis no Gateway2. Essa operação não importa arquivos para o armazenamento em cache do gateway. Ela atualiza apenas o inventário em cache para refletir as alterações no inventário dos objetos no bucket do S3.

Example Exemplo: notificação de upload do conjunto arquivos em uso

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

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

Nomes de campos	Description
version	A versão atual da política do IAM.
id	O ID que identifica a política do IAM.
detail-type	Uma descrição do evento que iniciou a notificação enviada.

Nomes de campos	Description
origem	O AWS serviço que é a fonte da solicitação e da notificação.
account	O ID da AWS conta da qual a solicitação e a notificação foram geradas.
horário	O horário em que a solicitação para fazer upload de arquivos para o Amazon S3 foi feita.
region	A AWS região de onde a solicitação e a notificação foram enviadas.
recursos	Os recursos do Storage Gateway aos quais a política se aplica.
event-type	Os CloudWatch eventos que iniciaram a notificação.
notification-id	O ID gerado aleatoriamente da notificação que foi enviada. Esse ID está no formato UUID. Esse é o ID da notificação que é retornada quando `NotifyWhenUploaded` é chamado.
request-received	O horário em que o gateway recebeu a solicitação `NotifyWhenUploaded` .
completed	Quando o upload de todos os arquivos no conjunto de trabalho foi feito para o Amazon S3.

Receber notificação de atualização do cache

Para o caso de uso de notificação de atualização do cache, é possível ter dois Gateways de Arquivos do S3 associados ao mesmo bucket do Amazon S3, e o cliente NFS para Gateway1 faz upload dos novos arquivos para o bucket do S3. É feito upload dos arquivos para o Amazon S3, mas eles não

serão exibidos no Gateway2 enquanto não atualizar o cache. Isso ocorre porque o Gateway2 usa uma versão armazenada localmente em cache dos arquivos no Amazon S3. Você pode querer fazer algo com os arquivos no Gateway2 quando a atualização do cache é concluída. Arquivos grandes podem demorar para serem exibidos no Gateway2. Portanto, convém optar por ser notificado quando a atualização do cache for concluída. Você pode solicitar uma notificação de atualização do cache do Gateway2 quando todos os arquivos estiverem visíveis nele.

Example Exemplo: notificações de atualização do cache

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

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

Nomes de campos	Description
version	A versão atual da política do IAM.

Nomes de campos	Description
id	O ID que identifica a política do IAM.
detail-type	Uma descrição do tipo de evento que iniciou a notificação enviada.
origem	O AWS serviço que é a fonte da solicitação e da notificação.
account	O ID da AWS conta da qual a solicitação e a notificação foram geradas.
horário	O horário em que a solicitação para atualizar os arquivos no conjunto de trabalho foi feita.
region	A AWS região de onde a solicitação e a notificação foram enviadas.
recursos	Os recursos do Storage Gateway aos quais a política se aplica.
event-type	Os CloudWatch eventos que iniciaram a notificação.
notification-id	O ID gerado aleatoriamente da notificação que foi enviada. Esse ID está no formato UUID. Esse é o ID da notificação que é retornada quando você chama `RefreshCache` .
started	O horário em que o gateway recebeu a solicitação `RefreshCache` e a atualização foi iniciada.
completed	O horário em que a atualização do conjunto de trabalho foi concluída.

Nomes de campos	Description
folderList	Uma lista separada por vírgulas de caminhos de pastas que foram atualizadas no cache. O padrão é ["/"].

Noções básicas de métricas de gateway

A tabela a seguir descreve métricas que abrangem Gateways de Arquivos do S3. Cada gateway tem um conjunto de métricas associadas a ele. Algumas métricas específicas do gateway têm o mesmo nome de determinadas métricas. file-share-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 compartilhamento 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 S3 File Gateway s.

Métrica	Description
`AuditNotifications`	Essa métrica relata o número de logs de auditoria emitidos. Unidades: contagem
`AvailabilityNotifications`	Essa métrica relata o número de notificações de integridade relacionadas à disponibilidade que foram geradas pelo gateway no período do relatório.

Métrica	Description
	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. 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

Métrica	Description
`CachePercentDirty`	A porcentagem geral do cache do gateway que não persistiu. AWS A amostra é capturada no final do período do relatório. Use essa métrica com a estatística `Sum`. Preferencialmente, essa métrica deve permanecer baixa. Unidades: percentual
`CachePercentUsed`	A porcentagem do cache de dados usado em todo o gateway. A amostra é capturada no final do período do relatório. Unidades: percentual
`CacheUsed`	Essa métrica relata o número de bytes utilizados no cache do gateway. Unidades: bytes
`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 estatística `Samples` para medir IOPS. Unidades: bytes

Métrica	Description
`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
`FileSharesUnavailable`	Essa métrica fornece o número de compartil hamentos de arquivos nesses gateways que estão no estado Indisponível. Se essa métrica informar que algum compartil hamento de arquivo não está disponível, é provável que haja um problema com o gateway que esteja causando interrupções no seu fluxo de trabalho. É recomendável criar um alarme para quando essa métrica informa um valor diferente de zero. Unidades: contagem

Métrica	Description
FilesRenamed	Essa métrica monitora o número de arquivos renomeados no período do relatório. 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
IoWaitPercent	Essa métrica informa a porcentagem de tempo que a CPU está aguardando uma resposta do disco local. Unidades: percentual

Métrica	Description
`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
`NfsSessions`	Essa métrica relata o número de sessões NFS que estão ativas no gateway. Unidades: contagem
`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
`S3GetObjectRequestTime`	Essa métrica relata o tempo necessário para o gateway concluir as solicitações de recuperaç ão de objetos do S3. Unidade: milissegundos

Métrica	Description
S3PutObjectRequestTime	Essa métrica relata o tempo necessário para o gateway concluir as solicitações de colocação de objetos do S3. Unidade: milissegundos
S3UploadPartRequestTime	Essa métrica relata o tempo necessário para o gateway concluir as solicitações de upload de partes do S3. Unidade: milissegundos
SmbV1Sessions	Essa métrica relata o número de SMBv1 sessões que estão ativas no gateway. Unidades: contagem
SmbV2Sessions	Essa métrica relata o número de SMBv2 sessões que estão ativas no gateway. Unidades: contagem
SmbV3Sessions	Essa métrica relata o número de SMBv3 sessões que estão ativas no gateway. 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 compartilhamento de arquivos

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

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

Métrica	Description
	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. **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 S3 File Gateway FSx

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

Operações

A tabela a seguir descreve as operações de acesso ao arquivo de log de auditoria do S3 FSx 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 arquivo de log de auditoria do Gateway de Arquivos do S3.

Atributo	Definição
`accessMode`	A configuração de permissão do objeto.
`accountDomain` (somente SMB)	O domínio do Active Directory (AD) ao qual pertence a conta do cliente.
`accountName` (somente SMB)	O nome de usuário do cliente do Active Directory.
`bucket`	O nome de um bucket do S3.
`clientGid` (somente NFS)	O identificador do grupo do usuário que está acessando o objeto.
`clientUid` (somente NFS)	O identificador do usuário que está acessando o objeto.
`ctime`	A hora em que o conteúdo ou os metadados do objeto foram modificados, definida pelo cliente.
`groupId`	O identificador do proprietário do grupo do objeto.
`fileSizeInBytes`	O tamanho do arquivo em bytes, definido pelo cliente no momento da criação do arquivo.
`gateway`	O ID do Storage Gateway.
`mtime`	A hora em que o conteúdo do objeto foi modificado, definida pelo cliente.
`newObjectName`	O caminho completo para o novo objeto depois que ele foi renomeado.

Atributo	Definição
`objectName`	O caminho completo para o objeto.
`objectType`	Define se o objeto é um arquivo ou uma pasta.
`operation`	O nome da operação de acesso ao objeto.
`ownerId`	O identificador do proprietário do objeto.
`securityDescriptor` (somente SMB)	Mostra a lista de controle de acesso discricio nário (DACL) definida em um objeto, no formato SDDL.
`shareName`	O nome do compartilhamento que está sendo acessado.
`source`	O ID do compartilhamento de arquivos que está sendo auditado.
`sourceAddress`	O endereço IP da máquina cliente de compartil hamento de arquivos.
`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).
`timestamp`	A hora em que a operação ocorreu com base no timestamp do sistema operacional do gateway.
`version`	A versão do formato do log de auditoria.

Atributos registrados em log por operação

A tabela a seguir descreve os atributos de log de auditoria do Gateway de Arquivos do S3 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: Somente SMB)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
access e			X	X					X	
accour main (somen SMB)	X	X	X	X	X	X	X	X	X	X
accour me (somen SMB)	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (somen NFS)	X	X	X	X	X	X		X	X	X
client (somen NFS)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			X	X						

	Ler dados	Gravar dados	Criar pasta	Criar arquivo	Renomea arquivo/ pasta	Excluir arquivo/ pasta	Atributos de gravação (alterar ACL: Somente SMB)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObj Name					X					
object e	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securi escrip (somen SMB)							X	X		
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X

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

Criar um relatório de cache para seu Gateway de Arquivos do S3

O Gateway de Arquivos do S3 pode gerar um relatório dos metadados dos arquivos que estão atualmente no cache de upload local para um compartilhamento de arquivos específico. Você pode aplicar filtros e critérios adicionais que determinem quais tipos específicos de arquivos em cache aparecem no relatório. Você pode usar esse relatório para ajudar a identificar e resolver problemas do gateway. Por exemplo, se houver falha no upload de arquivos do seu gateway para o Amazon S3, você poderá gerar um relatório que liste os arquivos específicos cujo upload não está sendo feito e os motivos da falha no upload. O relatório é um arquivo CSV que contém uma lista de arquivos que correspondem ao conjunto de parâmetros de filtro especificado por você. O arquivo de saída é armazenado como um objeto do Amazon S3 em um local de bucket que você especifica ao configurar o relatório. Para criar um relatório de cache usando a AWS Storage Gateway API, consulte a Referência StartCacheReportda API do Storage Gateway. Para criar um relatório de cache no console do Storage Gateway, use o procedimento a seguir.

Pré-requisitos

- Seu gateway deve ter as permissões `s3:PutObject` e `s3:AbortMultipartUpload` para o bucket do Amazon S3 em que você deseja armazenar o relatório de cache.

- Nenhum outro relatório de cache pode estar em andamento no momento para o compartilhamento de arquivos.
- Deve haver menos de dez relatórios de cache existentes para o compartilhamento de arquivos.
- O gateway deve estar on-line e conectado AWS a.
- O disco raiz do gateway deve ter pelo menos 20 GB de espaço livre.

Como criar um relatório de cache 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 no lado esquerdo da página, escolha Compartilhamentos de arquivos e, depois, escolha o compartilhamento de arquivos para o qual você deseja criar um relatório de cache.
3. No menu suspenso Ações, escolha Criar relatório de cache.
4. Em Localização do Amazon S3, informe o bucket do Amazon S3 e o prefixo do local onde você deseja salvar o objeto de arquivo CSV do relatório de cache completo no Amazon S3. Para selecionar o bucket e o prefixo do seu armazenamento do Amazon S3 existente, escolha Procurar S3.
5. Em Perfil do IAM, realize uma das seguintes ações para especificar um perfil do IAM que conceda permissões do Gateway de Arquivos para gerar e armazenar o relatório de cache:
   - Para especificar um perfil do IAM existente, escolha um na lista suspensa.
   - Para criar manualmente um perfil do IAM, escolha Criar um perfil e, depois, crie o perfil usando o console do IAM.

> **Note**
>
> O perfil do IAM que você especificar deverá ter as seguintes permissões para gravar objetos no Local do Amazon S3 do bucket de relatórios e interromper os uploads fragmentados no bucket de relatórios:
>
> - `s3:PutObject`
> - `s3:AbortMultipartUpload`

O perfil também deve permitir que o serviço `storagegateway.amazonaws.com` assuma o perfil utilizando a ação `sts:AssumeRole`.

6. Em Filtro de relatório, siga um destes procedimentos para decidir quais arquivos serão incluídos no relatório de cache:

   - Para incluir todos os arquivos em cache que estão atualmente com falha no upload para o Amazon S3, escolha Falha no upload de todos os arquivos.
   - Para incluir somente os arquivos que falharam no upload para o Amazon S3 por um motivo específico, escolha Apenas motivos específicos de falha no upload. Depois, em Motivos de falha, selecione um ou mais dos seguintes motivos:
     - Classe de armazenamento inacessível: o gateway não consegue acessar a classe de armazenamento do Amazon S3 na qual o objeto está armazenado. Para obter mais informações, consulte Erro: InaccessibleStorageClass.
     - Estado de objeto inválido: o estado do arquivo no gateway não corresponde ao estado no Amazon S3. Para obter mais informações, consulte Erro: InvalidObjectState.
     - Objeto ausente: o objeto foi excluído ou movido no Amazon S3. Para obter mais informações, consulte Erro: ObjectMissing.
     - Acesso ao S3 negado: o perfil do IAM de acesso ao bucket do Amazon S3 não permite que o gateway realize a operação de upload. Para obter mais informações, consulte Erro: S3 AccessDenied.

   Note

   O sinalizador de arquivos com falha de upload é redefinido a cada 24 horas e durante a reinicialização do gateway. Se esse relatório capturar os arquivos após a redefinição, mas antes que eles sejam sinalizados novamente, eles não serão relatados como arquivos com falha de upload.

7. Em Usar um endpoint da VPC para se conectar ao S3?, realize uma das seguintes ações para especificar como o gateway se conectará ao bucket do Amazon S3:

   - Para se conectar diretamente sem usar a Amazon VPC, escolha Conectar-se diretamente ao bucket.

- Para pesquisar uma lista de endpoints existentes da Amazon VPC, escolha Escolher um endpoint da VPC e, depois, especifique um endpoint na lista suspensa Endpoints da VPC exibida.
- Para especificar um endpoint da Amazon VPC existente por seu nome DNS, escolha Insira o nome DNS de um endpoint da VPC e, depois, digite o nome DNS no campo Inserir nome DNS do endpoint da VPC exibido.

> **Note**
>
> Se seu compartilhamento de arquivos usa um endpoint da VPC para se conectar ao Amazon S3 para operações normais, recomendamos usar a mesma VPC ao configurar seu relatório de cache. A criação do relatório de cache falhará se o gateway não conseguir se conectar ao bucket do Amazon S3 por qualquer motivo, incluindo configuração de VPC inválida.

8. (Opcional) Em Tags: opcional, escolha Adicionar nova tag e insira uma chave e um valor para o seu relatório de cache.

   Uma tag é um par de chave-valor que diferencia maiúsculas de minúsculas e ajuda você a categorizar os recursos do Storage Gateway. Adicionar tags pode facilitar a filtragem e a pesquisa do seu relatório de cache. Repita essa etapa para adicionar até cinquenta tags.

9. Quando terminar, escolha Criar relatório.

   O Storage Gateway começa a gerar o relatório. Verifique o andamento e visualizar o status na guia Relatórios de cache da página de detalhes do compartilhamento de arquivos.

Visualizar e gerenciar relatórios de cache para seu Gateway de Arquivos do S3

Os relatórios de cache listam os arquivos que estão atualmente no cache local para um compartilhamento de arquivos específico, de acordo com os filtros e os critérios que você especificar. Você pode ver uma lista dos relatórios de cache existentes para um compartilhamento de arquivo específico, verificar o progresso e o status do relatório e excluir relatórios que não são mais necessários usando a AWS Storage Gateway API ou o console do Storage Gateway.

Para gerenciar relatórios de cache usando a API, consulte as seguintes seções na Referência de API do Storage Gateway:

- ListCacheReports
- DescribeCacheReport
- CancelCacheReport
- DeleteCacheReport

Para gerenciar relatórios de cache no console do Storage Gateway, use o procedimento a seguir.

Como gerenciar relatórios de cache 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 no lado esquerdo da página, escolha Compartilhamentos de arquivos e, depois, selecione o compartilhamento de arquivos para o qual você deseja gerenciar relatórios de cache.
3. Na página Detalhes do compartilhamento de arquivos, escolha a guia Relatórios de cache. Essa guia lista os relatórios de cache existentes para o compartilhamento de arquivos e contém informações sobre status, andamento e o caminho do objeto em que o arquivo de relatório está armazenado no Amazon S3.
4. Execute um destes procedimentos:
   - Para visualizar detalhes adicionais de um relatório específico, como o ARN do relatório e as tags associadas, escolha um relatório na coluna ID do relatório.
   - Para especificar vários relatórios a fim de gerenciar simultaneamente, selecione os relatórios utilizando a coluna da caixa de seleção.
5. Para gerenciar um ou mais relatórios, escolha uma das seguintes opções no menu suspenso Ações:
   - Excluir relatório de cache: exclui o registro do relatório de cache do banco de dados do Storage Gateway. Exclua registros de relatórios de cache obsoletos para abrir espaço para novos relatórios. Cada compartilhamento de arquivos pode ter até dez relatórios de cache a qualquer momento.

> **Note**
>
> A exclusão do registro do relatório em cache por meio desse procedimento não exclui o objeto do arquivo de relatório do Amazon S3.

- Cancelar relatório: cancela um relatório que está em andamento no momento. Cancele um relatório em andamento se você cometeu um erro durante a configuração do relatório ou se ele demorar muito para ser concluído. Quando solicitado, confirme o cancelamento.

> **Note**
>
> Os tempos de conclusão podem variar significativamente dependendo do número de arquivos no cache. Normalmente, a maioria dos relatórios é concluída em 5 minutos.

O console do Storage Gateway exibe uma mensagem indicando o resultado da ação de cancelamento ou exclusão.

Noções básicas sobre as informações fornecidas nos relatórios de cache do Gateway de Arquivos do S3.

Os relatórios de cache listam os arquivos que estão atualmente no cache local para um compartilhamento de arquivos específico, de acordo com os filtros e os critérios que você especificar. Cada relatório de cache inclui as seguintes informações:

- Bucket: o bucket ou o ponto de acesso do Amazon S3 associado ao compartilhamento de arquivos.
- S3 ObjectKey — O objeto Amazon S3 que armazena os dados e os metadados desse arquivo. Esse objeto tem os dados mais recentes cujo upload foi feito para o S3, mas podem estar faltando dados cujo upload não está sendo realizado para o S3.
- FilePath— O caminho do arquivo para a entrada do arquivo no cache do gateway. É onde você pode encontrar o arquivo ao montar e navegar no compartilhamento de arquivos.
- RenamedTo— O novo caminho de um arquivo renomeado. Quando você renomeia um arquivo no compartilhamento de arquivos, o gateway precisa rastrear a localização antiga e a nova dele. Esse campo mostra para onde o arquivo foi transferido, ajudando a controlar as operações de

renomeação, mesmo que um arquivo tenha sido renomeado várias vezes. Essas informações são particularmente úteis quando você precisa entender como os arquivos em seu compartilhamento de arquivos correspondem aos objetos em seu bucket do Amazon S3.

O exemplo a seguir mostra as entradas do relatório de cache em um cenário complexo envolvendo um arquivo que está sendo substituído diretamente no Amazon S3 e, ao mesmo tempo, renomeado por meio do Gateway de Arquivos. Nesse cenário, o gateway faz upload do arquivo `A.txt` para o S3 e, depois, remove o conteúdo dele para liberar espaço no cache local. O objeto do S3 associado é então substituído diretamente no S3, não por meio de uma ação realizada pelo gateway, o que gera um `InvalidObjectState` devido à incompatibilidade entre o objeto do S3 e o que o gateway espera. Ao mesmo tempo, o arquivo `A.txt` foi renomeado para `B.txt` por meio do gateway.

Bucket	S3 ObjectK	FilePat	Renam	Tipo	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplc	Upload or	SizeInB es	IsWholeFi leInCache
sample ket-iad	A.txt	/B.txt		FILE	TRUE	FALSE	FALSE	TRUE	InvalidO jectSta	4	FALSE
sample ket-iad	A.txt	/A.txt	/B.txt	FILE	TRUE	FALSE	TRUE	FALSE		4	FALSE

- Tipo: indica se a entrada é para um `FILE` ou `DIRECTORY`.
- IsDirty— Relata `TRUE` se há algum tipo de alteração no arquivo que não foi carregado no Amazon S3. Isso inclui alterações nos metadados, como nome do arquivo e read/write permissões, mesmo que os dados do arquivo não tenham sido alterados.
- IsDataDirty— Relata `TRUE` se há alterações nos dados do arquivo que não foram carregadas no Amazon S3.
- IsDeleted— Informa `TRUE` se o arquivo foi excluído no gateway. Se um arquivo for marcado como excluído, ele sempre será marcado como sujo.
- IsFailingToUpload— Relata `TRUE` se há um problema ao fazer o upload do arquivo para o Amazon S3. Esse status é redefinido a cada 24 horas para permitir que o gateway tente fazer upload novamente e confira se o problema foi resolvido. O gateway rejeita qualquer nova operação de gravação de um arquivo cujo upload não esteja sendo feito. Se o gateway não tiver o arquivo inteiro no cache, ele também rejeitará as operações de leitura.

- UploadError— O erro que está impedindo o upload do arquivo para o Amazon S3. Para acessar mais informações e as etapas recomendadas para resolver esses erros, consulte Solução de problemas: problemas do Gateway de Arquivos.
- SizeInBytes— O tamanho total do arquivo.
- IsWholeFileInCache— Relata TRUE se todos os dados do arquivo estão atualmente armazenados no cache do gateway. Se for TRUE para um arquivo cujo upload não foi feito para o Amazon S3, o gateway permitirá que o arquivo seja lido.

Manter seu gateway

Manter o Gateway de Arquivos do Amazon S3 envolve fazer manutenção geral para otimizar a performance 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 Gateway de Arquivos do Amazon S3:

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 existente Gateways de Arquivos do S3 com uma nova instância: saiba como substituir o Gateway de Arquivos do S3 por uma nova instância quando quiser melhorar a performance 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 Notas de versão do software do dispositivo de gateway.

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/home.
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/home.
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/home.

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 Kernel-based virtual Linux (KVM), VMware ESXi ou plataforma Microsoft Manager. Hyper-V
- 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 Linux Kernel-based Virtual Machine (KVM), VMware ESXi e Microsoft Manager. Hyper-V

Tópicos

Acessar o console local do gateway com o Linux KVM

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

Como acessar o console local do gateway com a KVM

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

   ```
   # virsh list
   ```

   O comando retorna uma lista de VMs com informações de ID, nome e estado de cada uma. 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 .

Acesso ao console local do gateway com o VMware ESXi

Para acessar o console local de seu gateway com VMware ESXi

1. No cliente VMware vSphere, selecione a VM de seu gateway.
2. Verifique se 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 .

Acesse o console local do Gateway com a Microsoft Hyper-V

Para acessar o console local do seu 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 hipervisores VMware Hyper-V, Microsoft 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/home.
2. No painel de navegação, selecione Gateways e escolha o gateway para o qual você deseja definir uma nova senha.
3. Em Actions (Ações), escolha Set Local Console Password (Definir senha do console local).
4. Na caixa de diálogo Set Local Console Password (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 o registro em log no console local do VMware ESXi, consulte Acesso ao console local do gateway com o VMware ESXi.
- Para obter mais informações sobre como fazer login no console Hyper-V local da Microsoft, consulteAcesse o console local do Gateway com a Microsoft Hyper-V.
- Para obter mais informações sobre como fazer login no console local da Máquina Kernel-Based Virtual Linux (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 o registro em log no console local do VMware ESXi, consulte Acesso ao console local do gateway com o VMware ESXi.
   - Para obter mais informações sobre como fazer login no console Hyper-V local da Microsoft, consulteAcesse o console local do Gateway com a 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 hipervisor VMware, você pode editar a configuração do adaptador neste 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 o registro em log no console local do VMware ESXi, consulte Acesso ao console local do gateway com o VMware ESXi.
   - Para obter mais informações sobre como fazer login no console Hyper-V local da Microsoft, consulteAcesse o console local do Gateway com a 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 o registro em log no console do VMware ESXi, consulte Acesso ao console local do gateway com o VMware ESXi.
   - Para obter mais informações sobre como fazer login no console Hyper-V local da Microsoft, consulteAcesse o console local do Gateway com a 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 o registro em log no console local do VMware ESXi, consulte Acesso ao console local do gateway com o VMware ESXi.
- Para obter mais informações sobre como fazer login no console Hyper-V local da Microsoft, consulteAcesse o console local do Gateway com a 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 no VMware ESXi, configurar o horário do host do hiperviso r e sincronizar o horário da VM com o host é suficiente para evitar desvios de horário. Para obter mais informações, consulte Sincronizar o tempo da VM com o tempo do host VMware. Para um gateway implantado na Microsoft Hyper-V, você deve verificar periodicamente a hora da sua VM. Para obter mais informações, consulte Sincronize a hora da VM com Hyper-V ou a hora do host 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 o registro em log no console local do VMware ESXi, consulte Acesso ao console local do gateway com o VMware ESXi.
   - Para obter mais informações sobre como fazer login no console Hyper-V local da Microsoft, consulteAcesse o console local do Gateway com a 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 filtragem de pacotes IPv4 e NAT.
ip6tables	Ferramenta de administração para filtragem de pacotes IPv6 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 Support ajude a solucionar problemas do seu gateway EC2 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.

Command	Função
tcptraceroute	Colete a saída de traceroute no tráfego TCP para um destino.
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

Para saber mais sobre esta tarefa	Consulte este tópico
Testar a conectividade de rede	Como testar a conectividade de rede do gateway
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.

Mensagem	Description
[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	Description
	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.

Command	Função
	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.
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 filtragem de pacotes IPv4 e NAT.
ip6tables	Ferramenta de administração para filtragem de pacotes IPv6 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.

Command	Função
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 existente Gateways de Arquivos do S3 com uma nova instância

> **Note**
>
> Se você estiver realizando uma migração de AL2 para AL2023 do Storage Gateway, antes de começar, certifique-se de ter concluído todos os itens da lista de verificação Pre-migration da campanha de migração de AL2 para AL2023 do Storage Gateway.

Você pode substituir um S3 File Gateway Gateway existente por uma nova instância à medida que suas necessidades de dados e desempenho aumentarem ou se você receber AWS uma 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.

Há dois métodos para substituir um Gateway de Arquivos do S3 existente. A tabela a seguir descreve as vantagens e desvantagens de cada método. Usando essas informações, selecione o método mais adequado para seu ambiente de gateway e, em seguida, consulte as etapas do procedimento na seção correspondente a seguir.

> **Note**
>
> Se você precisar entrar no novo console local do Storage Gateway para concluir qualquer um dos métodos, o nome de usuário inicial é admin e a senha temporária é password.

> **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.

	Método 1: migrar o disco de cache e o ID do gateway para a instância de substituição*	Método 2: substituir a instância por um disco de cache vazio e um novo ID de gateway
Dados do disco de cache	Os dados no disco de cache são preservados. Esse método será útil se o gateway tiver um disco de cache grande ou se as aplicaçõe s forem sensíveis ao atraso causado pelas operações de leitura fora do cache.	Os dados em cache são baixados da AWS nuvem. Esse método é ideal para workloads com muita gravação, caso suas aplicações possam tolerar o atraso causado por leituras fora do cache.

	Método 1: migrar o disco de cache e o ID do gateway para a instância de substituição*	Método 2: substituir a instância por um disco de cache vazio e um novo ID de gateway
Tempo de inatividade	Seu gateway ficará offline por 1 a 2 horas durante o processo de migração.	Os compartilhamentos de arquivos permanecem disponíveis, mas os clientes terão um curto tempo de inatividade para substituição ao alternar de um compartil hamento de arquivos para outro durante a transição para a nova instância. **Note** A gravação em um bucket do Amazon S3 de dois compartil hamentos de arquivos simultaneamente não compatível. Portanto, todos os clientes devem ser reassocia dos de um compartil hamento ao outro de maneira simultânea em vez de gradual.
ID do gateway	O novo gateway herda o ID do gateway que ele substitui.	O gateway existente e o gateway de substituição têm IDs separados e exclusivos.

	Método 1: migrar o disco de cache e o ID do gateway para a instância de substituição*	Método 2: substituir a instância por um disco de cache vazio e um novo ID de gateway
Implicação de custo	A preservação de dados em cache elimina a necessida de de novos downloads, resultando em zero custos adicionais do S3.	Esse método pode incorrer em custos adicionais, especialmente se a recuperaç ão de dados do S3 for necessária. Essa abordagem também pode resultar em despesas substanciais de recuperação de dados do S3 se os compartilhamentos de arquivos apoiados por buckets do S3 usarem classes de armazenamento como S3, S3 Intelligent-Tiering, S3 One Zone-IA ou objetos transferidos para o Standard-IA GLACIER por meio de políticas de ciclo de vida do S3. No caso de compartil hamentos de arquivos SMB, se a ACL raiz estiver configurada no compartil hamento de arquivos, ela deverá ser reaplicada ao gateway migrado. Essa ação aplicará a configuração recursivamente a todos os objetos no compartilhamento de arquivos, introduzindo algumas implicações de custo.

> **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 Arquivos do FSx para um Gateway de Arquivos do S3.

Método 1: migrar o disco de cache e o ID do gateway para a instância de substituição

Para migrar seu Gateways de Arquivos do S3do disco de cache e do ID do gateway para uma instância substituta:

1. Interrompa todas as aplicações que estejam gravando no Gateway de Arquivos do S3 existente.
2. Use as etapas a seguir para atualizar o gateway para a versão mais recente

   a. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/home.

   b. No painel de navegação, escolha Gateways e, em seguida, escolha o antigo S3 File Gateway que você deseja migrar.

   c. Escolha Atualizar agora, se disponível. Caso contrário, seu gateway já está na versão mais recente.
3. Verifique se a métrica `CachePercentDirty` na guia Monitoramento do Gateway de Arquivos do S3 existente é `0`.
4. Encerre o Gateway de Arquivos do S3 existente desligando a máquina virtual (VM) do host utilizando seus controles de hipervisor.

   Para acessar mais informações sobre como desligar uma instância do Amazon EC2, consulte Parar e iniciar sua instância no Guia do usuário do Amazon EC2.

   Para obter mais informações sobre como desligar um KVM, VMware ou Hyper-V VM, consulte a documentação do hipervisor.
5. Desanexe todos os discos, incluindo o disco raiz e os discos de cache da antiga VM do gateway.

> **Note**
>
> Anote a ID do volume do disco raiz, bem como a ID do gateway associada a este disco raiz. Você precisará desanexar esse disco do hipervisor do novo Storage Gateway em uma etapa posterior.

Se você estiver usando uma instância do Amazon EC2 como VM para seu Gateway de Arquivos do S3, consulte Desanexar um volume do Amazon EBS de uma instância do Windows ou Desanexar um volume do Amazon EBS de uma instância do Linux no Guia do usuário do Amazon EC2.

Para obter informações sobre como desanexar discos de um KVM, VMware ou Hyper-V VM, consulte a documentação do seu hipervisor.

6. Crie uma nova instância de VM hipervisor do S3 File Gateway, mas não a ative como gateway. Em uma etapa posterior, essa nova VM assumirá a identidade do antigo gateway.

   Para acessar mais informações sobre como criar uma VM com hipervisor do Storage Gateway, consulte Escolher uma plataforma host e baixar a VM.

   > **Important**
   >
   > Use uma imagem do S3 File Gateway para a nova VM. Uma imagem de um tipo de gateway diferente (por exemplo, Volume Gateway ou Tape Gateway) fará com que o gateway migrado falhe na inicialização.

   > **Note**
   >
   > Não adicione discos de cache para a nova VM. Essa VM usará os mesmos discos de cache que foram usados pela antiga VM.

> **Note**
>
> Depois de baixar a VM, feche o assistente do console. Não prossiga com a ativação neste momento.

7. Configure sua nova VM do Storage Gateway para utilizar as mesmas configurações de rede que a antiga VM.

   A configuração de rede padrão para o gateway é Dynamic Host Configuration Protocol (DHCP). Com o DHCP, um endereço IP é atribuído automaticamente ao seu gateway.

   Se você precisar configurar manualmente um endereço IP estático para sua VM do gateway, consulte Configurar parâmetros de rede.

   Se sua VM do gateway precisar usar um proxy Socket Secure versão 5 (SOCKS5) para se conectar à Internet, consulte Rotear seu gateway implantado no EC2 por meio de um proxy HTTP.

   > **Note**
   >
   > Você pode reutilizar o mesmo endereço IP estático ou nome de host da antiga VM do gateway para evitar a reconfiguração de clientes NFS ou SMB.

8. Inicie a nova VM do Storage Gateway.
9. Conecte todos os discos que você desconectou da VM do gateway antigo à nova VM do gateway. Isso inclui o disco raiz e o (s) disco (s) de cache do gateway antigo. Não desconecte o próprio disco raiz da VM do novo gateway.

   > **Note**
   >
   > Todos os discos devem permanecer inalterados para que a migração seja bem-sucedida. Alterar o tamanho do disco ou outros valores causa inconsistências nos metadados, o que impede a migração bem-sucedida.

10. Inicie o processo de migração do gateway conectando-se ao console local da nova VM do gateway ou fazendo solicitações da web ao endereço IP da nova VM do gateway (descrito abaixo).

a. Para usar o console local, selecione a opção Migrate Gateway e forneça seu ID de gateway existente quando solicitado. Você receberá instruções para copiar as configurações aplicadas anteriormente no gateway antigo para o novo gateway. Você pode optar por aplicá-las ou configurá-las manualmente posteriormente. Consulte Acessando o console local do Gateway.

b. Como alternativa, você pode iniciar o processo de migração do gateway conectando-se à nova VM com uma URL que usa o formato a seguir.

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

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

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

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

Quando o processo de migração do gateway for concluído com êxito, você verá uma mensagem confirmando a migração bem-sucedida.

11. Aguarde até que o status do gateway apareça como Em execução no console do AWS Storage Gateway . Dependendo da largura de banda disponível, isso pode levar até 10 minutos.
12. Interrompa a nova VM do Storage Gateway.
13. Desvincule o disco raiz do antigo gateway, cujo ID de volume você anotou anteriormente, do novo gateway.
14. Inicie a nova VM do Storage Gateway.
15. Se seu gateway estava inserido em um domínio do Active Directory, reinsira-o no domínio. Para receber instruções, consulte Usar o Active Directory para autenticar usuários.

> **Note**
>
> Conclua essa etapa mesmo que o status do Gateway de Arquivos do S3 apareça como Ingressado.

16. Se seu gateway estava usando o método de autenticação SMB Guest Access, a senha precisará ser digitada novamente. Para obter instruções, consulte Fornecer acesso de convidado ao seu compartilhamento de arquivos.
17. Confirme se os compartilhamentos estão disponíveis no endereço IP da nova VM do gateway.

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

Consulte mais informações sobre como excluir uma instância do Amazon EC2 em Encerrar uma instância no Guia do usuário do Amazon EC2. Para obter mais informações sobre como excluir um KVM, VMware ou Hyper-V VM, consulte a documentação do seu hipervisor.

Método 2: substituir a instância por um disco de cache vazio e um novo ID de gateway

Para configurar uma substituição Gateways de Arquivos do S3 instância com disco de cache vazio e novo ID de gateway:

1. Interrompa todas as aplicações que estejam gravando no Gateway de Arquivos do S3 existente. Verifique se a métrica `CachePercentDirty` na guia Monitoramento é `0` antes de configurar os compartilhamentos de arquivos no novo gateway.
2. Use o AWS Command Line Interface (AWS CLI) para coletar e salvar as informações de configuração sobre seu S3 File Gateway Gateway existente e compartilhamentos de arquivos fazendo o seguinte:

   a. Salve as informações de configuração do gateway para o Gateway de Arquivos do S3.

   ```
   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 Gateway de Arquivos do S3.

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

Esse comando produz um bloco JSON que contém metadados sobre o compartilhamento de arquivos SMB, como o nome de domínio, o status do Microsoft Active Directory, se a senha do convidado está definida e o tipo de estratégia de segurança.

c. Salve as informações de compartilhamento de arquivos para cada compartilhamento de arquivos SMB e Network File System (NFS) do Gateway de Arquivos do S3:

- Use o comando a seguir para compartilhamentos de arquivos SMB.

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

Esse comando gera um bloco JSON que contém metadados sobre o compartilhamento de arquivos SMB, como nome, classe de armazenamento, status, o nome do recurso da Amazon (ARN) do perfil do IAM, uma lista de clientes que têm permissão para acessar o Gateway de Arquivos do S3 e o caminho usado pelo cliente SMB para identificar o ponto de montagem.

- Use o comando a seguir para compartilhamentos de arquivos NFS.

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

Esse comando gera um bloco JSON que contém metadados sobre o compartilhamento de arquivos NFS, como nome, classe de armazenamento, status, ARN do perfil do IAM, uma lista de clientes que têm permissão para acessar o Gateway de Arquivos do S3 e o caminho usado pelo cliente NFS para identificar o ponto de montagem.

3. Crie um Gateway de Arquivos do S3 com as mesmas configurações que o gateway antigo. Se necessário, consulte as informações que você salvou na Etapa 2.
4. Crie outros compartilhamentos de arquivos para o novo gateway com as mesmas definições e configurações que os compartilhamentos de arquivos configurados no antigo gateway. Se necessário, consulte as informações que você salvou na Etapa 2.

> **Note**
>
> Agora você pode copiar as configurações de compartilhamento de arquivos entre gateways. Para obter mais informações, consulte Copiar um compartilhamento de arquivos.

5. Confirme se o novo gateway está funcionando corretamente e, em seguida, remap/cut transfira seus clientes dos compartilhamentos de arquivos antigos para os novos compartilhamentos de arquivos da maneira mais adequada ao seu 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 Gateway de Arquivos do S3, verifique se não há nenhuma aplicação gravando no momento no cache do 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 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 Hyper-V Microsoft Manager Kernel-based ou o cliente Linux Virtual Machine (KVM) para se conectar ao host e remover a VM. Observe que você não pode reutilizar a VM do gateway excluído para ativar um novo gateway.

Para excluir um gateway

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

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

4. Verifique se você deseja excluir os gateways especificados, digite a palavra excluir na caixa de confirmação e escolha Excluir.

5. (Opcional) Se você quiser fornecer feedback sobre o gateway excluído, preencha a caixa de diálogo de comentários e escolha Enviar. Caso contrário, selecione Interromper.

> **Important**
>
> Ao excluir um gateway, você 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. Se você não precisar dos dados nos buckets do Amazon S3 associados aos compartilhamentos de arquivos, você poderá optar por remover seus buckets do Amazon S3. Para receber instruções, consulte Excluir seu bucket.

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 S3 File Gateway Gateway

Nesta seção, você pode encontrar orientações para o provisionamento de hardware para sua VM do Gateway de Arquivos do S3. 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.
> Para instâncias do Amazon EC2, se você tiver mais de 5 milhões de objetos no seu bucket do S3 e estiver usando um volume SSD de uso geral, será necessário um volume mínimo de EBS raiz de 350 GiB para a performance aceitável do seu gateway durante a inicialização. Para obter informações sobre como aumentar o tamanho do volume, consulte Modificar um volume do EBS usando volumes elásticos (console).
> O limite de tamanho sugerido para diretórios individuais nos compartilhamentos 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 compartilhamentos de arquivos que são feitas pelo cache. As operações de leitura de solicitações não atendidas pelo cache são leituras dos compartilhamentos de arquivos que são feitas pelo Amazon S3.

As tabelas a seguir mostram exemplos de configurações do Gateway de Arquivos do S3.

Performance do Gateway de Arquivos do S3 em clientes Linux

Exemplos 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 Disco de cache: caches de 512 GiB, io1, 1.500 IOPS provision adas Desempenho mínimo da rede: 10 Gbps CPU: 16 vCPU | RAM: 32 GB	NFSv3 - 1 tópico	110 MiB/sec (0,92 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 fios	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	NFSv4 - 1 tópico	130 MiB/sec (1,1 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)
	NFSv4 - 8 fios	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 tópico	115 MiB/sec (1,0 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 fios	190 MiB/sec (1,6 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)

Exemplos 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
Protocolo NFS recomendado para Linux				
Dispositivo de hardware do Storage Gateway Desempenho mínimo da rede: 10 Gbps	NFSv3 - 1 tópico	265 MiB/sec (2,2 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 fios	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	NFSv4 - 1 tópico	310 MiB/sec (2,6 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)
	NFSv4 - 8 fios	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 tópico	275 MiB/sec (2,4 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 fios	455 MiB/sec (3,8 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)

Exemplos 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 Disco de cache: quatro discos de cache NVME de 2 TB. Desempenho mínimo da rede: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protocolo NFS recomendado para Linux	NFSv3 - 1 tópico	300 MiB/sec (2,5 Gbps)	590 MiB/sec (4,9 Gbps)	325 MiB/sec (2,7 Gbps)
	NFSv3 - 8 fios	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)
	NFSv4 - 1 tópico	355 MiB/sec (3,0 Gbps)	590 MiB/sec (4,9 Gbps)	340 MiB/sec (2,9 Gbps)
	NFSv4 - 8 fios	575 MiB/sec (4,8 Gbps)	590 MiB/sec (4,9 Gbps)	575 MiB/sec (4,8 Gbps)
	SMBV3 - 1 tópico	230 MiB/sec (1,9 Gbps)	325 MiB/sec (2,7 Gbps)	245 MiB/sec (2,0 Gbps)
	SMBV3 - 8 fios	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)

Performance do Gateway de Arquivos em clientes do Windows

Exemplos 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	SMBV3 - 1 tópico	150 MiB/sec (1,3 Gbps)	180 MiB/sec (1,5 Gbps)	20 MiB/sec (0,2 Gbps)

Exemplos 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 de cache: caches de 512 GiB, io1, 1.500 IOPS provisionadas Desempenho mínimo da rede: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protocolo SMB recomendado para Windows	SMBV3 - 8 fios	190 MiB/sec (1,6 Gbps)	335 MiB/sec (2,8 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 tópico	95 MiB/sec (0,8 Gbps)	130 MiB/sec (1,1 Gbps)	20 MiB/sec (0,2 Gbps)
	NFSv3 - 8 fios	190 MiB/sec (1,6 Gbps)	330 MiB/sec (2,8 Gbps)	190 MiB/sec (1,6 Gbps)
Dispositivo de hardware do Storage Gateway Desempenho mínimo da rede: 10 Gbps	SMBV3 - 1 tópico	230 MiB/sec (1,9 Gbps)	255 MiB/sec (2,1 Gbps)	20 MiB/sec (0,2 Gbps)
	SMBV3 - 8 fios	835 MiB/sec (7,0 Gbps)	475 MiB/sec (4,0 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 tópico	135 MiB/sec (1,1 Gbps)	185 MiB/sec (1,6 Gbps)	20 MiB/sec (0,2 Gbps)
	NFSv3 - 8 fios	545 MiB/sec (4,6 Gbps)	470 MiB/sec (4,0 Gbps)	190 MiB/sec (1,6 Gbps)

Exemplos 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 Disco de cache: quatro discos de cache NVME de 2 TB. Desempenho mínimo da rede: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protocolo SMB recomendado para Windows	SMBV3 - 1 tópico	230 MiB/sec (1,9 Gbps)	265 MiB/sec (2,2 Gbps)	30 MiB/sec (0,3 Gbps)
	SMBV3 - 8 fios	835 MiB/sec (7,0 Gbps)	780 MiB/sec (6,5 Gbps)	250 MiB/sec (2,1 Gbps)
	NFSv3 - 1 tópico	135 MiB/sec (1,1). (Gbps)	220 MiB/sec (1,8 Gbps)	30 MiB/sec (0,3 Gbps)
	NFSv3 - 8 fios	545 MiB/sec (4,6 Gbps)	570 MiB/sec (4,8 Gbps)	240 MiB/sec (2,0 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.

Orientação de performance para gateways com vários compartilhamentos de arquivos

O Gateway de Arquivos do Amazon S3 é compatível com a anexação de até cinquenta compartilhamentos de arquivos a um único dispositivo do Storage Gateway. Ao adicionar vários compartilhamentos de arquivos por gateway, você pode oferecer suporte a mais usuários e workloads enquanto gerencia menos gateways e recursos de hardware virtual. Além de outros fatores, o número de compartilhamentos de arquivos gerenciados por um gateway pode afetar a performance desse gateway. Esta seção descreve como se espera que a performance do gateway mude dependendo do número de compartilhamentos de arquivos anexados e recomenda configurações de hardware virtual para otimizar a performance de gateways que gerenciam vários compartilhamentos.

Em geral, o aumento do número de compartilhamentos de arquivos gerenciados por um único Storage Gateway pode ter as seguintes consequências:

- Maior tempo necessário para reiniciar o gateway.
- Maior utilização de recursos de hardware virtual, como vCPU e RAM.
- Diminuição da performance das operações de dados e metadados se os recursos de hardware virtual ficarem saturados.

A tabela a seguir lista as configurações recomendadas de hardware virtual para gateways que gerenciam vários compartilhamentos de arquivos:

Compartilhamentos de arquivos por gateway	Configuração recomendada de capacidade do gateway	Núcleos de vCPU recomendados	RAM recomendada	Tamanho recomendado do disco raiz			
1 a 10	Small	4 (tipo de instância do EC2 m4.xlarge	16 GiB	80 GiB			

Compartilhamentos de arquivos por gateway	Configuração recomendada de capacidade do gateway	Núcleos de vCPU recomendados	RAM recomendada	Tamanho recomendado do disco raiz			
		ou posterior)					
10 a 20	Médio	8 (tipo de instância do EC2 m4.2xlarge ou posterior)	32 GiB	160 GiB			
20+	Grande	16 (tipo de instância do EC2 m4.4xlarge ou posterior)	64 GiB	240 GiB			

Além das configurações de hardware virtual indicadas acima, recomendamos as seguintes práticas para configurar e manter dispositivos do Storage Gateway que gerenciam vários compartilhamentos de arquivos:

- Pense que o relacionamento entre o número de compartilhamentos de arquivos e a demanda colocada no hardware virtual do gateway não é necessariamente linear. Alguns compartilhamentos de arquivos podem gerar maior throughput e, portanto, maior demanda de hardware do que outros. As recomendações na tabela anterior são baseadas nas capacidades máximas de hardware e em vários níveis de throughput de compartilhamento de arquivos.
- Se você achar que adicionar vários compartilhamentos de arquivos a um único gateway reduz a performance, pense em transferir os mais ativos para outros gateways. Em particular, se um

compartilhamento de arquivos for usado para um very-high-throughput aplicativo, considere criar um gateway separado para esse compartilhamento de arquivos.

- Não recomendamos configurar um gateway para várias aplicações de alto throughput e outro para várias aplicações de baixo throughput. Em vez disso, tente distribuir uniformemente compartilhamentos de arquivos de alto e baixo throughput entre os gateways para equilibrar a saturação do hardware. Para medir o throughput do compartilhamento de arquivos, use as métricas `ReadBytes` e `WriteBytes`. Para acessar mais informações, consulte Noções básicas das métricas de compartilhamento de arquivos.

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 em 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. Third-partyauditores 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 em AWS Storage Gateway

O modelo de responsabilidade AWS compartilhada O modelo de 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 obter mais informações sobre privacidade de dados, consulte Perguntas frequentes sobre privacidade de dados . Para obter informações sobre proteção de dados na Europa, consulte o Centro de Regulamento Geral sobre a Proteção de Dados (RGPD).

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, a API ou AWS os SDKs. AWS CLI 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 Storage Gateway usa SSL/TLS (Secure Layers/Transport Socket Layer Security) para criptografar dados que são transferidos entre seu dispositivo de gateway e o armazenamento. AWS Por padrão, o Storage Gateway usa as chaves de S3-Managed criptografia da Amazon (SSE-S3) para criptografar no lado do servidor todos os dados que ele armazena no Amazon S3. Você tem a opção de usar a API Storage Gateway para configurar seu gateway para criptografar dados armazenados na nuvem usando criptografia do lado do servidor com AWS Key Management Service chaves (). SSE-KMS

Como criptografar um compartilhamento de arquivos

Você pode configurar os compartilhamentos de arquivos no seu S3 File Gateway para criptografar objetos armazenados com chaves AWS KMS gerenciadas usando ou. SSE-KMS DSSE-KMS Para obter informações sobre os métodos de criptografia de compartilhamentos de arquivos aceitos, consulte Criptografar objetos armazenados pelo Gateway de Arquivos no Amazon S3.

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 Amazon S3.
- Os usuários do IAM devem ter as permissões necessárias para chamar as operações AWS KMS da API. Para obter mais informações, consulte Como usar políticas do IAM com o AWS KMS no Guia do desenvolvedor do AWS Key Management Service .

> **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

- Gerenciar o acesso usando políticas
- Como AWS O Storage Gateway funciona com o IAM
- Identity-based exemplos de políticas para AWS Storage Gateway
- Solução de problemas AWS Identidade e acesso ao Storage Gateway
- Usar tags para controlar o acesso ao gateway e aos recursos
- Usar ACLs do Windows para limitar o acesso a compartilhamentos de arquivos SMB

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 Identidade e acesso ao Storage Gateway).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como AWS O Storage Gateway funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Identity-based exemplos de políticas para AWS Storage Gateway)

Autenticação com identidades

A autenticação é 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-raiz

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.

Identity-based políticas

Identity-based políticas são documentos de políticas de permissões JSON que você anexa a uma identidade (usuário, grupo ou função). 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.

Identity-based as políticas 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.

Resource-based políticas

Resource-based políticas são documentos de política 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.

Resource-based políticas 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 Serviços (SCPs): as SCPs especificam o número máximo de permissões para uma organização ou uma unidade organizacional no AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs): definem o número máximo de permissões disponíveis para recursos em suas contas. Consulte mais informações em Resource control policies (RCPs) no Guia do usuário do AWS Organizations .
- 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 AWS O 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 AWS Storage Gateway

Recurso do IAM	AWS Suporte SGW
Identity-based políticas	Sim
Resource-based políticas	Não

Recurso do IAM	AWS Suporte SGW
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Service-linked funções	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.

Identity-based políticas para AWS SGW

Compatível com políticas baseadas em identidade: sim

Identity-based políticas são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, um grupo de usuários ou uma função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos 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.

Identity-based exemplos de políticas para AWS SGW

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

Resource-based políticas dentro AWS SGW

Compatibilidade com políticas baseadas em recursos: não

Resource-based políticas são documentos de política 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 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. Identity-based exemplos de políticas para AWS Storage Gateway

Recursos políticos 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. Identity-based exemplos de políticas 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. Identity-based exemplos de políticas para AWS Storage Gateway

ACLs em AWS SGW

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes 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

Attribute-based controle de acesso (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 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.

Service-linked funções para AWS SGW

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 a função de realizar uma ação em seu nome. Service-

linked as funções aparecem no seu 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 de Service-linked função. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Identity-based exemplos de políticas 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 dos ARNs para cada um dos tipos de recursos, consulte Actions, Resources, and Condition Keys for AWS Storage Gateway na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Usar o AWS Console SGW
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de política

Identity-based as políticas determinam se alguém pode criar, acessar ou excluir recursos do 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.

Usar o AWS Console 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 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 em AWS SGW
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS para acessar meu AWS Recursos do SGW

Não estou autorizado a realizar uma ação em 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 Conta da AWS para acessar meu AWS Recursos do 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 compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), é possível 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 AWS O 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"
            }
         }
      }
   ]
}
```

Usar ACLs do Windows para limitar o acesso a compartilhamentos de arquivos SMB

O Gateway de Arquivos do Amazon S3 oferece suporte a dois métodos diferentes para controlar o acesso a arquivos e diretórios armazenados por meio de um compartilhamento de arquivos SMB: permissões POSIX ou ACLs do Windows.

Esta seção descreve como usar listas de controle de acesso (ACLs) em compartilhamentos de arquivos SMB que usam o Microsoft Active Directory (AD) para autenticação. Ao usar ACLs do Windows, você pode definir permissões refinadas em arquivos e pastas no seu compartilhamento de arquivos SMB.

Veja a seguir algumas características importantes de ACLs do Windows em compartilhamentos de arquivos SMB:

- As ACLs do Windows são selecionadas por padrão para compartilhamentos de arquivos SMB quando o Gateway de Arquivos é associado a um domínio do Active Directory.
- Quando as ACLs são ativadas, as informações da ACL são mantidas em metadados de objetos do Amazon S3.
- O gateway preserva até 10 ACLs por arquivo ou pasta.
- Quando você usa um compartilhamento de arquivos SMB com ACLs ativadas para acessar objetos do S3 criados fora de seu gateway, os objetos herdam as informações das ACLs da pasta principal.

> **Note**
>
> A ACL raiz padrão para um compartilhamento de arquivos SMB fornece acesso total a todos os usuários, mas você pode alterar as permissões da ACL raiz. É possível usar ACLs raiz para controlar o acesso ao compartilhamento de arquivos. Você pode definir quem pode montar o compartilhamento de arquivos (mapear a unidade) e quais permissões o usuário recebe para os arquivos e as pastas recursivamente no compartilhamento de arquivos. No entanto, recomendamos que definir essa permissão na pasta de nível superior no bucket do S3 para que sua ACL seja mantida.

Você pode ativar as ACLs do Windows ao criar um novo compartilhamento de arquivos SMB usando a operação de CreateSMBFileShareAPI. Ou você pode ativar as ACLs do Windows em um compartilhamento de arquivos SMB existente usando a operação de UpdateSMBFileShareAPI.

Ativar ACLs do Windows em um novo compartilhamento de arquivos SMB

Execute as etapas a seguir para ativar as ACLs do Windows em um novo compartilhamento de arquivos SMB.

Como ativar as ACLs do Windows ao criar um compartilhamento de arquivos SMB

1. Crie um gateway de arquivos se você ainda não tiver um. Para obter mais informações, consulte Como criar um gateway.
2. Se o gateway não tiver ingressado em um domínio, adicione-o a um domínio. Para obter mais informações, consulte Usar o Active Directory para autenticar usuários.
3. Crie um compartilhamento de arquivos SMB. Para obter mais informações, consulte .
4. Ative as ACLs do Windows no compartilhamento de arquivos por meio do console do Storage Gateway.

   Para usar o console do Storage Gateway, faça o seguinte:

   a. Escolha o compartilhamento de arquivos e selecione Edit file share (Editar o compartilhamento de arquivos).

   b. Para a opção de File/directory acesso controlado por, escolha Lista de Controle de Acesso do Windows.

5. (Opcional) Adicione um usuário administrador ao AdminUsersList, se quiser que o usuário administrador tenha privilégios para atualizar ACLs em todos os arquivos e pastas no compartilhamento de arquivos.

   > **Note**
   >
   > Se você tiver configurado as listas de Usuários e grupos permitidos e negados nas configurações do compartilhamento de arquivos SMB, as ACLs não concederão nenhum acesso que ignore essas listas.
   > As listas de Usuários e grupos permitidos e negados são avaliadas antes das ACLs e controlam quais usuários podem montar ou acessar o compartilhamento de arquivos. Se algum usuário ou grupo for colocado na lista Permitidos, a lista será considerada ativa e somente esses usuários poderão montar o compartilhamento de arquivos.
   > Depois que um usuário monta um compartilhamento de arquivos, as ACLs fornecem uma proteção mais granular que controla quais arquivos ou pastas específicos o usuário pode acessar.

6. Atualize as ACLs das pastas pai na pasta raiz. Para fazer isso, use o Explorador de Arquivos do Windows para configurar as ACLs em pastas no compartilhamento de arquivos SMB.

   > **Note**
   >
   > Se você configurar as ACLs na raiz em vez de na pasta principal na raiz, as permissões da ACL não serão mantidas no Amazon S3.

   Recomendamos definir ACLs na pasta de nível superior na raiz do seu compartilhamento de arquivos, em vez de definir ACLs diretamente na raiz do compartilhamento de arquivos. Essa abordagem mantém as informações como metadados de objeto no Amazon S3.

7. Ative a herança conforme apropriado.

   > **Note**
   >
   > Você pode ativar a herança para compartilhamentos de arquivos criados após 8 de maio de 2019.

Se você ativar a herança e atualizar as permissões de forma recursiva, o Storage Gateway atualizará todos os objetos no bucket do S3. Dependendo do número de objetos no bucket, a atualização pode demorar um pouco para ser concluída.

Ativar ACLs do Windows em um compartilhamento de arquivos SMB existente

Execute as etapas a seguir para ativar as ACLs do Windows em um compartilhamento de arquivos SMB existente com permissões POSIX.

Como ativar as ACLs do Windows em um compartilhamento de arquivos SMB existente usando o console do Storage Gateway

1. Escolha o compartilhamento de arquivos e selecione Edit file share (Editar o compartilhamento de arquivos).
2. Para a opção de File/directory acesso controlado por, escolha Lista de Controle de Acesso do Windows.
3. Ative a herança conforme apropriado.

> **Note**
>
> Não recomendamos definir as ACLs no nível raiz porque, se você fizer isso e excluir seu gateway, precisará redefinir as ACLs novamente.

Se você ativar a herança e atualizar as permissões de forma recursiva, o Storage Gateway atualizará todos os objetos no bucket do S3. Dependendo do número de objetos no bucket, a atualização pode demorar um pouco para ser concluída.

Limitações ao usar ACLs do Windows

Mantenha os seguintes limites em mente ao usar as ACLs do Windows para controlar o acesso a compartilhamentos de arquivos SMB:

- As ACLs do Windows são aceitas somente em compartilhamentos de arquivos que usam o Active Directory para autenticação quando você utiliza clientes SMB do Windows para acessar os compartilhamentos de arquivos.
- Os gateways de arquivos comportam um máximo de 10 entradas de ACL para cada arquivo e diretório.

- Os Gateways de Arquivos não aceitam as entradas `Audit` e `Alarm`, que são entradas da lista de controle de acesso do sistema (SACL). Os Gateways de Arquivos aceitam as entradas `Allow` e `Deny`, que são entradas da lista de controle de acesso discricionário (DACL).
- Os Gateways de Arquivos não são compatíveis com permissões de entradas de controle de acesso (ACEs) avançadas.
- As configurações de ACL raiz de compartilhamentos de arquivos SMB estão apenas no gateway, e as configurações são mantidas em atualizações e reinicializações de gateway.

> **Note**
>
> Se você configurar as ACLs na raiz em vez de na pasta principal na raiz, as permissões da ACL não serão mantidas no Amazon S3.

Dadas essas condições, faça o seguinte:

- Se você configurar vários gateways para acessar o mesmo bucket do Amazon S3, configure a ACL raiz em cada um dos gateways para manter as permissões consistentes.
- Se você excluir um compartilhamento de arquivos e recriá-lo no mesmo bucket do Amazon S3, use o mesmo conjunto de ACLs raiz.

Validação de conformidade AWS Storage Gateway

Third-party os auditores avaliam a segurança e a conformidade do AWS Storage Gateway como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, ENS High, OSPAR e HITRUST CSF. K-ISMS

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. AWS HIPAA-compliant
- 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 em 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 região da Região da AWS consiste em no mínimo três AZs isoladas e fisicamente separadas em 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 energia, resfriamento e segurança física independentes e está conectada por redes redundantes de latência ultrabaixa. Se a implantação exigir um foco na alta disponibilidade, você poderá configurar serviços e recursos em várias 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 AZs é criptografado. A performance da rede é suficiente para realizar a replicação síncrona entre AZs. As AZs facilitam os serviços e recursos de particionamento para oferecer alta disponibilidade. Se uma implantação for particionada entre AZs, você terá níveis melhores de isolamento e proteção de recursos contra determinados problemas, como falta de energia elétrica, raios, tornados, terremotos e muito mais. As AZs estão separadas fisicamente por uma distância significativa de qualquer outra AZ, embora todas estejam a no máximo 100 km (60 milhas) de distância umas das outras.

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 Usar VMware vSphere High Availability com o Storage Gateway.

Segurança da infraestrutura em AWS Storage Gateway

Como um 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 oferecer suporte a pacotes de criptografia com sigilo direto perfeito (PFS), como Ephemeral (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta 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 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

Veja a seguir informações sobre as práticas recomendadas e a solução de problemas relacionados a gateways, plataformas de host, compartilhamentos de arquivos, alta disponibilidade, recuperação de dados e segurança. 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 em compartilhamento de arquivos: saiba mais sobre ações que você pode adotar se enfrentar problemas inesperados em seu compartilhamento de arquivos.

- 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. • 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.
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

Problema	Medida a ser tomada
	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.
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.

Solução de problemas: verificações de segurança mostram portas NFS abertas

Algumas portas NFS são habilitadas por padrão, mesmo em gateways que você usa somente com compartilhamentos de arquivos SMB. Se você usa um software de segurança de terceiros, como o Qualys, para verificar a rede em que o Gateway de Arquivos está implantado, os resultados da verificação poderão indicar essas portas NFS abertas como uma possível vulnerabilidade de segurança. Se você usa seu gateway somente com compartilhamentos de arquivos SMB e deseja desabilitar as portas NFS não utilizadas por motivos de segurança, siga o procedimento abaixo:

Para desabilitar as portas NFS em um Gateway de Arquivos:

1. Acesse o prompt de comando do console local do gateway utilizando o procedimento descrito em Como executar comandos do Storage Gateway no console local.
2. Digite os seguintes comandos para desabilitar o tráfego NFS:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ```

```
ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. Digite o comando a seguir para confirmar se as portas NFS bloqueadas aparecem nas tabelas IP:

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

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, consulteAcesso ao console local do gateway com o VMware ESXi.
   - Microsoft Hyper-V: para obter mais informações, consulte Acesse o console local do Gateway com a 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	Esse erro pode ocorrer pelos seguintes motivos:

Problema	Medida a ser tomada
seguinte mensagem de erro: “A server error occurred while attempting to import the virtual machine. Import 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”.	• 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: `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 Implantar um host padrão do Amazon EC2 para o Gateway de Arquivos do S3.

Para obter informações sobre como usar o armazenamento temporário, consulte Usar o armazenamento temporário com gateways do EC2.

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: 1344 (0x00000540)

Ao migrar arquivos para o Amazon S3, você pode encontrar `ERROR 1344 (0x00000540)` um se estiver tentando copiar arquivos com mais de 10 entradas de controle de acesso ACEs () para o Amazon S3. As entradas de controle de acesso são listadas na lista de controle de acesso (ACL).

O Gateway de Arquivos do Amazon S3 só pode preservar dez entradas ACE por determinado arquivo ou pasta.

Para resolver o erro 1344: copiar a segurança NTFS para o diretório de destino.

Reduza o número de entradas nas permissões do Windows para arquivos ou pastas que contenham mais de dez entradas. Uma abordagem comum é criar um grupo com a lista completa de entradas e, depois, substituir a lista de entradas por esse único grupo. Quando o número de entradas for menor que dez, você poderá tentar copiar novamente os arquivos ou pastas para o gateway.

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: InaccessibleStorageClass

Você pode ver o erro `InaccessibleStorageClass` quando um objeto é transferido para fora da classe de armazenamento Amazon S3 Standard.

O Gateway de Arquivos geralmente encontra esse erro quando tenta fazer upload de um objeto ou ler o objeto do bucket do Amazon S3. Geralmente, esse erro significa que o objeto foi transferido para o Amazon Glacier e está na classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

Seu Gateway de Arquivos do S3 pode gerar um relatório em cache que lista todos os arquivos do cache do gateway cujo upload atualmente falha para o Amazon S3 devido a esse erro. As informações neste relatório podem ajudá-lo a Suporte resolver problemas com sua configuração de gateway, Amazon S3 ou IAM. Para acessar mais informações, consulte Criar um relatório de cache.

Para resolver um InaccessibleStorageClass erro

- Restaure o objeto da classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive para a classe de armazenamento original no S3.

  Se você restaurar o objeto para o bucket do S3 a fim de corrigir um erro de upload, o upload do arquivo acabará ocorrendo. Se você transferir o objeto a fim de corrigir um erro de leitura, o cliente SMB ou NFS do Gateway de Arquivos poderá, então, ler o arquivo.

Erro: InvalidObjectState

Você pode receber um erro `InvalidObjectState` quando um gravador diferente do Gateway de Arquivos determinado modifica o arquivo especificado no bucket do Amazon S3 estabelecido. Como resultado, o estado do arquivo do Gateway de Arquivos não corresponde ao seu estado no Amazon S3. Todos os uploads subsequentes do arquivo para o Amazon S3 ou as recuperações do arquivo do Amazon S3 falharão.

Seu Gateway de Arquivos do S3 pode gerar um relatório de cache que lista todos os arquivos no cache do gateway cujo upload atualmente não estão sendo feito para o Amazon S3 devido a esse erro. As informações neste relatório podem ajudá-lo a Suporte resolver problemas com sua configuração de gateway, Amazon S3 ou IAM. Para acessar mais informações, consulte Criar um relatório de cache.

Para resolver um InvalidObjectState erro

Se a operação que modifica o arquivo for `S3Upload` ou `S3GetObject`, faça o seguinte:

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB ou NFS (você precisará dessa cópia de arquivo na etapa 4). Se a versão do arquivo no Amazon S3 for a mais recente, baixe essa versão. Você pode fazer isso usando o Console de gerenciamento da AWS ou AWS CLI.
2. Exclua o arquivo no Amazon S3 usando o Console de gerenciamento da AWS ou. AWS CLI
3. Exclua o arquivo do Gateway de Arquivos utilizando o cliente SMB ou NFS.
4. Copie a versão mais recente do arquivo que você salvou na etapa 1 para o Amazon S3 utilizando seu cliente SMB ou NFS. Faça isso por meio do Gateway de Arquivos.

Erro: ObjectMissing

Você pode receber o erro `ObjectMissing` quando um gravador diferente do Gateway de Arquivos determinado exclui o arquivo especificado do bucket do S3. Todos os uploads subsequentes para o Amazon S3 ou as recuperações do Amazon S3 para o objeto falham.

Seu Gateway de Arquivos do S3 pode gerar um relatório de cache que lista todos os arquivos no cache do gateway cujo upload não está sendo feito para o Amazon S3 devido a esse erro. As informações neste relatório podem ajudá-lo a Suporte resolver problemas com sua configuração de gateway, Amazon S3 ou IAM. Para acessar mais informações, consulte Criar um relatório de cache.

Para resolver um ObjectMissing erro

Se a operação que modifica o arquivo for `S3Upload` ou `S3GetObject`, faça o seguinte:

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB ou NFS (você precisará dessa cópia de arquivo na etapa 3).
2. Exclua o arquivo do Gateway de Arquivos utilizando o cliente SMB ou NFS.
3. Copie a versão mais recente do arquivo que você salvou na etapa 1 utilizando seu cliente SMB ou NFS. Faça isso por meio do Gateway de Arquivos.

Erro: RoleTrustRelationshipInvalid

Você recebe esse erro quando o perfil do IAM de um compartilhamento de arquivos tem um relacionamento de confiança do IAM configurado incorretamente (ou seja, o perfil do IAM não confia na entidade principal do Storage Gateway chamada `storagegateway.amazonaws.com`). Como resultado, o Gateway de Arquivos não poderia receber as credenciais para executar nenhuma operação no bucket do S3 que comporte o compartilhamento de arquivos.

Para resolver um RoleTrustRelationshipInvalid erro

- Use o console do IAM ou a API do IAM para incluir `storagegateway.amazonaws.com` como principal o que seu compartilhamento de arquivos confia IAMrole. Para obter informações sobre a função do IAM, consulte Tutorial: delegar acesso entre AWS contas usando funções do IAM.

Erro: S3 AccessDenied

Você pode receber um `S3AccessDenied` erro na função de acesso ao bucket AWS Identity and Access Management (IAM) do Amazon S3 de um compartilhamento de arquivos. Nesse caso, o perfil do IAM de acesso ao bucket do S3 que é especificado pelo `roleArn` no erro não permite a operação envolvida. A operação não é permitida devido às permissões para os objetos no diretório especificado pelo prefixo do Amazon S3.

Seu Gateway de Arquivos do S3 pode gerar um relatório de cache que lista todos os arquivos no cache do gateway cujo upload atualmente não estão sendo feito para o Amazon S3 devido a esse erro. As informações neste relatório podem ajudá-lo a Suporte resolver problemas com sua configuração de gateway, Amazon S3 ou IAM. Para acessar mais informações, consulte Criar um relatório de cache.

Para resolver um erro do S3 AccessDenied

- Modifique a política de acesso do Amazon S3 anexada ao `roleArn` no log de integridade do Gateway de Arquivos para conceder permissões para a operação do Amazon S3. Verifique se a política de acesso concede permissão para a operação que causou o erro. Além disso, conceda permissão para o diretório especificado no log para `prefix`. Para acessar informações sobre as permissões do Amazon S3, consulte Especificar permissões em uma política no Guia do usuário do Amazon Simple Storage Service.

  Essas operações podem fazer com que ocorra um erro `S3AccessDenied`.

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

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: verificações de segurança mostram portas NFS abertas

Algumas portas NFS são habilitadas por padrão, mesmo em gateways que você usa somente com compartilhamentos de arquivos SMB. Se você usa um software de segurança de terceiros, como o Qualys, para verificar a rede em que o Gateway de Arquivos está implantado, os resultados da verificação poderão indicar essas portas NFS abertas como uma possível vulnerabilidade de segurança. Se você usa seu gateway somente com compartilhamentos de arquivos SMB e deseja desabilitar as portas NFS não utilizadas por motivos de segurança, siga o procedimento abaixo:

Para desabilitar as portas NFS em um Gateway de Arquivos:

1. Acesse o prompt de comando do console local do gateway utilizando o procedimento descrito em Como executar comandos do Storage Gateway no console local.
2. Digite os seguintes comandos para desabilitar o tráfego NFS:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

3. Digite o comando a seguir para confirmar se as portas NFS bloqueadas aparecem nas tabelas IP:

   IPv4

```
iptables -n -L -v --line-numbers
```

IPv6

```
ip6tables -n -L -v --line-numbers
```

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
- O gateway não está respondendo
- O gateway demora a transferir dados para o Amazon S3
- Seu gateway está realizando mais operações do Amazon S3 do que o esperado
- Não é possível ver arquivos no bucket do Amazon S3
- O trabalho de backup do gateway falha ou há erros quando você grava no gateway

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 Amazon FSx 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 bucket S3 relacionado e as recomendações para melhorar o desempenho com base em 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.

O gateway demora a transferir dados para o Amazon S3

Se o Gateway de Arquivos estiver demorando a transferir dados para o Amazon S3, faça o seguinte:

- Caso a métrica `CachePercentDirty` seja 80 ou mais, significa que o Gateway de Arquivos está gravando dados mais depressa no disco do que consegue fazer upload deles para o Amazon S3. Pense em aumentar a largura de banda para upload do Gateway de Arquivos, adicionar um ou mais discos de cache ou desacelerar as gravações do cliente.
- Se 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.

- Se `S3PutObjectRequestTime`, `S3UploadPartRequestTime` ou `S3GetObjectRequestTime` forem altos, pode haver um gargalo na rede. Tente analisar sua rede para verificar se o gateway tem a largura de banda esperada.

Seu gateway está realizando mais operações do Amazon S3 do que o esperado

Se o seu Gateway de Arquivos estiver executando mais operações do Amazon S3 do que o esperado, confira a métrica `FilesRenamed`. As operações de renomeação são caras para serem executadas no Amazon S3. Otimize seu fluxo de trabalho para minimizar o número de operações de renomeação.

Não é possível ver arquivos no bucket do Amazon S3

Se você perceber que os arquivos no gateway não aparecem no bucket do Amazon S3, confira a métrica `FilesFailingUpload`. 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.

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 Amazon FSx 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 Amazon FSx 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.

Para o NFS, verifique se o cliente está montado usando uma montagem rígida em vez de uma montagem flexível.

Solução de problemas: problemas em compartilhamento de arquivos

Você pode encontrar informações a seguir sobre as ações a adotar se enfrentar problemas inesperados em um compartilhamento de arquivos.

Tópicos

O compartilhamento de arquivos travou no estado CRIANDO, ATUALIZANDO ou EXCLUINDO

O status do compartilhamento de arquivos resume a integridade do compartilhamento de arquivos. Se o compartilhamento de arquivos do S3 File Gateway estiver preso no `DELETING` estado

`CREATINGUPDATING`, ou, use as etapas de solução de problemas a seguir para identificar e resolver o problema.

Confirme as permissões da função e a relação de confiança do IAM

A função AWS Identity and Access Management (IAM) associada ao seu compartilhamento de arquivos deve ter permissões suficientes para acessar o bucket do Amazon S3. Além disso, a política de confiança da função deve conceder permissões ao serviço Storage Gateway para assumir a função.

Para verificar as permissões da função do IAM:

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Escolha a função do IAM associada ao seu compartilhamento de arquivos.
4. Selecione a guia Trust relationships (Relações de confiança).
5. Confirme se o Storage Gateway está listado como uma entidade confiável. Se o Storage Gateway não for uma entidade confiável, escolha Editar relação de confiança e adicione a seguinte política:

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

6. Verifique se a função do IAM tem as permissões corretas e se o bucket do Amazon S3 está listado como um recurso na política do IAM. Para obter mais informações, consulte Conceder acesso a um bucket do Amazon S3.

> **Note**
>
> Para evitar problemas confusos de prevenção delegada entre serviços, use uma política de relacionamento de confiança que inclua chaves de contexto de condição. Para obter mais informações, consulte the section called “Prevenção contra o ataque do “substituto confuso” em todos os serviços”.

Verifique se o AWS STS está ativado em sua região

Os compartilhamentos de arquivos podem ficar presos no `UPDATING` estado `CREATING` ou se AWS Security Token Service (AWS STS) estiver desativado em sua AWS região.

Para verificar o status do AWS STS:

1. Abra o AWS Identity and Access Management console em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Configurações da conta.
3. Na seção Security Token Service (STS), verifique se o status está ativo para a AWS região em que você deseja criar o compartilhamento de arquivos.
4. Se o status for Inativo, escolha Ativar para ativar AWS STS nessa região.

Verifique se o bucket S3 existe e segue as regras de nomenclatura

Seu compartilhamento de arquivos requer um bucket válido do Amazon S3 que siga as convenções de nomenclatura do Amazon S3.

Para verificar seu bucket do S3:

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Confirme se o bucket do Amazon S3 mapeado para seu compartilhamento de arquivos existe. Se o bucket não existir, crie-o. Depois de criar o bucket, o status do compartilhamento de arquivos deve mudar para`AVAILABLE`. Para obter mais informações, consulte Criar um bucket no Guia do usuário do Amazon Simple Storage Service.
3. Verifique se o nome do seu bucket está em conformidade com as regras de nomenclatura do bucket no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> O S3 File Gateway não é compatível com buckets do Amazon S3 com pontos `.` () no nome do bucket.

Forçar a exclusão de um compartilhamento de arquivos travado no estado EXCLUINDO

Quando você exclui um compartilhamento de arquivos, o gateway remove o compartilhamento do bucket Amazon S3 associado. No entanto, os dados que estão sendo carregados no momento continuam sendo carregados antes que a exclusão seja concluída. Durante esse processo, o compartilhamento de arquivos mostra um `DELETING` status.

> **Important**
>
> Verifique a CloudWatch métrica da Amazon `CachePercentDirty` para seu gateway para determinar quantos dados estão pendentes de upload. Para obter mais informações sobre as métricas do Storage Gateway, consultethe section called “Monitorando seu gateway de arquivos S3, gateway de ”.

Se você não quiser esperar que todos os uploads em andamento terminem, você pode forçar a exclusão do compartilhamento de arquivos.

Para forçar a exclusão de um compartilhamento de arquivos:

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/.
2. No painel de navegação, escolha Compartilhamentos de arquivos.
3. Selecione o compartilhamento de arquivos que você deseja excluir.
4. Escolha a guia Detalhes e revise a mensagem Este compartilhamento de arquivos está sendo excluído.
5. Verifique a ID do compartilhamento de arquivos na mensagem e selecione a caixa de confirmação.

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

6. Escolha Forçar exclusão agora.

Como alternativa, você pode usar o AWS CLI delete-file-sharecomando com o `--force-delete` parâmetro definido como`true`.

> **Important**
>
> Antes de forçar a exclusão de um compartilhamento de arquivos, confirme se o gateway não está em um `OFFLINE` estado. Se o gateway estiver off-line, primeiro resolva o problema off-line. Para obter mais informações, consulte the section called “Solucionar problemas de gateway off-line”.

Se a máquina virtual (VM) do gateway já tiver sido excluída, você deverá excluir o gateway do console do Storage Gateway para remover todos os compartilhamentos de arquivos associados, incluindo aqueles presos no `DELETING` estado. Para obter mais informações, consulte the section called “Como excluir o gateway e remover recursos”.

Solucionar problemas de conectividade de rede

Problemas de rede podem impedir que seu compartilhamento de arquivos saia do estado `CREATINGUPDATING`, ou`DELETING`. Os problemas comuns de rede incluem:

- Seu gateway está off-line ou a VM do gateway foi excluída.
- O acesso à rede entre o Storage Gateway e o endpoint do serviço Amazon S3 está bloqueado.
- O endpoint Amazon S3 Amazon VPC que o gateway usa para se comunicar com o Amazon S3 foi excluído.
- As portas de rede necessárias não estão abertas ou o roteamento de rede está configurado incorretamente.

Teste a conectividade do S3 a partir do console local do gateway

Para testar a conectividade do S3:

1. Faça login no console local do gateway. Para obter mais informações, consulte the section called “Fazer login no console local do Gateway de Arquivos”.
2. No menu principal Storage Gateway - Configuração, insira o número correspondente ao Teste de conectividade do S3.
3. Escolha o tipo de endpoint do Amazon S3:
   - Para o tráfego do Amazon S3 que flui por meio de um gateway de Internet, gateway NAT, gateway de trânsito ou gateway do Amazon S3 Gateway, endpoint Amazon VPC, escolha Público.
   - Para o tráfego do Amazon S3 que flui por meio de um endpoint Amazon VPC da interface do Amazon S3, escolha VPC (). PrivateLink
   - Para um endpoint FIPS, escolha a opção FIPS.
4. Insira a região do bucket do Amazon S3.
5. Se estiver usando um endpoint Amazon VPC, insira o nome DNS do endpoint Amazon S3 Amazon VPC (por exemplo,). `vpce-0329c2790456f2d01-0at85l34`

O gateway executa automaticamente um teste de conectividade que valida a conexão de rede e a conexão SSL. Se o teste falhar:

- Falha no teste de rede - geralmente causada por regras de firewall, configurações de grupos de segurança ou roteamento de rede incorreto. Verifique se as portas necessárias estão abertas e se o roteamento de rede está configurado corretamente.
- Falha no teste SSL - Indica que a inspeção SSL ou a inspeção profunda de pacotes está ocorrendo entre a VM do gateway e os endpoints do serviço Amazon S3. Desative o SSL e a inspeção profunda de pacotes para o tráfego do Storage Gateway.

Verificar a configuração do proxy

Se o gateway usa um servidor proxy, verifique se o proxy não está bloqueando a comunicação de rede.

Para verificar a configuração do proxy:

1. No menu principal Storage Gateway - Configuration, insira o número correspondente à configuração do proxy HTTP/SOCKS.
2. Selecione a opção para visualizar a configuração atual do proxy de rede.
3. Se um proxy estiver configurado, verifique se o tráfego do Amazon S3 pode fluir do Storage Gateway para o servidor proxy pela porta 3128 (ou sua porta de ouvinte configurada) e, em seguida, para o endpoint do Amazon S3 pela porta 443.
4. Confirme se o proxy ou firewall permite o tráfego de e para as portas de rede e os endpoints de serviço exigidos pelo Storage Gateway. Para obter mais informações, consulte as portas de rede necessárias.

Se os problemas persistirem, você poderá remover temporariamente a configuração do proxy para determinar se o proxy está causando o problema.

Verifique os grupos de segurança e o roteamento de rede

- Para gateways no Amazon EC2 - Confirme se o grupo de segurança tem a porta 443 aberta para os endpoints do Amazon S3. Verifique se a tabela de rotas da sub-rede do Amazon EC2 roteia adequadamente o tráfego do Amazon S3 para os endpoints do Amazon S3. Para obter mais informações, consulte as portas de rede necessárias.
- Para gateways locais - Confirme se as regras de firewall permitem as portas necessárias e se as tabelas de rotas locais roteiam adequadamente o tráfego do Amazon S3 para os endpoints do Amazon S3. Para obter mais informações, consulte as portas de rede necessárias.
- VPC endpoints — Verifique se o endpoint Amazon S3 Amazon VPC usado pelo gateway não foi excluído. Se o endpoint da Amazon VPC for excluído e o gateway não tiver um endereço IP público, o gateway não poderá se comunicar com o Amazon S3.

Você não consegue criar um compartilhamento de arquivos

1. Se não conseguir criar um compartilhamento de arquivos porque o compartilhamento está paralisado no status CREATING, verifique se o bucket do S3 ao qual você associa seu compartilhamento de arquivos existe. Para obter informações sobre como fazer isso, consulte o tópico precedente, O compartilhamento de arquivos travou no estado CRIANDO, ATUALIZANDO ou EXCLUINDO.

2. Se o bucket do S3 existir, verifique se ele AWS Security Token Service está ativado na região em que você está criando o compartilhamento de arquivos. Se um token de segurança não estiver ativo, você deverá ativá-lo. Para obter informações sobre como ativar um token usando AWS Security Token Service, consulte Como ativar e desativar o AWS STS em uma AWS região no Guia do usuário do IAM.

Os compartilhamentos de arquivos SMB não permitem vários métodos diferentes de acesso

Os compartilhamentos de arquivo SMB possuem as seguintes restrições:

1. Quando o mesmo cliente tenta montar um compartilhamento de arquivos SMB com acesso de convidado e do Active Directory, a seguinte mensagem de erro é exibida: `Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Um usuário do Windows não pode permanecer conectado a dois compartilhamentos de arquivos SMB com acesso de convidado, e pode ser desconectado quando uma nova conexão com acesso de convidado é estabelecida.
3. Um cliente Windows não pode montar um compartilhamento de arquivos SMB com acesso de convidado e um do Active Directory exportado pelo mesmo gateway.

Vários compartilhamentos de arquivos não conseguem gravar no bucket do S3 associado

Não é recomendável configurar o bucket do S3 para permitir que vários compartilhamentos de arquivos gravem nele. Esse procedimento pode provocar resultados imprevisíveis.

Em vez disso, é recomendável permitir que apenas um compartilhamento de arquivos grave em cada bucket do S3. Você cria uma política de bucket para permitir que apenas a função associada ao compartilhamento de arquivos grave no bucket. Para acessar mais informações, consulte Práticas recomendadas do Gateway de Arquivos.

Notificação para um grupo de logs excluído ao usar logs de auditoria

Se o grupo de logs não existir, o usuário poderá selecionar o link do grupo de logs abaixo dessa mensagem para criar outro ou usar um existente como destino dos logs de auditoria.

Não é possível fazer upload de arquivos para o bucket do S3

Se não conseguir fazer upload de arquivos para o bucket do S3, faça o seguinte:

1. Verifique se você concedeu a permissão de acesso necessária para o Gateway de Arquivos do Amazon S3 fazer upload de arquivos para o bucket do S3. Para obter mais informações, consulte Conceder acesso a um bucket do Amazon S3.
2. Verifique se a função que criou o bucket tem permissão para gravar no bucket do S3. Para acessar mais informações, consulte Práticas recomendadas do Gateway de Arquivos.
3. Se o seu gateway de arquivos usa SSE-KMS ou DSSE-KMS para criptografia, certifique-se de que a função do IAM associada ao compartilhamento de arquivos inclua as permissões kms:encrypt, kms:decrypt, kms: *, kms: e kms:. ReEncrypt GenerateDataKey DescribeKey Para acessar mais informações, consulte Usar políticas baseadas em identidade (políticas do IAM) para o Storage Gateway.

Não é possível alterar a criptografia padrão para a SSE-KMS para criptografar os objetos armazenados no meu bucket do S3

Se você alterar a criptografia padrão e tornar a SSE-KMS (criptografia no lado do servidor com as chaves gerenciadas pelo AWS KMS) padrão para o bucket do S3, os objetos armazenados pelo Gateway de Arquivos do Amazon S3 no bucket não serão criptografados com a SSE-KMS. Por padrão, um Gateway de Arquivos usa a criptografia no lado do servidor gerenciada com o Amazon S3 (SSE-S3) quando grava dados em um bucket do S3. Alterar o padrão não altera automaticamente a criptografia.

Para alterar a criptografia para usar o SSE-KMS com sua própria AWS KMS chave, você deve ativar a criptografia SSE-KMS. Para fazer isso, forneça o nome de recurso da Amazon (ARN) da chave do KMS ao criar o compartilhamento de arquivos. Você também pode atualizar as configurações do KMS para seu compartilhamento de arquivos usando a operação de API `UpdateNFSFileShare` ou `UpdateSMBFileShare`. Essa atualização se aplica a objetos armazenados nos buckets do S3 após a atualização. Para obter mais informações, consulte Criptografia de dados usando AWS KMS.

As alterações feitas diretamente em um bucket do S3 com o versionamento de objetos ativado podem afetar o que você vê no seu compartilhamento de arquivos.

Se seu bucket do S3 tiver objetos gravados nele por outro cliente, sua visualização do bucket do S3 pode não ser up-to-date resultado do controle de versão do objeto do bucket do S3. Você deve sempre atualizar seu cache antes de examinar arquivos de interesse.

Versionamento de objeto é um recurso de bucket do S3 opcional que ajuda a proteger dados ao armazenar múltiplas cópias do objeto de mesmo nome. Cada cópia tem um valor de ID separado, por exemplo `file1.jpg`: `ID="xxx"` e `file1.jpg`: `ID="yyy"`. O número de objetos com nomes idênticos e suas vidas são controlados por políticas de ciclo de vida do Amazon S3. Para ver mais detalhes sobre esses conceitos do Amazon S3, consulte Usar versionamento e Gerenciamento do ciclo de vida de objetos no Guia do desenvolvedor do Amazon S3.

Quando você exclui um objeto versionado, esse objeto será sinalizado com um marcador de exclusão, mas retido. Somente um proprietário do bucket do S3 pode excluir permanentemente um objeto com o controle de versão habilitado.

Em seu Gateway de Arquivos do S3, os arquivos mostrados são as versões mais recentes dos objetos em um bucket do S3 no momento em que o objeto foi buscado ou o cache foi atualizado. O Gateway de Arquivos ignora quaisquer versões mais antigas ou quaisquer objetos marcados para exclusão. Ao ler um arquivo, você lê os dados da versão mais recente. Quando você gravar um arquivo em seu compartilhamento de arquivos, o Gateway de Arquivos do S3 criará outra versão de um objeto nomeado com suas alterações, e essa versão se torna a mais recente.

Seu Gateway de Arquivos do S3 continua a ler a versão anterior, e as atualizações que você faz são baseadas na versão anterior caso uma nova versão deva ser adicionada ao bucket do S3 fora da sua aplicação. Para ler a versão mais recente de um objeto, use a ação da RefreshCacheAPI ou atualize a partir do console conforme descrito emAtualizar o cache de objetos do bucket do Amazon S3.

> **Important**
>
> Não recomendamos que objetos ou arquivos sejam gravados em seu bucket do S3 do Gateway de Arquivos de fora do compartilhamento de arquivos.

Ao gravar em um bucket do S3 com o versionamento ativado, o Gateway de Arquivos do Amazon S3 pode criar várias versões dos objetos do Amazon S3

Com o versionamento de objetos ativado, você pode ter várias versões de um objeto criado no Amazon S3 em cada atualização de um arquivo do seu cliente NFS ou SMB. Veja abaixo alguns cenários que podem gerar a criação de várias versões de um objeto em seu bucket do S3:

- Quando um arquivo é modificado no Gateway de Arquivos do Amazon S3 por um cliente NFS ou SMB após o upload para o Amazon S3, o Gateway de Arquivos do S3 faz upload dos dados novos ou modificados em vez de fazer upload do arquivo inteiro. A modificação do arquivo gera a criação de uma versão do objeto do Amazon S3.
- Quando um arquivo é gravado no Gateway de Arquivos do S3 por um cliente NFS ou SMB, o Gateway de Arquivos do S3 faz upload dos dados do arquivo para o Amazon S3 seguidos por seus metadados (propriedades, carimbos de data/hora etc.). O upload dos dados do arquivo cria um objeto do Amazon S3, e o upload dos metadados atualiza os metadados do objeto do Amazon S3. Esse processo cria outra versão do objeto, gerando duas versões dele.
- Quando o Gateway de Arquivos do S3 está fazendo upload de arquivos maiores, talvez seja necessário fazer upload de partes menores do arquivo antes que o cliente termine de gravar no Gateway de Arquivos. Alguns motivos para isso são liberar espaço no cache ou uma alta taxa de gravações em um arquivo. Isso pode gerar diversas versões de um objeto no bucket do S3.

Monitore seu bucket do S3 para saber quantas versões de um objeto existem antes de configurar políticas de ciclo de vida a fim de migrar objetos para diferentes classes de armazenamento. Configurar a expiração do ciclo de vida das versões anteriores para minimizar o número de versões de um objeto em seu bucket do S3. O uso da replicação na mesma região (SRR) ou a replicação entre regiões (CRR) entre buckets do S3 aumentará o armazenamento usado. Para acessar mais informações sobre a replicação, consulte Replicação.

> **Important**
>
> Não configure a replicação entre buckets do S3 até entender quanto armazenamento está sendo utilizado quando o versionamento de objetos está ativado.

O uso de buckets do S3 versionados pode aumentar significativamente a quantidade de armazenamento no Amazon S3, pois cada modificação em um arquivo cria uma versão do objeto do S3. Por padrão, o Amazon S3 continua armazenando todas essas versões, a não ser que você crie especificamente uma política para substituir esse comportamento e limitar o número de versões que são mantidas. Se você observar uso de armazenamento grande incomum com versionamento de objetos ativado, confira se você tem políticas de armazenamento definidas adequadamente. Um aumento no número de respostas de `HTTP 503-slow down` para solicitações de navegador também pode ser o resultado de problemas com o versionamento de objetos.

Se você ativar o versionamento de objetos após a instalação de um Gateway de Arquivos do S3, todos os objetos exclusivos serão retidos (`ID="NULL"`) e você poderá ver todos eles no sistema de arquivos. Novas versões de objetos recebem um ID exclusivo (versões mais antigas são retidas). Com base no carimbo de data e hora do objeto, apenas o objeto versionado mais recentemente é visualizável no sistema do arquivo NFS.

Depois de ativar o versionamento de objetos, o bucket do S3 não pode ser retornado para um estado sem versionamento. Você pode, contudo, suspender o versionamento. Quando você suspender o versionamento, um novo objeto recebe um ID. Se o mesmo objeto nomeado existe com um valor de `ID="NULL"`, a versão mais antiga será substituída. No entanto, qualquer versão que contém um ID que não é `NULL` é retida. Os carimbos de data e hora identificam o novo objeto como o atual, e é aquele que aparece no sistema de arquivos NFS.

Alterações em um bucket do S3 não são exibidas no Storage Gateway

O Storage Gateway atualiza o cache do compartilhamento de arquivos automaticamente quando você grava arquivos no cache localmente utilizando o compartilhamento de arquivos. No entanto, o Storage Gateway não atualiza automaticamente o cache quando você faz upload de um arquivo direto para o Amazon S3. Ao fazer isso, realize uma operação `RefreshCache` para ver as alterações no compartilhamento de arquivos. Se você tiver mais de um compartilhamento de arquivos, deverá realizar a operação `RefreshCache` em cada um.

Você pode atualizar o cache utilizando o console do Storage Gateway e a AWS Command Line Interface (AWS CLI):

- Para atualizar o cache utilizando o console do Storage Gateway, consulte Atualizar objetos no bucket do Amazon S3.
- Como atualizar o cache utilizando a AWS CLI:

  1. Execute o comando `aws storagegateway list-file-shares`

2. Copie o número do recurso da Amazon (ARN) do compartilhamento de arquivos no cache que deseja atualizar.
3. Execute o comando `refresh-cache` com seu ARN como valor para `--file-share-arn`:

```
aws storagegateway refresh-cache --file-share-arn
arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
```

Para automatizar a `RefreshCache` operação, consulte Como posso automatizar a RefreshCache operação no Storage Gateway?

As permissões da ACL não estão funcionando como esperado

Se as permissões da lista de controle de acesso (ACL) não estiverem funcionando conforme esperado com o compartilhamento de arquivos SMB, você pode executar um teste.

Para fazer isso, primeiro teste as permissões em um servidor de arquivos do Microsoft Windows ou um compartilhamento de arquivos do Windows local. Em seguida, compare o comportamento com o compartilhamento de arquivos do gateway.

Ocorreu deterioração da performance do gateway depois de uma operação recursiva

Em alguns casos, você pode realizar uma operação recursiva, como renomear um diretório ou ativar a herança para uma ACL, e forçar para baixo na árvore. Se você fizer isso, o Gateway de Arquivos do S3 aplicará recursivamente a operação a todos os objetos no compartilhamento de arquivos.

Por exemplo, suponha que você aplique a herança a objetos existentes em um bucket do S3. O Gateway de Arquivos do S3 aplica recursivamente a herança a todos os objetos no bucket. Essas operações podem causar queda de desempenho do gateway.

Notificações de integridade de alta disponibilidade

Ao executar 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

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

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 de de arquivos para o bucket Amazon S3 FSx 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 Implantar um host padrão do Amazon EC2 para o Gateway de Arquivos do S3.

2. Crie um no gateway do EC2 que você criou. Para obter mais informações, consulte Criar um compartilhamento de arquivos .
3. Monte seu de compartilhamento de arquivos em seu cliente e mapeie-o para o bucket S3 FSx que contém os dados que você deseja recuperar. Para obter mais informações, consulte Montar e usar um compartilhamento de arquivos.

Práticas recomendadas: gerenciar uploads fragmentados

Quando você transfere arquivos grandes, o Gateway de Arquivos do S3 usa o recurso de upload fragmentado do Amazon S3 para dividir os arquivos em partes menores e transferi-los em paralelo para melhorar a eficiência. Para obter mais informações sobre o upload fragmentado, consulte Fazer upload e copiar objetos usando o upload fragmentado no Guia do usuário do Amazon Simple Storage Service.

Se um upload fragmentado não for concluído com êxito por algum motivo, o gateway normalmente interromperá a transferência, excluirá todas as partes do arquivo parcialmente transferido do Amazon S3 e tentará realizar a transferência novamente. Em casos raros, como quando uma falha de hardware ou de rede impede que o gateway seja limpo após um upload fragmentado malsucedido, as partes do arquivo parcialmente transferido poderão permanecer no Amazon S3, onde podem gerar cobranças de armazenamento.

Como prática recomendada para minimizar os custos de armazenamento do Amazon S3 decorrentes de uploads fragmentados incompletos, recomendamos configurar uma regra de ciclo de vida do bucket do Amazon S3 que use a ação de API `AbortIncompleteMultipartUpload` para interromper automaticamente transferências malsucedidas e excluir as partes de arquivo associadas após um número de dias específico. Para conferir instruções, consulte Configurar um ciclo de vida de um bucket para excluir uploads fragmentados incompletos no Guia do usuário do Amazon Simple Storage Service.

Práticas recomendadas: descompactar arquivos compactados localmente antes de copiar para um gateway

Se você tentar descompactar um arquivo que contém milhares de arquivos enquanto ele estiver armazenado no gateway, poderá haver atrasos significativos relacionados ao desempenho. O processo de descompactar um arquivo que contém um grande número de arquivos em qualquer tipo de compartilhamento de arquivos de rede envolve inerentemente um alto volume de input/output

operações, manipulação do cache de metadados, sobrecarga da rede e latência. Além disso, o Storage Gateway não consegue determinar quando cada arquivo do arquivamento terminou de ser descompactado e pode começar a fazer upload de arquivos antes que o processo seja concluído, o que afeta ainda mais o desempenho. Esses problemas são agravados quando os arquivos dentro do arquivamento são numerosos, mas pequenos.

Como prática recomendada, indicamos primeiro transferir arquivos compactados do gateway para a máquina local, antes de descompactá-los. Depois, se necessário, você poderá usar uma ferramenta, como robocopy ou rsync, para transferir os arquivos descompactados de volta para o gateway.

Reter os atributos de arquivo ao copiar dados do Windows Server

É possível copiar arquivos para o seu Gateway de Arquivos utilizando o comando `copy` básico no Microsoft Windows, mas esse comando copia somente os dados de arquivo por padrão, omitindo determinados atributos, como descritores de segurança. Se os arquivos forem copiados para o gateway sem as restrições de segurança correspondentes e as informações da lista de controle de acesso discricionário (DACL), é possível que eles possam ser acessados por usuários não autorizados.

Como prática recomendada para preservar todos os atributos de arquivo e informações de segurança quando você copia arquivos para o gateway no Microsoft Windows Server, recomendamos usar os comandos `robocopy` ou `xcopy`, com os sinalizadores `/copy:DS` ou `/o`, respectivamente. Para obter mais informações, consulte robocopy e xcopy na documentação de referência de comandos do Microsoft Windows Server.

Práticas recomendadas: dimensionamento adequado dos discos de cache

Para ter o melhor desempenho, o tamanho total do disco de cache deve ser grande o suficiente para cobrir o tamanho do seu conjunto em uso ativo. Para read/write cargas de trabalho mistas e com muita leitura, isso garante que você possa obter uma alta porcentagem de acessos ao cache nas leituras, o que é desejável. Você pode monitorar isso por meio da métrica `CacheHitPercent` do Gateway de Arquivos do S3.

Para workloads de uso intenso de gravação (por exemplo, para backup e arquivamento), o Gateway de Arquivos do S3 armazena em buffer as gravações recebidas no cache do disco antes de copiar esses dados de forma assíncrona para o Amazon S3. Você deve garantir que tenha capacidade

de cache suficiente para armazenar dados gravados em buffer. A `CachePercentDirty` métrica fornece uma indicação da porcentagem do cache de disco que ainda não foi mantida. AWS

Valores baixos de `CachePercentDirty` são desejáveis. Valores consistentemente próximos de 100% indicam que o Gateway de Arquivos do S3 não consegue acompanhar a taxa de tráfego de gravação recebido. Você pode evitar isso aumentando a capacidade do cache de disco provisionado ou aumentando a largura de banda da rede dedicada disponível do Gateway de Arquivos do S3 para o Amazon S3, ou ambos.

Para obter mais informações sobre o dimensionamento do disco de cache, consulte as melhores práticas de dimensionamento de cache do Amazon S3 File Gateway no canal oficial da Amazon Web Services. YouTube

Trabalhar com vários compartilhamentos de arquivos e buckets do Amazon S3

Quando você configura um único bucket do Amazon S3 para permitir que vários gateways ou compartilhamentos de arquivos gravem nele, os resultados podem ser imprevisíveis. Você pode configurar os buckets de duas maneiras para evitar resultados imprevisíveis. Escolha o método mais adequado para seu caso de uso entre as seguintes opções:

- Configure os buckets do S3 para que somente um compartilhamento de arquivos possa gravar em cada bucket. Use um compartilhamento de arquivos diferente para gravar em cada bucket.

  Para evitar isso, crie uma política de bucket do S3 que negue todos os perfis exceto o perfil usado para o compartilhamento de arquivos específico inserir ou excluir objetos no bucket. Anexe uma política semelhante a cada bucket, especificando um compartilhamento de arquivos diferente para gravar em cada bucket.

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

  JSON

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

```
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

- Se você quiser que vários compartilhamentos de arquivos gravem no mesmo bucket do Amazon S3, deverá evitar que os compartilhamentos de arquivos tentem gravar nos mesmos objetos simultaneamente.

  Para fazer isso, configure um prefixo de objeto separado e exclusivo para cada compartilhamento de arquivos. Isso significa que cada compartilhamento de arquivos grava somente em objetos com o prefixo correspondente e não grava em objetos associados aos outros compartilhamentos de arquivos em sua implantação. Configure o prefixo do objeto no campo Nome do prefixo do S3 ao criar um compartilhamento de arquivos.

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.
- Usar o Storage Gateway com o 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.
- Suporte para atributos de arquivo: saiba como um gateway lida com os atributos de arquivo do DOS e do Windows.
- 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.
- Noções básicas sobre recursos e IDs de recurso- 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 do Open-source: 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.
- Usar classes de armazenamento: saiba mais sobre as classes de armazenamento do Amazon S3 aceitas pelo Gateway de Arquivos e o que considerar ao escolher uma classe de armazenamento.
- Usar drivers da CSI do Kubernetes: saiba como instalar e configurar os drivers da Container Storage Interface (CSI) para permitir que as instâncias do Kubernetes usem o Gateway de Arquivos para armazenamento.

- Módulo Terraform: saiba como usar o Terraform para implantar o Gateway de Arquivos como uma máquina virtual.

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

- Implantar um host padrão do Amazon EC2 para o Gateway de Arquivos do S3
- Implantar um host personalizado do Amazon EC2 para o Gateway de Arquivos do S3
- Modificar as opções de metadados da instância do Amazon EC2
- Sincronize a hora da VM com Hyper-V ou a hora do host Linux KVM
- Sincronizar o tempo da VM com o tempo do host VMware
- Como configurar adaptadores de rede para o gateway
- Como usar o VMware vSphere High Availability com o Storage Gateway

Implantar um host padrão do Amazon EC2 para o Gateway de Arquivos do S3

Este tópico lista as etapas para implantar um host Amazon EC2 usando as especificações padrão.

É possível implantar e ativar um Gateway de Arquivos do Amazon S3 em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). A Imagem de máquina da Amazon (AMI) do AWS Storage Gateway está disponível como uma AMI de comunidade.

> **Note**
>
> As AMIs de comunidade do Storage Gateway são publicadas e totalmente apoiadas pela AWS. Você pode ver que o editor é AWS um provedor verificado.

1. Para configurar a instância do Amazon EC2, escolha Amazon EC2 como Plataforma host na seção Opções da plataforma do fluxo de trabalho. Para receber instruções sobre como

configurar a instância do Amazon EC2, consulte Implantar uma instância do Amazon EC2 para hospedar o Gateway de Arquivos do Amazon S3.

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.

     - Auto-assign IP público — Ativado
     - 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				
111	TCP e UDP	NFSv3				
139	TCP e UDP	SMB				
445	TCP	SMB				
2049	TCP e UDP	NFS				
20048	TCP e UDP	NFSv3				

- 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				
IOPS	3000	3000				
Excluir no encerramento	Sim	Sim				
Encriptado	Não	Não				
Throughput	125	125				

Implantar um host personalizado do Amazon EC2 para o Gateway de Arquivos do S3

É possível implantar e ativar um Gateway de Arquivos do Amazon S3 em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). A Imagem de máquina da Amazon (AMI) do AWS Storage Gateway está disponível como uma AMI de comunidade.

> **Note**
>
> As AMIs de comunidade do Storage Gateway são publicadas e totalmente apoiadas pela AWS. Você pode ver que o editor é AWS um provedor verificado.

As AMIs do Gateway de Arquivos do S3 usam a convenção de nomenclatura a seguir. O número da versão anexado ao nome da AMI muda a cada lançamento da versão. `aws-storage-gateway-FILE_S3-1.25.0`

Como implantar uma instância do Amazon EC2 para hospedar o Gateway de Arquivos do Amazon S3

1. Comece a conectar um novo gateway de fitas usando o console do Storage Gateway. Para obter instruções, consulte Configurar um Gateway de Arquivos do Amazon S3. 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, particularmente de i3 do EC2, usam discos SSD NVMe. 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 for0. 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 IP Auto-assign público, escolha Habilitar.
7. Na subseção Firewall (grupos de segurança), revise as configurações pré-definidas. É possível alterar o nome padrão e a descrição do novo grupo de segurança a ser criado para sua instância do Amazon EC2, se quiser, ou optar por aplicar regras de firewall de um grupo de segurança existente.
8. Na subseção Regras de grupos de segurança de entrada, adicione regras de firewall para abrir as portas que os clientes usarão para se conectar à sua instância. Para obter mais informações sobre as portas necessárias para o Gateway de Arquivos do Amazon S3, consulte Requisitos de porta. Para obter mais informações sobre regras de firewall, consulte Regras de grupo de segurança no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

   > **Note**
   >
   > O Gateway de Arquivos do Amazon S3 exige que a porta TCP 80 esteja aberta para tráfego de entrada e para o acesso HTTP único durante a ativação do gateway. Após a ativação, será possível fechar essa porta.
   > Se você planeja criar compartilhamentos de arquivos NFS, deve abrir a TCP/UDP porta 2049 para acesso NFS, a porta 111 para acesso NFSv3 e TCP/UDP a TCP/UDP porta 20048 para acesso NFSv3.
   > Se você planeja criar compartilhamentos de arquivos SMB, deve abrir a porta TCP 445 para acesso SMB.

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 retorne à página Configurar gateway no console do Storage Gateway para retomar a configuração do Gateway de Arquivos do Amazon S3.

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 Gateway de Arquivos do Amazon S3. 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_S3/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_S3/latest
```

O comando da CLI retorna uma saída semelhante à seguinte:

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_S3/latest",
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

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 de entrada que usam IMDS Versão 1 (IMDSv1) ou exigir que todas as solicitações de metadados usem IMDS Versão 2 (IMDSv2). O IMDSv2 usa solicitações orientadas para sessão e mitiga vários tipos de vulnerabilidades que podem ser usadas para tentar acessar o IMDS. Para obter mais informações sobre o IMDSv2, consulte Como o serviço de metadados de instância versão 2 funciona no Manual do usuário do Amazon Elastic Compute Cloud.

Recomendamos que você exija o IMDSv2 para todas as instâncias do Amazon EC2 que hospedam o Storage Gateway. O IMDSv2 é exigido por padrão em todas as instâncias de gateway recém-lançadas. Se você tem instâncias que ainda estão configuradas para aceitar solicitações de metadados do IMDSv1, consulte Exigir o uso de IMDSv2 no Manual do usuário do Amazon Elastic Compute Cloud para obter instruções sobre como modificar as opções de metadados da instância para exigir o uso do IMDSv2. A aplicação dessa alteração não exige a reinicialização da instância.

Sincronize a hora da VM com Hyper-V ou a hora do host Linux KVM

Para um gateway implantado no VMware ESXi, definir o tempo de host do hipervisor e sincronizar o tempo da máquina virtual com o host é suficiente para evitar a deriva de tempo. Para obter mais informações, consulte Sincronizar o tempo da VM com o tempo do host VMware. Para um gateway implantado no KVM Microsoft Hyper-V ou Linux, recomendamos que você verifique periodicamente a hora 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 como fazer login no console Hyper-V local da Microsoft, consulteAcesse o console local do Gateway com a Microsoft Hyper-V.
   - Para obter mais informações sobre como fazer login no console local da Máquina Kernel-based Virtual Linux (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.

Sincronizar o tempo da VM com o tempo do host VMware

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, Ferramentas VMware 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 do host vSphere no painel esquerdo e 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 o 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

- Configurar o Gateway para várias NICs em um host do VMware ESXi
- Configurando seu gateway para várias NICs no Microsoft Host Hyper-V

Configurar o Gateway para várias NICs em um host do VMware ESXi

O procedimento a seguir pressupõe que a VM do gateway já tem um adaptador de rede definido e que você está adicionando um segundo adaptador no VMware ESXi.

Para configurar um adaptador de rede adicional no host do VMware ESXi para seu gateway

1. Encerre o gateway.
2. No cliente VMware vSphere, selecione a VM de seu gateway.

   A VM pode permanecer ativada para esse procedimento.
3. No cliente, abra o menu de contexto (clique com o botão direito do mouse) da VM do gateway e escolha Editar COnfigurações.
4. Na guia Hardware da caixa de diálogo Propriedades da Máquina Virtual, escolha Adicionar para adicionar um dispositivo.
5. Siga o assistente Add Hardware para adicionar um adaptador de rede.

   a. No painel Tipo de Dispositivo, escolha Adaptador Ethernet para adicionar um adaptador e em seguida Seguinte.

   b. No painel Tipo de Rede, confirme se Connect at power on está selecionada para Tipo e escolha Seguinte.

      É recomendável usar o adaptador de rede VMXNET3 com o Storage Gateway. Para obter mais informações sobre o tipo de adaptador que pode ser exibido na lista de adaptadores, consulte Network Adapter Types em ESXi and vCenter Server Documentation.

   c. No painel Pronto para Completar, reveja as informações e escolha Terminar.
6. Escolha a guia Resumo da VM e escolha Visualizar tudo, ao lado da caixa Endereço IP. A janela Endereços IP da Máquina Virtual exibe todos os endereços IP que podem ser usados para acessar o gateway. Confirme se um segundo endereço IP é listado para o gateway.

> **Note**
>
> Pode demorar vários minutos para as alterações do adaptador entrarem em vigor e as informações resumidas da VM atualizarem.

7. No console do Storage Gateway, ative o gateway.
8. No painel Navegação do console do Storage Gateway, escolha Gateways e o gateway ao qual você adicionou o adaptador. Confirme se o segundo endereço IP está listado na guia Details.

> **Note**
>
> Os exemplos de comandos de montagem fornecidos na página de informações de um compartilhamento de arquivos no console do Storage Gateway sempre incluirão o endereço IP do adaptador de rede que foi adicionado mais recentemente ao gateway associado ao compartilhamento de arquivos.

Para obter informações sobre tarefas de console local comuns aos hosts VMware e KVM Hyper-V, consulte Realizar tarefas no console local da máquina virtual

Configurando seu gateway para várias NICs no Microsoft Host Hyper-V

O procedimento a seguir pressupõe que a VM do gateway já tem um adaptador de rede definido e que você está adicionando um segundo adaptador. Este procedimento mostra como adicionar um adaptador para um Hyper-V host da Microsoft.

Para configurar seu gateway para usar um adaptador de rede adicional em um Microsoft Hyper-V Host

1. No console do Storage Gateway, desative o gateway.
2. No Microsoft Hyper-V Manager, selecione sua 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. Right-click o nome da VM do gateway para abrir o menu de contexto e, em seguida, 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.

> **Note**
>
> Os exemplos de comandos de montagem fornecidos na página de informações de um compartilhamento de arquivos no console do Storage Gateway sempre incluirão o endereço IP do adaptador de rede que foi adicionado mais recentemente ao gateway associado ao compartilhamento de arquivos.

Para obter informações sobre tarefas de console local comuns aos hosts VMware e KVM Hyper-V, consulte Realizar tarefas no console local da máquina virtual

Como usar o VMware vSphere High Availability com o Storage Gateway

O Storage Gateway fornece uma alta disponibilidade no VMware por meio de um conjunto de verificações de integridade no nível da aplicação integradas à Alta Disponibilidade do VMware vSphere (VMware HA). Essa abordagem ajuda a proteger as cargas de trabalho de armazenamento contra falhas de hardware, de hipervisor ou de rede. Ela também ajuda a proteger contra erros de software, como tempos limite de conexão e compartilhamento de arquivos ou indisponibilidade de volume.

Com essa integração, um gateway implantado em um ambiente VMware 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 HA:

- Implante o pacote .ova do VMware ESX 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 seguintes tópicos descrevem como implantar o Storage Gateway em um cluster VMware HA:

Tópicos

Configurar o cluster do vSphere VMware HA

Primeiro, se você ainda não tiver criado um cluster do VMware, crie um. Para obter informações sobre como criar um cluster do VMware, consulte Create a vSphere HA Cluster na documentação do VMware.

Depois, configure o cluster do VMware para trabalhar com o Storage Gateway.

Como configurar o cluster do VMware

1. Na página Edit Cluster Settings (Editar configurações do cluster) no VMware vSphere, verifique se o monitoramento da VM está configurado para monitoramento de VM e aplicativos. Para isso, defina os seguintes valores para cada opção:

   - Host Failure Response (Resposta à falha do host): Restart VMs (Reiniciar VMs)

- Response for Host Isolation (Resposta ao isolamento do host): Shut down and restart VMs (Desligar e reiniciar VMs)
- Datastore with PDL (Armazenamento de dados com PDL): Disabled (Desativado)
- Datastore with APD (Armazenamento de dados com APD): Disabled (Desativado)
- VM Monitoring (Monitoramento de VM): VM and Application Monitoring (Monitoramento de VM e aplicativos)

2. Fine-tune a sensibilidade do cluster ajustando os seguintes valores:

   - Intervalo de falha: após esse intervalo, a VM será reiniciada se uma pulsação da VM não for recebida.
   - Tempo mínimo de atividade: o cluster aguarda esse tempo depois que uma VM começa a monitorar as pulsações das ferramentas de VM.
   - Redefinições máximas por VM: define o máximo de vezes que o cluster reinicia a VM durante a janela temporal para o máximo de redefinições.
   - Janela de tempo de redefinições máximas: a janela de tempo na qual ocorre a contagem de redefinições máximas por VM.

   Se você não tiver certeza de quais valores definir, use estas configurações de exemplo:

   - Failure interval (Intervalo de falha): **30** segundos
   - Minimum uptime (Tempo mínimo de atividade): **120** segundos
   - Maximum per-VM resets (Máximo de redefinições por VM): **3**
   - Maximum resets time window (Janela temporal para o máximo de redefinições): **1** hora

Se você tiver outras VMs em execução no cluster, talvez você queira definir esses valores especificamente para sua VM. Não é possível fazer isso até implantar a VM a partir do .ova. Para obter mais informações sobre como definir esses valores, consulte (Opcional) Adicionar opções de substituição para outras VMs no cluster.

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 — Criar e ativar um Gateway de Arquivos para o Amazon S3

Implantar o gateway

No cluster configurado, implante a imagem .ova em um dos hosts do cluster. Para conferir instruções, consulte Implantar um modelo de 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) Adicionar opções de substituição para outras VMs no cluster

Se tiver outras VMs em execução no cluster, talvez você queira definir os valores do cluster especificamente para cada VM. Para obter instruções, consulte Customize an Individual Virtual Machine na documentação on-line do VMware vSphere.

Como adicionar opções de substituição para outras VMs no cluster

1. Na página Summary (Resumo) do VMware vSphere, escolha o cluster para abrir a página do cluster e selecione Configure (Configurar).
2. Selecione a guia Configuration (Configuração) e selecione VM Overrides (Substituições de VM).
3. Adicione uma nova opção de substituição de VM para alterar cada valor.

   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 ambiente VMware, ative o gateway usando o console do Storage Gateway. Para conferir instruções, consulte Revisar as configurações e ativar o Gateway de Arquivos do Amazon S3.

Teste a configuração do VMware High Availability

Depois de ativar o gateway, teste a configuração.

Como testar a configuração do VMware HA

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, selecione Gateways e escolha o gateway que você deseja testar para o VMware HA.
3. Em Actions (Ações), selecione Verify VMware HA (Verificar VMware HA).
4. Na caixa Verify VMware High Availability Configuration (Verificar configuração do VMware High Availability) exibida, selecione OK.

   > **Note**
   >
   > Testar a configuração do VMware HA reinicializa a VM do gateway e interrompe a conectividade com o gateway. O teste pode levar alguns minutos para ser concluído.

   Se o teste for bem-sucedido, o status Verified (Verificado) será exibido na guia de detalhes do gateway no console.
5. Selecione Exit (Sair).

Você pode encontrar informações sobre eventos do VMware HA nos grupos de CloudWatch log da Amazon. Para obter mais informações, consulte Obtendo registros de integridade do S3 FSx 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 endereço IPv4 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 onde 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`

Endpoint público

Para obter uma chave de ativação para um endpoint público, use um dos seguintes comandos:

Endpoints padrão

Para obter a chave de ativação para um endpoint padrão:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Dual-stack endpoints

Para obter a chave de ativação para um endpoint de pilha dupla:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

Endpoints do FIPS

Para obter a chave de ativação para um endpoint FIPS:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

Endpoints da VPC

Para obter a chave de ativação de um endpoint da VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

O exemplo a seguir mostra como usar o Linux (bash/zsh) para buscar a resposta HTTP, analisar cabeçalhos HTTP e obter a chave de ativação.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
```

```
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

O exemplo a seguir mostra como usar o Microsoft Windows PowerShell para buscar a resposta HTTP, analisar cabeçalhos HTTP e obter a chave de ativação.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Como usar seu console local

Os exemplos a seguir mostram como usar o console local para gerar e exibir uma chave de ativação.

Gateways baseados no Amazon Linux 2 (AL2)

Você pode selecionar endpoints padrão ou FIPS para gateways baseados no AL2.

> **Note**
>
> Os endpoints FIPS não estão disponíveis em todos. Regiões da AWS Para obter mais informações, consulte Endpoints FIPS por serviço.

Para obter uma chave de ativação para seu AL2-based gateway a partir do console local

1. Faça login no console local como admin.
2. No menu principal 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. Insira a AWS região em que você deseja ativar seu gateway.
5. Para o tipo de rede, insira 1 para pública ou 2 para VPC.
6. Para o tipo de endpoint, insira 1 para padrão ou 2 para Federal Information Processing Standards (FIPS).

Gateways baseados no Amazon Linux 2023 (AL2023)

Para gateways baseados no AL2023, os seguintes endpoints estão disponíveis:

- Endpoints padrão (suporte somente a IPv4)
- Endpoints FIPS (suporte somente a IPv4)
- Dual-stack endpoints (suporte a IPv4 e IPv6)
- Dual-stack Endpoints FIPS (suporte a IPv4 e IPv6)

Para obter mais informações, consulte Tipos de endpoint.

Para obter uma chave de ativação para seu AL2023-based gateway a partir do console local

1. Faça login no console local. Se você estiver se conectando à instância do Amazon EC2 em um computador Windows, faça login como administrador.
2. No menu principal 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. Insira a AWS região em que você deseja ativar seu gateway.

5. Para o tipo de rede, insira 1 para pública ou 2 para endpoint da VPC.
6. Em Selecionar tipo de endpoint, Habilitar FIPS?, insira Y para habilitar FIPS ou N para usar um endpoint não FIPS.
7. Para o tipo de endpoint, insira 1 para endpoint padrão ou 2 para endpoint de pilha dupla.
    - Para um endpoint de pilha dupla, em Selecionar versão de IP ou sair:, insira 1 para IPv4 ou 2 para IPv6.

Suporte para atributos de arquivo no Gateway de Arquivos do Amazon S3

O Gateway de Arquivos do Amazon S3 é compatível com atributos de arquivo do DOS ou Windows por padrão. Usando o Gateway de Arquivos do S3, você pode preservar os dados e metadados do arquivo e atualizar as configurações, como marcar itens como arquivados quando eles são colocados no Amazon S3. Para obter mais informações sobre os atributos de arquivo do DOS e do Windows, consulte o artigo Constantes de atributo de arquivo no site da documentação de desenvolvimento de aplicações do Windows.

O Gateway de Arquivos do S3 é compatível com os seguintes atributos:

- ReadOnly— O S3 File Gateway impede alterações nos arquivos que têm o ReadOnly atributo definido.
- Archive: o Gateway de Arquivos do S3 define esse atributo quando os arquivos são adicionados pela primeira vez ao gateway.

> **Note**
>
> As aplicações de backup geralmente fazem backup de arquivos que têm o bit de Archive definido e apagam o bit após o backup bem-sucedido.

- Hidden: os clientes Server Message Block (SMB) ocultam arquivos que usam esse conjunto de bits.
- System: esse atributo persiste depois de configurado.

Quando você copia um arquivo para o Gateway de Arquivos do S3 com os atributos definidos, os atributos do DOS ou Windows do arquivo são preservados no Gateway de Arquivos do S3 e no

Amazon S3. Você pode atualizar esses atributos para arquivos no gateway, e essas atualizações também se aplicam ao objeto no Amazon S3. Se um arquivo for removido do gateway, este extrairá o arquivo, seus metadados e seus atributos persistentes do Amazon S3 quando você solicitar.

> **Note**
>
> Os atributos do DOS só são compatíveis com compartilhamentos SMB e se o acesso for controlado por listas de controle de acesso do Windows.

Utilizar Direct Connect com 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 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 compartilhados 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:

- Host do VMware: Acesso ao console local do gateway com o VMware ESXi
- Host do HyperV: Acesse o console local do Gateway com a Microsoft Hyper-V
- Host de máquina Kernel-based virtual Linux (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.

Suporte a IPv6

O suporte a IPv6 só está disponível nas versões 2.x ou posterior do dispositivo de gateway. A versão 1.x do dispositivo de gateway não pode ser atualizada para a versão 2.x. Você deve migrar ou substituir o dispositivo de gateway versão 1.x para obter suporte a IPv6.

Os endpoints de pilha dupla a seguir são necessários para IPv6.

```
storagegateway.region.api.aws:443
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
s3.dualstack.region.amazonaws.com
```

Noções básicas sobre os recursos e IDs de recurso do Storage Gateway

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 recurso da Amazon (ARN) exclusivos associados a eles, conforme mostrado na tabela a seguir.

Tipo de recurso	Formato do ARN
ARN de gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*

Tipo de recurso	Formato do ARN
ARN de compartilhamento de arquivos	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

Como trabalhar com IDs de recurso

Ao criar um recurso, o Storage Gateway atribui ao recurso um ID de recurso exclusivo. Esse ID de recurso faz parte do ARN do recurso. Um ID de recurso assume a forma de um identificador de recurso, seguido de um hífen e uma combinação única de oito letras e números. Por exemplo, um ID de gateway ID assume a forma `sgw-12A3456B`, em que `sgw` é o identificador de recursos para gateways.

Os IDs de recursos do Storage Gateway estão em letras maiúsculas. No entanto, se você usar esses IDs de recursos com a API do Amazon EC2, o Amazon EC2 espera IDs de recursos em letras minúsculas. Você deve alterar o ID do recurso para minúscula para usá-lo com a API do EC2. Por exemplo, no Storage Gateway, a ID de um gateway pode ser`sgw-12A3456B`. Se você usar esse ID com a API do EC2, deverá alterá-lo para`sgw-12a3456b`. Do contrário, a API do EC2 talvez não se comporte como esperado.

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 UTF-8 letras e números, espaço e caracteres especiais + - =. _:/e @.

Como trabalhar com tags

É possível trabalhar com tags usando o console, a API ou a interface de linha de comandos (CLI) do Storage Gateway. Os procedimentos a seguir mostram como adicionar, editar e excluir uma tag no console.

Para adicionar uma tag

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, escolha o recurso o qual você deseja 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, escolha Add/edittags.
4. Na caixa de diálogo de Add/edit tags, escolha Criar tag.
5. Digite uma chave em Key e um valor em Value. Por exemplo, você pode digitar **`Department`** para a chave e **`Accounting`** para o valor.

> **Note**
>
> Você pode deixar a caixa Value em branco.

6. Escolha Create Tag para adicionar mais tags. Você pode adicionar várias tags a um recurso.
7. Quando terminar de adicionar tags, escolha Save.

Para editar uma tag

1. Abra o console do Storage Gateway em https://console.aws.amazon.com/storagegateway/home.
2. Escolha o recurso cuja tag você deseja editar.
3. Escolha Tags para abrir a caixa de diálogo de Add/edittags.
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/home.
2. Escolha o recurso cuja tag você deseja excluir.
3. Escolha Tags e, em seguida, escolha Add/edittags para abrir a caixa de diálogo de 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

- Open-source componentes para Storage Gateway
- Open-source componentes para o Amazon S3 File Gateway

Open-source componentes para 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 do Storage Gateway implantados no VMware ESXi: sources.tar
- Para dispositivos Storage Gateway implantados na Microsoft Hyper-V: sources_hyperv.tar
- Para dispositivos Storage Gateway implantados na Máquina Kernel-based Virtual Linux (KVM): sources_ KVM.tar

Este produto inclui software desenvolvido pelo projeto OpenSSL para uso no OpenSSL Toolkit (). http://www.openssl.org/ Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulte Third-Party Licenças.

Open-source componentes para o Amazon S3 File Gateway

Várias ferramentas e licenças de terceiros são usadas para fornecer a funcionalidade do Gateway de Arquivos do Amazon S3 (Gateway de Arquivos do S3).

Use os links a seguir para fazer download do código-fonte de determinados componentes de software de código aberto incluídos no software do Gateway de Arquivos do S3:

- Para o Gateway de Arquivos do Amazon S3: sgw-file-s3-open-source.tgz

Este produto inclui software desenvolvido pelo projeto OpenSSL para uso no OpenSSL Toolkit (). http://www.openssl.org/ Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulte Third-Party Licenças.

Limites e cotas para Gateway de Arquivos do Amazon S3

Cotas para compartilhamentos de arquivos

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

Description	Limite
Número máximo de compartilhamentos de arquivos por gateway **Note** Cada compartilhamento de arquivos só pode se conectar a um bucket do S3, mas vários compartilhamentos podem se conectar ao mesmo bucket. Se você conectar mais de um compartilhamento de arquivos ao mesmo bucket, deverá configurar cada compartilhamento de arquivo para usar um nome de prefixo exclusivo e não sobreposto para evitar conflitos. read/write O número de compartilhamentos de arquivos gerenciados por um gateway pode afetar seu desempenho. Para obter mais informações, consulte Orientação de desempenho para gateways com vários compartilhamentos de arquivos.	50
O número máximo de arquivos para os quais um gateway pode armazenar metadados simultaneamente. **Note** Como o Gateway de Arquivos do S3 funciona com base no Amazon S3, não há tamanho máximo de pasta nem limite para o número de arquivos que você pode armazenar ou acessar usando um gateway.	Capacidade do gateway: Pequeno: 5 milhões de arquivos Médio: 10 milhões de arquivos Grande: 20 milhões de arquivos

Description	Limite
Cada gateway tem um limite configurável que determina o número de arquivos para os quais ele pode armazenar metadados simultaneamente. Você pode usar a ação UpdateGatewayInformationda API GatewayCapacitypara definir como `SmallMedium`, ou`Large`. Essa configuração afeta o desempenho do gateway e as recomendações de hardware. Para obter mais informações, consulte Orientação de desempenho para gateways com vários compartilhamentos de arquivos.	
O tamanho máximo de um arquivo individual. **Note** Se você tentar gravar arquivos maiores que o limite de tamanho, parte por parte, será feito upload somente dos primeiros 5 TiB. Se tentar gravar os arquivos maiores do que o limite de tamanho de uma só vez, nenhum arquivo será criado em clientes Windows e, em clientes Linux, um arquivo de tamanho zero será criado.	5 TiB

Description	Limite
Tamanho máximo de caminho **Note** Os clientes não podem criar um caminho que exceda esse comprimento, e isso ao fazer isso um erro ocorre. Esse limite se aplica aos dois protocolos compatíveis com Gateways de Arquivos: NFS e SMB. O comprimento do caminho em bytes é calculado a partir dos valores de bits de caracteres na UTF-8 codificação.	1024 bytes
O tamanho máximo do nome de arquivo. **Note** O Gateway de Arquivos não aceita nomes de arquivo que excedam esse tamanho. O tamanho do nome do arquivo em bytes é calculado a partir dos valores de bits de caracteres na UTF-8 codificação.	255 bytes

Tamanhos de disco local recomendados para seu gateway

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

Tipo de gateway	Cache (mínimo)	Cache (máximo)
Gateways de Arquivos do S3	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.

Usar classes de armazenamento

O Amazon S3 File Gateway oferece suporte às classes de armazenamento Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 Zone-Infrequent One Access, Amazon S3 e Intelligent-Tiering Amazon Glacier. Para obter mais informações sobre as classes de armazenamento, consulte Classes de armazenamento do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> O Gateway de Arquivos do S3 ainda não aceita a classe de armazenamento Amazon S3 Glacier Instant Retrieval.

Tópicos

Usar classes de armazenamento com um Gateway de Arquivos

Ao criar ou atualizar um compartilhamento de arquivos, você tem a opção de selecionar uma classe de armazenamento para os objetos. Você pode escolher a classe de armazenamento Amazon S3 Standard ou qualquer uma das classes de armazenamento S3 Standard-IA, S3 One Zone-IA ou S3.

Intelligent-Tiering Os objetos armazenados em qualquer uma dessas classes de armazenamento podem ser migrados para GLACIER com uma política de ciclo de vida.

Classe de armazenamento do Amazon S3	Considerações
Standard	Selecione Standard (Padrão) para armazenar seus arquivos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Essa é a classe de armazenamento padrão. Para obter mais detalhes, consulte Definição de preço do Amazon S3.
S3 Intelligent-Tiering	Opte por Intelligent-Tiering otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso ao armazenamento mais econômico. Objetos menores que 128 KB não estão qualificados para classificação automática em camadas na classe Intelligent-Tiering de armazenamento. Esses objetos são cobrados de acordo com as taxas do nível de acesso frequente, e a taxa de monitoramento não é cobrada por objetos com hierarquização automática. O S3 Intelligent-Tiering agora oferece suporte a uma camada de acesso ao arquivamento e a uma camada de acesso ao arquivamento profundo. O S3 move Intelligent-Tiering automaticamente objetos que não foram acessados por 90 dias para a camada Archive Access e, após 180 dias sem serem acessados, para a camada Deep Archive Access. Sempre que um objeto em um dos níveis de acesso de arquivamento é restaurado, o objeto passa para o nível de acesso Frequent em algumas

Classe de armazenamento do Amazon S3	Considerações
	horas e está pronto para ser recuperado. Isso cria erros de tempo limite para usuários ou aplicações que tentam acessar arquivos por meio de um compartilhamento de arquivos se o objeto existir somente em um dos dois níveis de arquivamento. Não use as camadas de arquivamento com o S3 Intelligent-Tiering se seus aplicativos estiverem acessando arquivos por meio dos compartilhamentos de arquivos apresentados pelo File Gateway. Quando operações de arquivo que atualizam metadados (como proprietário, carimbo de data/hora, permissões e ACLs) são realizadas em arquivos gerenciados pelo Gateway de Arquivos, o objeto existente é excluído e uma nova versão do objeto é criada nessa classe de armazenamento do Amazon S3. Valide como as operações de arquivo afetam a criação de objetos antes de usar essa classe de armazenamento na produção. Para obter mais detalhes, consulte Definição de preço do Amazon S3.

Classe de armazenamento do Amazon S3	Considerações
S3 Standard-IA	Escolha Standard-IA armazenar seus arquivos acessados com pouca frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Os objetos armazenados na classe Standard-IA de armazenamento podem incorrer em cobranças adicionais pela substituição, exclusão, solicitação, recuperação ou transição de objetos entre as classes de armazenam ento em 30 dias. Há uma duração mínima de armazenamento de 30 dias. Objetos excluídos antes de 30 dias geram uma cobrança proporcional equivalente à cobrança de armazenamento dos dias restantes. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Objetos menores que 128 KB são cobrados por 128 KB e as taxas de exclusão antecipada se aplicam. Quando operações de arquivo que atualizam metadados (como proprietário, carimbo de data/hora, permissões e ACLs) são realizada s em arquivos gerenciados pelo Gateway de Arquivos, o objeto existente é excluído e uma nova versão do objeto é criada nessa classe de armazenamento do Amazon S3. Você deve validar como as operações de arquivo afetam a criação de objetos antes de usar essa classe de armazenamento na produção, pois as taxas de exclusão antecipada se aplicam. Para obter mais detalhes, consulte Definição de preço do Amazon S3.

Classe de armazenamento do Amazon S3	Considerações
S3 Um Zone-IA	Escolha um Zone-IA para armazenar seus arquivos acessados com pouca frequência em uma única zona de disponibilidade. Os objetos armazenados na classe Zone-IA de armazenamento One podem incorrer em cobranças adicionais pela substituição, exclusão, solicitação, recuperação ou transição de objetos entre as classes de armazenamento em 30 dias. Há uma duração mínima de armazenamento de 30 dias, e objetos excluídos antes de 30 dias geram uma cobrança proporcional equivalente à cobrança de armazenamento dos dias restantes. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Objetos menores que 128 KB são cobrados por 128 KB e as taxas de exclusão antecipada se aplicam. Quando operações de arquivo que atualizam metadados (como proprietário, carimbo de data/hora, permissões e ACLs) são realizadas em arquivos gerenciados pelo Gateway de Arquivos, o objeto existente é excluído e uma nova versão do objeto é criada nessa classe de armazenamento do Amazon S3. Você deve validar como as operações de arquivo afetam a criação de objetos antes de usar essa classe de armazenamento na produção, pois as taxas de exclusão antecipada se aplicam. Para obter mais detalhes, consulte Definição de preço do Amazon S3.

Embora você possa gravar objetos diretamente de um compartilhamento de arquivos na classe de Intelligent-Tiering armazenamento S3-Standard-IA S3-One Zone-IA, ou S3, recomendamos que você use uma política de ciclo de vida para fazer a transição de seus objetos em vez de gravar diretamente do compartilhamento de arquivos, especialmente se você espera atualizar ou excluir o objeto dentro de 30 dias após o arquivamento. Para obter informações sobre a política de ciclo de vida, consulte Gerenciamento do ciclo de vida de objetos.

Usar a classe de armazenamento GLACIER com o Gateway de Arquivos

Se você fizer a transição de um arquivo para o Amazon Glacier por meio das políticas de ciclo de vida do Amazon S3 e o arquivo estiver visível para seus clientes de compartilhamento de arquivos por meio do cache, você I/O encontrará erros ao atualizar o arquivo. Recomendamos que você configure CloudWatch Eventos para receber notificações quando esses I/O erros ocorrerem e use a notificação para agir. Por exemplo, é possível restaurar o objeto arquivado para o Amazon S3. Depois que o objeto é restaurado para o S3, os clientes de compartilhamento de arquivos podem acessá-los e atualizá-los com êxito por meio do compartilhamento de arquivos.

Para obter informações sobre como restaurar objetos arquivados, consulte Restaurar objetos arquivados no Guia do usuário do Amazon Simple Storage Service.

> **Important**
>
> Oficialmente, o Gateway de Arquivos do S3 não aceita a classe de armazenamento S3 Glacier Instant Retrieval. Embora você possa designar objetos em um bucket de compartilhamento de arquivos para a classe de armazenamento S3 Glacier Instant Retrieval usando políticas de ciclo de vida ou solicitações PUT diretas, o Gateway de Arquivos do S3 não consegue reconhecer quais arquivos estão nessa classe de armazenamento e executará operações de arquivo neles como qualquer outro objeto. Como a classe de armazenamento S3 Glacier Instant Retrieval tem custos de acesso mais altos do que outras classes de armazenamento do Amazon S3, operações de arquivos em massa, como verificações de vírus, `rsync` e renomeações, podem gerar grandes cobranças do Amazon S3 se não forem gerenciadas com cuidado. Por esse motivo, não recomendamos o uso da classe de armazenamento S3 Glacier Instant Retrieval com o Gateway de Arquivos do S3.

Usar drivers da Container Storage Interface do Kubernetes

O Kubernetes é um sistema de código aberto para automatizar a implantação, a escalabilidade e o gerenciamento de aplicações em contêineres. Em um ambiente do Kubernetes, um contêiner é semelhante a uma VM, mas tem propriedades de isolamento relaxadas para compartilhar o sistema operacional (SO) entre suas aplicações. Portanto, os contêineres são considerados mais leves do que as VMs. Semelhante a uma VM, um contêiner tem seu próprio sistema de arquivos, uma parte da CPU alocada, memória, espaço de processo e muito mais. Como estão desacoplados da infraestrutura subjacente, eles são portáteis entre nuvens e distribuições de sistemas operacionais. Se você tiver um cluster Kubernetes, poderá instalar e configurar drivers da Container Storage Interface (CSI) do Kubernetes nas instâncias do cluster para permitir que eles usem um Gateway de Arquivos do Amazon S3 existente para armazenamento.

Depois de instalar os drivers da CSI para o tipo de compartilhamento de arquivos que deseja usar, você deve criar um ou mais objetos de armazenamento. Dependendo do tipo de provisionamento que deseja que o Kubernetes use quando seus pods solicitam armazenamento, você deve criar um único objeto `StorageClass` do Kubernetes ou um objeto `PersistentVolume` e um objeto `PersistentVolumeClaim` para conectar seus pods de computação do Kubernetes ao seu compartilhamento de arquivos. Para obter mais informações, consulte a documentação on-line do Kubernetes em https://kubernetes.io/docs/concepts/storage/.

Tópicos

Trabalhar com drivers SMB da CSI

Siga os procedimentos nesta seção para instalar, configurar ou excluir os drivers da CSI necessários para usar um compartilhamento de arquivos SMB em um Gateway de Arquivos do Amazon S3 para armazenamento em um cluster Kubernetes. Para obter mais informações, consulte a documentação de código aberto do driver SMB CSI em. GitHub https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md

> **Note**
>
> Ao criar um objeto `PersistentVolume` ou `StorageClass`, você pode especificar um parâmetro `ReclaimPolicy` para determinar o que acontece com o armazenamento externo

quando os objetos são excluídos. O driver SMB da CSI é compatível com as opções `Retain` e `Recycle`, mas ainda não é compatível com uma opção `Delete`.

Instalar drivers

Para instalar drivers SMB da CSI do Kubernetes:

1. Em um terminal de linha de comandos com acesso a `kubectl` para o cluster Kubernetes, execute o seguinte comando:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. Aguarde a conclusão do comando anterior e use os comandos a seguir para garantir que os pods de driver da CSI estejam em execução:

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   A saída deve ser semelhante à seguinte:

```
NAME                                     READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-smb-controller-56bfddd689-dh5tk      4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4      4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                       3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                       3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Criar um objeto SMB StorageClass

Para criar um novo StorageClass objeto SMB para seu cluster Kubernetes:

1. Crie um arquivo de configuração chamado `storageclass.yaml` com conteúdo semelhante ao exemplo a seguir. Substitua suas próprias informações específicas de implantação pelas mostradas. *ExampleValues*

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub
 directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. Em um terminal de linha de comandos com acesso a `kubectl` e `storageclass.yaml`, execute o seguinte comando:

   kubectl apply -f storageclass.yaml

> **Note**
>
> Você também pode criar o StorageClass fornecendo o texto de `.yaml` configuração da etapa anterior para a maioria das plataformas de gerenciamento e conteinerização de Kubernetes de terceiros.

3. Configure os pods em seu cluster Kubernetes para usar o novo StorageClass que você criou. Para obter mais informações, consulte a documentação on-line do Kubernetes em https://kubernetes.io/docs/concepts/storage/.

Crie SMB PersistentVolume e objetos PersistentVolumeClaim

Para criar novos SMB PersistentVolume e PersistentVolumeClaim objetos:

1. Crie dois arquivos de configuração. Um chamado `persistentvolume.yaml` e outro chamado `persistentvolumeclaim.yaml`.
2. Para `persistentvolume.yaml`, adicione conteúdos semelhantes ao exemplo a seguir. Substitua suas próprias informações específicas de implantação pelas mostradas. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
```

```
        driver: smb.csi.k8s.io
        readOnly: false
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. Para `persistentvolumeclaim.yaml`, adicione conteúdos semelhantes ao exemplo a seguir. Substitua suas próprias informações específicas de implantação pelas mostradas. *ExampleValues*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
 name of the PersistentVolume you created
        storageClassName: ""
```

4. Em um terminal de linha de comandos com acesso a `kubectl` e ambos os arquivos `.yaml` que você criou, execute os seguintes comandos:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

> **Note**
>
> Você também pode criar os PersistentVolumeClaim objetos PersistentVolume e fornecendo o texto de `.yaml` configuração da etapa anterior para a maioria das plataformas terceirizadas de gerenciamento e conteinerização do Kubernetes.

5. Configure os pods em seu cluster Kubernetes para usar o novo PersistentVolumeClaim que você criou. Para obter mais informações, consulte a documentação on-line do Kubernetes em https://kubernetes.io/docs/concepts/storage/.

Desinstalar drivers

Para desinstalar os drivers SMB da CSI do Kubernetes:

- Em um terminal de linha de comandos com acesso a `kubectl` para o cluster Kubernetes, execute o seguinte comando:

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

Trabalhar com drivers NFS da CSI

Siga os procedimentos nesta seção para instalar, configurar ou excluir os drivers da CSI necessários para usar um compartilhamento de arquivos NFS em um Gateway de Arquivos do Amazon S3 para armazenamento em um cluster Kubernetes. Para obter mais informações, consulte a documentação do driver CSI NFS de código aberto em. GitHub https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md

Instalar drivers

Para instalar drivers NFS da CSI do Kubernetes:

1. Em um terminal de linha de comandos com acesso a `kubectl` para o cluster Kubernetes, execute o seguinte comando:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --

2. Aguarde a conclusão do comando anterior e use os comandos a seguir para garantir que os pods de driver da CSI estejam em execução:

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   A saída deve ser semelhante à seguinte:

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-nfs-controller-56bfddd689-dh5tk   4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4   4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                    3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-dr4s4                    3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Criar um objeto NFS StorageClass

Para criar um StorageClass objeto NFS para seu cluster Kubernetes:

1. Crie um arquivo de configuração chamado `storageclass.yaml` com conteúdo semelhante ao exemplo a seguir. Substitua suas próprias informações específicas de implantação pelas mostradas. *ExampleValues*

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: example-nfs-classname
    namespace: example-namespace
provisioner: nfs.csi.k8s.io
parameters:
    server: gateway-dns-name-or-ip-address
    share: /example-share-name
reclaimPolicy: Retain
```

```
volumeBindingMode: Immediate
mountOptions:
    - hard
    - nfsvers=4.1
```

2. Em um terminal de linha de comandos com acesso a `kubectl` e `storageclass.yaml`, execute o seguinte comando:

   kubectl apply -f storageclass.yaml

   > **Note**
   >
   > Você também pode criar o StorageClass fornecendo o texto de `.yaml` configuração da etapa anterior para a maioria das plataformas de gerenciamento e conteinerização de Kubernetes de terceiros.

3. Configure os pods em seu cluster Kubernetes para usar o novo StorageClass objeto que você criou. Para obter mais informações, consulte a documentação on-line do Kubernetes em https://kubernetes.io/docs/concepts/storage/.

Crie NFS PersistentVolume e objetos PersistentVolumeClaim

Para criar novos NFS PersistentVolume e PersistentVolumeClaim objetos:

1. Crie dois arquivos de configuração chamados `persistentvolume.yaml` e `persistentvolumeclaim.yaml`.
2. Para `persistentvolume.yaml`, adicione conteúdos semelhantes ao exemplo a seguir. Substitua suas próprias informações específicas de implantação pelas mostradas. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
```

```
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
            share: /example-share-name
```

3. Para `persistentvolumeclaim.yaml`, adicione conteúdos semelhantes ao exemplo a seguir. Substitua suas próprias informações específicas de implantação pelas mostradas. *ExampleValues*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name
 of the PersistentVolume you created
    storageClassName: ""
```

4. Em um terminal de linha de comandos com acesso a `kubectl` e ambos os arquivos `.yaml`, execute os seguintes comandos:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

> **Note**
>
> Você também pode criar os PersistentVolumeClaim objetos PersistentVolume e fornecendo o texto de `.yaml` configuração da etapa anterior para a maioria das plataformas terceirizadas de gerenciamento e conteinerização do Kubernetes.

5. Configure os pods em seu cluster Kubernetes para usar o novo PersistentVolumeClaim objeto que você criou. Para obter mais informações, consulte a documentação on-line do Kubernetes em https://kubernetes.io/docs/concepts/storage/.

Desinstalar drivers

Para desinstalar drivers NFS da CSI do Kubernetes:

- Em um terminal de linha de comandos com acesso a `kubectl` para o cluster Kubernetes, execute o seguinte comando:

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/uninstall-driver.sh | bash -s master --

AWS Storage Gateway Módulo Terraform

HashiCorpO Terraform é um mecanismo de infraestrutura como código (IaC) de código aberto desenvolvido usando a Linguagem de HashiCorp Configuração (HCL). O Terraform fornece um fluxo de trabalho consistente de interface de linha de comandos (CLI) que, em conjunto com o Gateway de Arquivos do Amazon S3 para a infraestrutura de backend, pode gerenciar centenas de serviços em nuvem e codificar APIs de nuvem em arquivos de configuração declarativos.

Você pode usar o Terraform para implantar com segurança um Gateway de Arquivos do Amazon S3 como uma máquina virtual (VM) em sua infraestrutura virtual on-premises. O Terraform fornece automação para infraestrutura virtual on-premises. Consulte Automatizar implantações do Amazon S3 File Gateway no VMware com o Terraform HashiCorp by para obter informações sobre como implantar rapidamente um Amazon S3 File Gateway usando o Terraform em um ambiente virtual VMware local.

> **Note**
>
> Talvez seja necessário configurar o Terraform para ter a versão mais recente da imagem de máquina do AWS Storage Gateway da sua plataforma de hipervisor preferida. As imagens de máquina do Storage Gateway usam a convenção de nomenclatura a seguir. O número de versão anexado ao nome da imagem muda a cada lançamento.
> `aws-storage-gateway-FILE_S3-1.25.0`

Essa automação fornece um módulo Terraform personalizável que você pode usar para provisionar um Gateway de Arquivos do Amazon S3 com todos os recursos e dependências necessários para implantar totalmente o gateway e os compartilhamentos de arquivos em seu ambiente de VM. O módulo Terraform provisiona a VM do gateway, ativa o gateway, configura o disco de cache, associa o gateway a um domínio, cria os buckets do Amazon S3, cria os compartilhamentos de arquivos e os associa aos buckets. Para obter um exemplo completo de um repositório que contém o código do Terraform para criar os recursos necessários para executar o Amazon S3 File Gateway localmente, consulte o código-fonte do módulo Terraform Storage Gateway em. GitHub

> **Note**
>
> O módulo Terraform para Gateway de Arquivos do Amazon S3 é um esforço apoiado pela comunidade. Não faz parte de um AWS serviço. Best-effort o suporte é fornecido pela comunidade AWS de armazenamento.

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 solicitação 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 legibilidade): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` Na sintaxe anterior, você especifica 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 assinatura AWS V4. Os detalhes da assinatura são discutidos no tópico Solicitações 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
`MaximumVolumeCountExceeded`	A contagem máxima de volume foi excedida.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	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 do documento do Guia do usuário do Gateway de Arquivos do Amazon S3

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
IPv6 apoio	IPv6o suporte está disponível nas versões 2.x ou superiores do gateway appliance.	10 de setembro de 2025
Adição de throughput e orientações sobre otimização	O capítulo Performance e otimização agora inclui recomendações e práticas recomendadas para maximizar o throughput do Gateway de Arquivos do S3 e otimizar sua implantação para casos de uso de backup de banco de dados SQL Server. Para acessar mais informaçõ es, consulte Maximizar o throughput do Gateway de Arquivos do S3 e Otimizar o Gateway de Arquivos do S3 para backups de bancos de dados do SQL Server.	13 de junho de 2025
Adição da funcionalidade de relatórios de cache	O Gateway de Arquivos do S3 agora pode gerar um relatório dos metadados dos arquivos que estão atualment e no cache de upload local para um compartilhamento	31 de março de 2025

	de arquivos específico. Para acessar mais informações, consulte Criar um relatório de cache para seu Gateway de Arquivos do S3, Visualizar e gerenciar relatórios de cache para seu Gateway de Arquivos do S3 e Noções básicas sobre as informações fornecidas nos relatórios de cache do Gateway de Arquivos do S3.	
Foi adicionado suporte para criptografia de duas camadas do lado do servidor com chaves (DSSE-KMS) AWS KMS	Agora você pode usar criptografia de camada dupla no lado do servidor com AWS KMS chaves para criptografar os arquivos que o S3 File Gateway carrega para o Amazon S3. Para acessar mais informaçõ es sobre DSSE-KMS, consulte Criptografar objetos armazenados pelo Gateway de Arquivos no Amazon S3.	13 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 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 .	6 de junho de 2024
Adição de um novo nível de segurança SMB	O Gateway de Arquivos do S3 agora oferece suporte a um nível de segurança adicional que você pode usar para aplicar a criptografia AES de 256 bits para conexões de clientes SMB. Para acessar mais informações, consulte Definir um nível de segurança para seu gateway.	23 de maio de 2024

Relatórios de versão de software do dispositivo Gateway e notas de versão do Gateway de Arquivos do S3	Adição de notas de versão para descrever os recursos novos e atualizados, melhorias e correções incluídos em cada versão do dispositivo do Gateway de Arquivos de Amazon S3. Você pode determinar o número da versão do software de um gateway no console do Storage Gateway ou usando a AWS CLI. Para acessar mais informações, consulte Notas de versão: software de dispositivo do gateway.	5 de outubro de 2023
CloudWatch Alarmes recomendados atualizados	O CloudWatch `HealthNotifications` alarme agora se aplica e é recomendado para todos os tipos de gateway e plataformas de host. As configurações recomendadas também foram atualizadas para `HealthNotifications` e `AvailabilityNotifications`. Para obter mais informações, consulte Entendendo os CloudWatch alarmes os alarmes.	2 de outubro de 2023

Aumento do máximo de compartilhamentos de arquivos por gateway	O Gateway de Arquivos do S3 agora oferece suporte a até cinquenta compartil hamentos de arquivos por gateway, acima do limite anterior de dez. Isso permite criar mais compartilhamentos de arquivos em um único gateway, reduzindo o número de gateways que você precisa gerenciar. Para acessar mais informações, consulte Cotas para compartilhamentos de arquivos.	18 de janeiro de 2023
Adição de suporte para atributos do DOS	Agora o Gateway de Arquivos do S3 oferece suporte a atributos do DOS para arquivos armazenados no Amazon S3. Isso permite que você preserve atributos de arquivos do Windows, como somente leitura, oculto, sistema e arquivamento, quando é feito upload dos arquivos para o Amazon S3. Para acessar mais informaçõ es, consulte Suporte para os atributos de arquivos no Gateway de Arquivos do Amazon S3.	18 de janeiro 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 do controle de utilização da largura de banda da rede baseada em agendamento	Agora o Gateway de Arquivos do S3 oferece suporte ao controle de utilização de largura de banda de rede baseada em agendamento para uploads de dados para o Amazon S3. Esse recurso permite limitar a quantidade de largura de banda de rede que seu gateway usa durante períodos específicos, ajudando você a gerenciar o uso da rede durante o horário comercial de pico. Para acessar mais informações, consulte Gerenciar a largura de banda do seu Gateway de Arquivos do S3.	18 de janeiro 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 para fechament o forçado de arquivos em compartilhamentos de arquivos SMB	Agora você pode usar as configurações de grupo local para atribuir permissões de administrador do Gateway. Os administradores do Gateway podem usar o snap-in do Console de Gerenciamento da Microsoft de Pastas Compartil hadas para forçar o fechament o de arquivos abertos e bloqueados em compartil hamentos de arquivos SMB. Para acessar mais informaçõ es, consulte Configurar grupos locais para o seu gateway.	12 de outubro de 2021

Suporte de log de auditoria para compartilhamentos de arquivos NFS	Agora você pode configurar compartilhamentos de arquivos NFS para gerar logs de auditoria que fornecem detalhes sobre o acesso do usuário aos arquivos e pastas em um compartilhamento de arquivos. É possível usar esses logs para monitorar as atividades do usuário e tomar medidas se forem identificados padrões de atividade inadequados. Para acessar mais informações, consulte Noções básicas dos logs de auditoria do Gateway de Arquivos.	12 de outubro de 2021
Suporte a alias de ponto de acesso	Os compartilhamentos de arquivos do Gateway de Arquivos agora podem se conectar ao armazenamento do Amazon S3 usando aliases de ponto de acesso no estilo bucket. Para obter mais informações, consulte Criar um compartilhamento de arquivos.	12 de outubro de 2021

Suporte para endpoints da VPC e pontos de acesso	Os compartilhamentos de arquivos do Gateway de Arquivos agora podem se conectar aos buckets do S3 por meio de pontos de acesso ou endpoints de interface em sua VPC desenvolvida por AWS PrivateLink. Para obter mais informações, consulte Criar um compartilhamento de arquivos.	7 de julho de 2021
Suporte ao bloqueio oportunista	Os compartilhamentos de arquivos do Gateway de Arquivos agora podem usar o bloqueio oportunista para otimizar sua estratégia de armazenamento em buffer de arquivos, o que melhora a performance na maioria dos casos, principalmente no que diz respeito aos menus de contexto do Windows. Para acessar mais informações, consulte Criar um compartilhamento de arquivos SMB.	7 de julho 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

Notificação de upload de arquivo para o Gateway de Arquivos	O Gateway de Arquivos agora fornece uma notificação de upload de arquivo, que notifica você quando o upload de um arquivo foi totalmente concluído para o Amazon S3 pelo Gateway de Arquivos. Para acessar mais informaçõ es, consulte Receber notificaç ão de upload de arquivos.	9 de novembro de 2020
Enumeração baseada em acesso para o Gateway de Arquivos	O File Gateway agora fornece enumeração baseada em acesso, que filtra a enumeraçã o de arquivos e pastas em um compartilhamento de arquivos SMB com base no compartil hamento. ACLs Para acessar mais informações, consulte Criar um compartilhamento de arquivos SMB.	9 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

Suporte para vários compartilhamentos de arquivos anexados a um único bucket do Amazon S3	O Gateway de Arquivos agora oferece suporte à criação de vários compartilhamentos de arquivos para um único bucket do S3 e a sincronização do cache local do Gateway de Arquivos com um bucket com base na frequência de acesso ao diretório. Você pode limitar o número de buckets necessários para gerenciar os compartilhamentos de arquivos que você cria no seu Gateway de Arquivos. Você pode definir vários prefixos do S3 para um bucket do S3 e associar um único prefixo a um único compartilhamento de arquivos do gateway. Você também pode definir nomes de compartilhamento de arquivos do gateway para que sejam independentes do nome do bucket, de acordo com a convenção de nomenclatura de compartilhamento de arquivos on-premises. Para acessar mais informações, consulte Criar um compartilhamento de arquivos NFS ou Criar um compartilhamento de arquivos SMB.	7 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

Suporte ao compartilhamento de arquivos SMB para Microsoft Windows ACLs	Para gateways de arquivos, agora você pode usar as listas de controle de acesso (ACLs) do Microsoft Windows para controlar o acesso aos compartilhamentos de arquivos do Server Message Block (SMB). Para obter mais informações, consulte Usando o Microsoft Windows ACLs para controlar o acesso a um compartilhamento de arquivos SMB.	8 de maio de 2019
O Gateway de Arquivos oferece suporte à autorização com base em tag	O Gateway de Arquivos agora oferece suporte à autorizaç ão com base em tag. Você pode controlar o acesso aos recursos do Gateway de Arquivos com base nas tags desses recursos. Também é possível controlar o acesso com base nas tags que podem ser transmiti das em uma condição de solicitação do IAM. Para obter mais informações, consulte Controlar o acesso aos recursos do gateway de arquivos.	4 de março de 2019

Disponibilidade do dispositivo de hardware AWS Storage Gateway na Europa	O AWS Storage Gateway Hardware Appliance agora está disponível na Europa. Para obter mais informações, consulte Regiões do equipamento de hardware do AWS Storage Gateway na Referência geral da AWS. Além disso, agora 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 informações, 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

Compatibilidade com o protocolo de Server Message Block (SMB)	Os gateways de arquivos acrescentaram suporte ao protocolo de Server Message Block (SMB) para compartil hamentos de arquivos. Para obter mais informações, consulte Como criar um compartilhamento de arquivos.	20 de junho de 2018

Atualizações anteriores

A tabela a seguir descreve alterações importantes em cada versão do Guia do usuário do AWS Storage Gateway antes de maio de 2018.

Alteração	Descrição	Alterado em
Suporte à classe de armazenam ento S3 One Zone-IA	Para os Gateways de Arquivos, agora é possível escolher o S3 One Zone-IA como a classe de armazenamento padrão para o compartilhamentos de arquivos. Ao usar esta classe de armazenamento, é possível armazenar seus dados de objetos em uma única zona de disponibilidade do Amazon S3. Para obter mais informações, consulte Criar um compartil hamento de arquivos.	4 de abril de 2018
Novo Região da AWS	Agora o gateway de fitas está disponível na região Ásia-Pacífico (Singapura). Para obter informações detalhadas, consulte Regiões da AWSque suportam Storage Gateway.	3 de abril de 2018
Support para notificação de atualização do cache, Requester Pays e canned	Com os gateways de arquivo, é possível enviar notificações quando o gateway termina de atualizar o cache para seu bucket do Amazon S3. Para obter mais informações, consulte RefreshCache.html na Referência da API do Storage Gateway.	1º de março de 2018

Alteração	Descrição	Alterado em
para buckets do Amazon ACLs S3	Para os Gateways de Arquivos, agora você pode especificar que o solicitante ou o leitor pague as cobranças de acesso em vez do proprietário do bucket. Agora, o Gateway de Arquivos pode conceder controle total dos arquivos gravados ao proprietário do bucket do S3 associado ao compartilhamento de arquivos NFS. Para obter mais informações, consulte Criar um compartilhamento de arquivos.	
Novo Região da AWS	Agora o Storage Gateway está disponível na região Europa (Paris). Para obter informações detalhada s, consulte Regiões da AWSque suportam Storage Gateway.	18 de dezembro de 2017
Suporte para notificação de upload de arquivos e adivinhação do tipo MIME	Agora, o Gateway de Arquivos envia notificações quando é feito upload de todos os arquivos gravados no compartilhamento de arquivos NFS para o Amazon S3. Para obter mais informações, consulte NotifyWhenUploadedna Referência da API do Storage Gateway. Agora, o Gateway de Arquivos permite adivinhar o tipo MIME dos objetos cujo upload foi feito com base nas extensões de arquivo. Para obter mais informações, consulte Criar um compartilhamento de arquivos.	21 de novembro 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 AWSque suportam Storage Gateway.	02 de maio de 2017
Atualizações nas configurações de compartilhamento de arquivos Compatibilidade com atualização de cache para compartilhamento de arquivos	Agora, os gateway de arquivos adicionam opções de montagem às configurações do compartilhamento de arquivos. Agora você pode definir opções de esmagamento e somente leitura para o compartil hamento de arquivos. Para obter mais informações, consulte Criar um compartilhamento de arquivos. Agora, os gateways de arquivos agora podem encontrar objetos no bucket do Amazon S3 que foram adicionados ou removidos desde que a última vez em que o gateway indicou conteúdo e resultados armazenados em cache do bucket. Para obter mais informações, consulte RefreshCachea Referência da API.	28 de março de 2017

Alteração	Descrição	Alterado em
Compatibilidade com gateways de arquivos no Amazon EC2	AWS Storage Gateway agora fornece a capacidade de implantar um gateway de arquivos no Amazon EC2. É possível ativar um gateway de arquivos no Amazon EC2 usando a Imagem de Máquina da Amazon (AMI) do Storage Gateway, agora disponível como uma AMI de comunidade. Para acessar informações sobre como criar um Gateway de Arquivos e implantá-lo em uma instância do EC2, consulte Criar e ativar um Gateway de Arquivos para o Amazon S3. Para acessar informações sobre como iniciar uma AMI de Gateway de Arquivos, consulte Implantar um host padrão do Amazon EC2 para o Gateway de Arquivos do S3. 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 detalhadas, consulte Regiões da AWSque suportam Storage Gateway.	13 de dezembro de 2016
Novo Região da AWS	Agora o Storage Gateway está disponível na região Canadá (Central). Para obter informações detalhadas, consulte Regiões da AWSque suportam Storage Gateway.	08 de dezembro de 2016

Alteração	Descrição	Alterado em
Suporte para gateway de arquivos	Além dos gateways de volumes e do gateway de fitas, o Storage Gateway agora fornece o gateway de arquivos. O gateway de arquivos é ao mesmo tempo um serviço e um dispositivo de software virtual que permite que você armazene e recupere objetos no Amazon S3 usando protocolos de arquivo padrão do setor, como o Network File System (NFS). O gateway oferece acesso a objetos no Amazon S3 como arquivos em um ponto de montagem NFS.	29 de novembro de 2016

Campanha de migração do Storage Gateway AL2 para AL2023

AWSestá fazendo a transição do sistema operacional (OS) do dispositivo Storage Gateway do Amazon Linux 2 para o AL2023 para habilitar novos recursos de armazenamento em nuvem híbrida e manter padrões ideais de desempenho e segurança. Essa transição afetará todas as versões do dispositivo AL2-based Storage Gateway S3 File Gateway versão 1.x, Tape Gateway versão 2.x e Volume Gateway versão 2.x. Você deve concluir a migração antes de 30 de junho de 2026, pois AWS interromperá o suporte a esses sistemas posteriormente.

Você pode identificar se seus gateways precisam de migração por meio de vários métodos. O AWS console exibe uma mensagem de descontinuação na guia Detalhes do gateway para os gateways afetados. Além disso, a `DescribeGatewayInformation`API fornece acesso programático para verificar o campo da data de suspensão de uso. O AWS Health Dashboard lista os gateways afetados na guia Recursos afetados. No entanto, a lista não é atualizada imediatamente após a migração de um gateway. O processo de migração em si foi projetado com a segurança dos dados como prioridade, armazenando uma cópia dos dados da VM do gateway local AWS antes do início da migração para permitir uma recuperação fácil, se necessário.

AWSfornece guias de migração abrangentes específicos para cada tipo de gateway.
Depois de concluir a migração, você deve verificar o sucesso verificando se os avisos de depreciação não aparecem mais na guia Detalhes do gateway do AWS console ou usando a `DescribeGatewayInformation`API para confirmar que o campo de data de suspensão está ausente. Fundamentalmente, você não deve reverter para o gateway AL2 depois de migrar com sucesso para o AL2023, pois a reversão pode causar problemas operacionais.

Durante todo o período de migração, AWS enviará notificações de lembretes mensais por e-mail e pela guia Alterações agendadas do AWS Health Dashboard para ajudá-lo a planejar e concluir suas migrações. Se você encontrar problemas durante a migração, entre em contato com o AWSSupport para obter assistência e orientação para solução de problemas.

Links e recursos rápidos

Referência de migração da versão do gateway

Entender quais gateways precisam de migração é simples com base no número da versão do software do gateway. É importante observar que mesmo os gateways recentemente ativados com base no sistema operacional Amazon Linux 2 ainda precisam ser migrados até 30 de junho de 2026.

Tipo de gateway	Versão AL2 (requer migração)	Versão AL2023 (alvo)
Gateways de Arquivos do S3	Versão 1.x	Versão 2.x
Gateway de fitas	Versão 2.x	Versão 3.x
Gateway de volumes	Versão 2.x	Versão 3.x

Cronograma de migração

O cronograma de migração inclui vários marcos essenciais:

- 28 de outubro de 2025: todas as novas implantações de gateway iniciadas a partir do console do Storage Gateway usarão como padrão as imagens AL2023.
- 5 de janeiro de 2026: AWS começará a restringir novas ativações do gateway AL2.
- 30 de junho de 2026: os AL2-based gateways deixarão de receber atualizações de software e o AWS suporte será encerrado. Após essa data, embora você possa continuar usando os AL2-based dispositivos, eles não receberão novas atualizações de software, patches de segurança ou correções de bugs, e a manutenção desses sistemas se tornará de sua exclusiva responsabilidade.

Pre-migration Lista de verificação

> **Important**
>
> Antes de iniciar o processo de migração, verifique os requisitos a seguir para garantir uma migração bem-sucedida.

- Use a imagem mais recente do gateway. Ao criar a nova VM do Storage Gateway:
  - Para gateways do Amazon EC2, use a AMI mais recente do parâmetro SSM público ou use o console do Storage Gateway.
  - Para gateways locais, baixe a imagem mais recente da VM no console do Storage Gateway.
- Combine a configuração do hardware. Certifique-se de que a nova VM do gateway use a mesma CPU, memória e taxa de transferência de rede do gateway existente. Para gateways EC2, use o mesmo tipo de instância.
- Verifique o tamanho do disco raiz. O disco raiz da nova VM do gateway deve ter pelo menos o mesmo tamanho do disco raiz do gateway existente. Se o disco raiz existente tiver menos de 20 GB de espaço disponível, dimensione o novo disco raiz para: (tamanho do disco raiz existente) + (20 GB menos espaço disponível no disco raiz existente).
- Aplique as atualizações de software pendentes. Antes de iniciar a migração, aplique todas as atualizações de software pendentes no gateway existente. Abra o console do Storage Gateway, selecione seu gateway e escolha Atualizar agora, se disponível.
- Verifique a conectividade de rede a partir do novo gateway. Antes de iniciar a migração, confirme se a nova VM do gateway pode alcançar:
  - Endpoints do serviço Storage Gateway (ou seus endpoints de VPC).
  - Endpoints Amazon S3.
  - Servidores Active Directory/DNS (se seu gateway for associado a um domínio).
  - Use o teste de conectividade de rede do console local do gateway para validar a aprovação de todos os endpoints.
- Resolva falhas no upload de arquivos. Certifique-se de que a `FilesFailingUpload` CloudWatch métrica do seu gateway seja zero antes de iniciar a migração. Arquivos em estado de falha indicam erros não resolvidos que devem ser resolvidos primeiro. Para identificar os arquivos afetados, crie um relatório de cache e resolva os problemas subjacentes antes de continuar.
- Aguarde a sincronização do cache. Verifique se a `CachePercentDirty` métrica na guia Monitoramento do gateway é 0. Isso confirma que todos os dados em cache foram enviados para o S3.

Guias de migração

- Guia de migração do S3 File Gateway
- Guia de migração do gateway de fita

- Guia de migração do Volume Gateway

Support and Monitoring

- Console Storage Gateway
- AWSPersonal Health Dashboard
- Entre em contato com o AWS Support

Perguntas frequentes

O que acontece com meus dados durante a migração?

Seus dados permanecem armazenados de forma durável AWS durante todo o processo de migração. O procedimento de migração inclui armazenar uma cópia dos dados da VM do gateway local AWS para facilitar a recuperação, se necessário.

Haverá tempo de inatividade durante a migração?

O tempo de migração e qualquer possível interrupção do serviço dependem do tipo e da configuração do gateway. Consulte o guia de migração específico do gateway para sua implantação para obter informações detalhadas.

O que acontece se eu não migrar até 30 de junho de 2026?

Seu gateway continuará operando normalmente e os dados permanecerão armazenados com segurançaAWS, mas você deve migrar os gateways afetados até 30 de junho de 2026 para continuar recebendo atualizações e suporte.

Posso continuar usando meu gateway baseado em AL2 após a migração?

Não, você não deve usar o gateway AL2 junto com o novo gateway AL2023 após a migração bem-sucedida. Use somente seu novo AL2023-based gateway daqui para frente. Usar os gateways AL2 e AL2023 simultaneamente pode causar problemas operacionais.

Estou tendo problemas durante a migração. O que devo fazer?

Entre em contato com AWSo Support para obter ajuda. Nossa equipe de suporte pode ajudar a solucionar problemas de migração e orientá-lo durante o processo.

Notas de versão do software do dispositivo do gateway

Essas notas de versão descrevem os recursos novos e atualizados, melhorias e correções incluídos em cada versão do dispositivo do Gateway de Arquivos do Amazon S3. Cada versão do software é identificada por sua data de lançamento e um número de versão exclusivo.

Você pode determinar o número da versão do software de um gateway verificando sua página de detalhes no console do Storage Gateway ou chamando a ação da DescribeGatewayInformationAPI usando um AWS CLI comando semelhante ao seguinte:

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

O número da versão é retornado no campo `SoftwareVersion` da resposta da API.

> **Note**
>
> Um gateway não relatará informações da versão do software nas seguintes circunstâncias:
>
> - O gateway está off-line.
> - O gateway está executando um software antigo que não oferece suporte a relatórios de versão.
> - O tipo de gateway é Gateway de Arquivos do S3.

Para obter mais informações sobre as atualizações do S3 File Gateway Gateway, incluindo como modificar a manutenção automática padrão e o agendamento de atualização de um gateway, consulte Gerenciando atualizações do gateway usando o console do Storage AWS Gateway Gerenciando atualizações do AWS gateway .

Para obter mais informações sobre a migração do S3 File Gateway do Amazon Linux 2 para o AL2023, consulte. Migração de AL2 para AL2023

Gateways baseados no Amazon Linux 2023 (AL2023)

A tabela a seguir lista as notas de versão dos gateways baseados em AL2023.

> **Note**
>
> As versões 1.x.x do gateway não podem ser atualizadas para 2.x.x.

Data de lançamento	Versão do software	Notas da versão
2026-07-20	2.1.10	• Atualiza os componentes do sistema operacional e os pacotes de software para melhorar a segurança e o desempenho. • Corrige um possível problema de estabilidade do gateway quando o cache está extremamente baixo.
2026-07-15	2.1.9	• Atualiza os componentes do sistema operacional e os pacotes de software para melhorar a segurança e o desempenho.
2026-06-16	2.1.8	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-05-21	2.1.7	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-05-14	2.1.6	Atualizações de manutenção:

Data de lançamento	Versão do software	Notas da versão
		• Melhorias na migração de 1.x para 2.x (AL2 para AL2023). • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-04-16	2.1.5	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-03-26	2.1.4	Atualizações de manutenção: **Note** Esta versão introduz uma dependência mais forte do serviço DCE/RPC Endpoint Mapper (porta TCP 135) nos controlad ores de domínio AD. Se seu ambiente bloquear o tráfego de saída nessa porta, desbloqueie-a para evitar problemas de conectividade. Consulte Requisitos de porta do gateway de arquivos para obter detalhes. • Continue a descontinuação do NTLM para interações entre os controladores de domínio do Active Directory e o Gateway. • Melhor resiliência da pilha SMB durante interrupções na rede.

Data de lançamento	Versão do software	Notas da versão
2026-03-16	2.1.3	Atualizações de manutenção: • Melhor resiliência do DNS com tráfego SMB. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-03-02	2.0.7	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-02-12	2.1.2	Atualizações de manutenção: **Note** Lançamento pausado. Essa versão foi lançada em um conjunto limitado de gateways. • Corrija um problema com a falta de guias de segurança e cota ao usar o Windows Explorer em um compartil hamento SMB. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-02-02	2.1.1	Atualizações de manutenção: **Note** Lançamento pausado. Essa versão foi lançada em um conjunto limitado de gateways. • Corrija o problema com o SMB em relação ao acesso a arquivos sem distinção entre maiúsculas e minúsculas. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-01-21	2.0.6	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-01-16	2.1.0	Atualizações de manutenção: **Note** Lançamento pausado. Essa versão foi lançada em um conjunto limitado de gateways. • Atualização da pilha SMB. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-12-15	2.0.5	Atualizações de manutenção: • Corrigido um problema com a métrica do tamanho do disco raiz. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-11-12	2.0.4	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2025-11-12	2.0.4	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-10-15	2.0.3	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-09-15	2.0.2	Atualizações de manutenção: • Correção de um problema que impedia a alteração da capacidade do gateway. • Correção de um problema com a API `UpdateSMBLocalGroups` . • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-08-29	2.0.1	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance. • Versão inicial para gateways on-premises.

Data de lançamento	Versão do software	Notas da versão
2025-08-21	2.0.0	Recursos: • Lançamento inicial do novo sistema operacional. • Adição de suporte para IPv6.

Amazon Linux 2 (AL2) gateways baseados em)

A tabela a seguir lista as notas de versão dos gateways baseados em AL2.

Data de lançamento	Versão do software	Notas da versão
2026-07-20	1.28.10	Note Essa versão foi lançada em um conjunto limitado de gateways. • Atualiza os componentes do sistema operacional e os pacotes de software para melhorar a segurança e o desempenho. • Corrige um possível problema de estabilidade do gateway quando o cache está extremamente baixo.
2026-07-15	1.28.9	Note Essa versão foi lançada em um

Data de lançamento	Versão do software	Notas da versão
		conjunto limitado de gateways. • Atualiza os componentes do sistema operacional e os pacotes de software para melhorar a segurança e o desempenho.
2026-06-16	1.28.8	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-05-26	1.28.7	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-05-18	1.28.6	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-04-16	1.28.5	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-03-26	1.28.4	Atualizações de manutenção: **Note** Esta versão está disponível apenas para gateways que já estão na versão 1.28.* **Note** Esta versão introduz uma dependência mais forte do serviço DCE/RPC Endpoint Mapper (porta TCP 135) nos controlad ores de domínio AD. Se seu ambiente bloquear o tráfego de saída nessa porta, desbloqueie-a para evitar problemas de conectividade. Consulte Requisitos de porta do gateway de arquivos para obter detalhes. • Continue a descontinuação do NTLM para interações entre os controladores de

Data de lançamento	Versão do software	Notas da versão
		domínio do Active Directory e o Gateway. • Melhor resiliência da pilha SMB durante interrupções na rede.
2026-03-16	1.27.21	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-03-16	1.28.3	Atualizações de manutenção: **Note** Esta versão está disponível apenas para gateways que já estão na versão 1.28.* • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-02-27	1.27.20	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-02-11	1.28.2	Atualizações de manutenção: **Note** Lançamento pausado. Essa versão foi lançada em um conjunto limitado de gateways. • Corrija um problema com a falta de guias de segurança e cota ao usar o Windows Explorer em um compartil hamento SMB. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-02-02	1.28.1	Atualizações de manutenção: **Note** Lançamento pausado. Essa versão foi lançada em um conjunto limitado de gateways. • Corrija o problema com o SMB em relação ao acesso a arquivos sem distinção entre maiúsculas e minúsculas. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2026-01-21	1.27.19	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2026-01-16	1.28.0	Atualizações de manutenção: **Note** Lançamento pausado. Essa versão foi lançada em um conjunto limitado de gateways. • Atualização da pilha SMB. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-12-15	1.27.18	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-11-17	1.27.17	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2025-10-15	1.27.16	Atualizações de manutenção: • Correção de um problema no log da ordem de renomeação de upload. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-09-22	1.27.15	Atualizações de manutenção: • Correção de um problema no log da ordem de renomeação de upload.
2025-09-15	1.27.14	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-08-21	1.27.13	Atualizações de manutenção: • Adição de estatísticas e métricas do sistema para fornecer informações mais detalhadas sobre a performance do gateway.
2025-08-18	1.27.12	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2025-08-11	1.27.11	Atualizações de manutenção: • Correção de um problema que afetava as atualizaç ões de metadados do S3 em operações de arquivo específicas para alguns gateways.
2025-07-15	1.27.10	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance. • Solução dos problemas no log de ordem de renomeaçã o de upload para gateways.
2025-06-23	1.27.9	Atualizações de manutenção: • Solução dos problemas no log de ordem de renomeaçã o de upload para gateways. • Ativação do log de ordem de renomeação de upload para novos gateways. • Correção do problema para que o gateway agora manipule corretamente as operações de exclusão de arquivos cujo upload não foi feito com êxito.

Data de lançamento	Versão do software	Notas da versão
2025-06-16	1.27.8	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-05-26	1.27.7	Atualizações de manutenção: • Solução de problemas na ordem de renomeação. **Note** Esse problema afeta apenas alguns gateways. Você será notificado se seu gateway precisar ser atualizado. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-05-15	1.27.6	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2025-04-28	1.27.5	Atualizações de manutenção: • Correção dos problemas relacionados ao log de ordem de renomeação de upload. • Adição de ferramentas de depuração para ajudar a determinar as causas dos problemas de upload. • Adição de estatísticas e métricas do sistema para fornecer insights mais detalhados sobre a performance do gateway. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-04-14	1.27.4	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-04-01	1.27.3	Atualizações de manutenção: • Atualização para configuração do registro em log do gateway. Não será necessária nenhuma ação do cliente.

Data de lançamento	Versão do software	Notas da versão
2025-03-17	1.27.2	Atualizações de manutenção: • Adição de uma ação de API que remove dados e metadados de compartil hamento de arquivos em cache para arquivos que falharam no upload do seu gateway para o Amazon S3. Você Conta da AWS deve estar na lista de permissões para usar essa função. Se seu gateway tiver problemas com falha no upload de arquivos, AWS Support pode desbloquear a função e fornecer orientaçõ es sobre seu uso. • Adição da capacidade de novos gateways registrar em em log a ordem das operações de upload de renomeação de objetos. Isso ajuda a evitar que os arquivos falhem no upload para o Amazon S3 após operações de renomeação repetidas ou sobrepostas. • Correção de um problema relacionado à abertura involuntária de portas por SMB. • Atualização dos elementos do sistema operacional e

Data de lançamento	Versão do software	Notas da versão
		do software para melhorar a segurança e a performance.
2025-02-17	1.27.1	Atualizações de manutenção: • Remoção do Java 11. • Função de cache adicionad a para Suporte uso. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2025-01-17	1.27.0	Recursos: • Relatórios de cache (em breve): atualização do software de gateway para oferece suporte ao lançamento de um recurso futuro projetado para gerar relatórios dos metadados de arquivos atualmente armazenados em cache por um Gateway de Arquivos do S3. Você poderá usar esses relatórios para solucionar problemas se houver falha no upload de arquivos do seu gateway para o Amazon S3. Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2025-01-09	1.26.9	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2024-12-18	1.26.8	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
18/11/2024	1.26.7	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-10-17	1.26.6	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-09-30	1.26.5	Atualizações de manutenção: • Correção de um problema com gateways on-premises que não permitiam canais de suporte • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2024-09-16	1.26.3	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-08-21	1.26.1	Atualizações de manutenção: • Correção de um problema relacionado ao registro em log.
2024-08-19	1.26.0	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-07-16	1.25.2	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-06-17	1.25.1	Atualizações de manutenção: • Correção de um problema em atualizações ao usar um proxy com o DNS desabilit ado. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2024-05-15	1.25.0	Recursos: • Capacidade adicional de definir AES-128 ou AES-256 criptografar o mínimo. Essa é apenas uma alteração no gateway e estará disponível no console do Storage Gateway em uma próxima versão. • Aumento da rotação dos logs do sistema quando o espaço em disco está baixo. Anteriormente, a gravação de logs que preenchia o disco raiz fazia com que o gateway parasse. Agora, à medida que o espaço diminui, o gateway abre mais espaço para logs mais novos, eliminando os mais antigos. • Adição do caminho do S3 às notificações de integridade para erros de upload de arquivos. Anteriormente, as notificações de integridade mostravam apenas o caminho do arquivo no gateway. As notificações agora mostram o caminho para ajudar os usuários a localizar o arquivo no S3.

Data de lançamento	Versão do software	Notas da versão
		• O serviço agora ignora bloqueadores de backend durante exclusões forçadas de compartilhamento de arquivos. Anteriormente, as exclusões forçadas paravam sem explicação ao encontrar bloqueado res. As exclusões forçadas agora continuam ininterru ptas nesses cenários. Atualizações de manutenção: • Atualização da pilha NFS. • Atualização do Java 17 JRE. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-04-15	1.24.5	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-04-01	1.24.4	Atualizações de manutenção: • Correção do problema de ausência do component e Network Time Protocol (NTP).

Data de lançamento	Versão do software	Notas da versão
2024-03-18	1.24.3	Atualizações de manutenção: • Correção de um problema relacionado à performance de pesquisa com distinção de maiúsculas e minúsculas. • Correção de um problema que causava uma falha nos processadores. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.
2024-01-12	1.24.2	Atualizações de manutenção: • Solução de um problema de registro em log de SMB.
2023-12-27	1.24.1	Atualizações de manutenção: • Solução de um problema de estabilidade do SMB.

Data de lançamento	Versão do software	Notas da versão

2023-12-01	1.24,0	Recursos:
		• Atualização da pilha SMB.
		  • Foi adicionado suporte para AES-256 criptografia, além de variantes mais seguras de AES-128 criptografia e assinatura ao usar um cliente SMB 3.1.1 que a solicita.
		  • A cópia do lado do servidor do SMBv1 (LANMAN/CIFS) e a funcionalidade de expansão curinga do lado do servidor foram removidas. (O SMBv2 e o SMBv3 não foram afetados.) Isso pode afetar negativamente a performance de determinadas workloads do SMBv1. Se você usa SMBv1, recomendamos migrar para o SMBv2 ou o SMBv3.
		
		Atualizações de manutenção:
		• Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2023-10-24	1.23.2	Atualizações de manutenção: • Correção de um problema relacionado à não conexão adequada do canal de suporte para determinados usuários.
2023-08-14	1.23.1	Atualizações de manutenção: • Atualização do servidor NTP para usar o servidor de sincronização para novos gateways.
2023-06-12	1.23,0	Recursos: • Aumento do número de tópicos de upload para algumas AWS contas. Atualizações de manutenção: • Correção de um problema de violação de acesso em cópias grandes. • Correção de um problema de NFS. • Remoção do Java 8. • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2023-04-19	1.22.1	Atualizações de manutenção: • Correção de um problema relacionado à renomeação de pastas e arquivos.
2023-01-18	1.22.0	Recursos: • Adição de suporte para atributos do DOS. • Aumentamos o número de compartilhamentos de arquivos aceitos por gateway de 10 para 50. • Implementação de um mecanismo de detecção de distorção do relógio para determinar quando um gateway e um serviço estão fora de sincronia. Atualizações de manutenção: • Atualização da pilha SMB.
2022-07-06	1.21.2	Atualizações de manutenção: • Atualização dos elementos do sistema operacional e do software para melhorar a segurança e a performance.

Data de lançamento	Versão do software	Notas da versão
2022-02-16	1.21.1	Recursos: • Adição de novas métricas para renomeação e exclusão no cache. Atualizações de manutenção: • Correção de problemas em geral.
2022-01-18	1.21.0	Recursos: • Novas CloudWatch métricas adicionadas. • Adição de controle de utilização de largura de banda para uploads de dados.
2021-12-12	1.20.0	***URGENT UPDATE***: • Solução da vulnerabilidade do Log4j.

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.