Benutzerhandbuch

AWSStorage Gateway

API-Version 2013-06-30

AWSStorage Gateway: Benutzerhandbuch

Table of Contents

Was ist Amazon S3 File Gateway

AWSStorage Gateway verbindet eine lokale Software-Anwendung mit Cloud-basiertem Speicher, um eine nahtlose und sichere Integration mit Datensicherheitsfunktionen zwischen der lokalen IT-Umgebung und derAWSSpeicherinfrastruktur. Sie können den Dienst verwenden, um Daten imAWSCloud für skalierbaren und kosteneffizienten Speicher, in dem die Datensicherheit gewährleistet wird.AWS Storage Gateway bietet Speicherlösungen mit Dateien, Volume und Tapes.

Themen

Amazon S3 S3-Datei-Gateway-Dateien

Amazon S3 S3-Datei-Gateway-Dateien—Amazon S3 File Gateway unterstützt eine Dateischnittstelle inAmazon Simple Storage Service (Amazon S3)und kombiniert einen Service und eine virtuelle Software-Anwendung. Mit dieser Kombination können Sie Objekte in Amazon S3 über branchenkonforme Dateiprotokolle wie Network File System (NFS) und Server Message Block (SMB) speichern und abrufen. Die Software-Appliance oder das Gateway wird in Ihrer lokalen Umgebung als virtuelle Maschine (VM) auf VMware ESXi, Microsoft-Hyper-V oder Linux Kernel-basierte virtuelle Maschine (KVM) Hypervisor bereitgestellt. Das Gateway stellt Objekte in S3 als Dateien oder Dateifreigabe-Mountingpunkte bereit. Mit einem S3 File Gateway können Sie folgende Aktionen ausführen:

- Sie können Dateien direkt mithilfe von NFS Version 3 oder 4.1 speichern und abrufen.
- Sie können Dateien direkt mithilfe von SMB-Dateisystemversion 2 oder 3 speichern und abrufen.
- Sie können auf Ihre Daten direkt in Amazon S3 vonAWSCloud-Anwendung oder -Dienst.
- Sie können Ihre S3-Daten in mithilfe von Richtlinien für den Lebenszyklus, regionsübergreifender Replikation und Versioning verwalten. Sie können sich das S3-File Gateway als ein Dateisystem-Mount in Amazon S3 vorstellen.

Ein S3 File Gateway vereinfacht die Dateispeicherung in Amazon S3, lässt sich durch branchenübliche Dateisystemprotokolle in vorhandene Anwendungen integrieren und bietet eine wirtschaftliche Alternative zu lokalem Speicher. Es bietet auch einen schnellen Zugriff auf Daten über transparentes lokales Caching. Ein S3 File Gateway verwaltet die Datenübertragung von und nachAWSpuffert Anwendungen und Datenströme aus Netzwerküberlastungen, optimiert Daten

parallel und verwaltet Bandbreitennutzung. S3 File Gateway integrieren mitAWSDienstleistungen, z. B. mit folgenden:

- Gängige Zugriffsverwaltung mithilfe von AWS Identity and Access Management (IAM)
- Verschlüsselung mit AWS Key Management Service (AWS KMS)
- Überwachung mit Amazon CloudWatch (CloudWatch)
- Audit mitAWS CloudTrail(CloudTrail)
- Operationen mit der AWS Management Console und AWS Command Line Interface (AWS CLI)
- Fakturierung und Kostenmanagement

Die folgende Dokumentation enthält einen Abschnitt "Erste Schritte", in dem Informationen zur Einrichtung für alle Gateways erläutert werden. Außerdem gibt es Gateway-spezifische Abschnitte. Im Abschnitt "Erste Schritte" erfahren Sie, wie Speicher in einem Gateway bereitgestellt, aktiviert und konfiguriert wird. Im Abschnitt "Verwaltung" erfahren Sie, wie Sie das Gateway und die Ressourcen verwalten:

- Anweisungen zum Erstellen und Verwenden eines S3-File Gateways finden Sie unter. Hier erfahren Sie, wie Sie eine Datei freigeben, ein Laufwerk einem Amazon S3-Bucket zuweisen und Dateien und Ordner in Amazon S3 hochladen.

- beschreibt die Ausführung von Verwaltungsaufgaben für alle Gateway-Typen und Ressourcen.

In dieser Anleitung finden Sie in erster Linie Informationen zum Arbeiten mit den Gateway-Operationen mithilfe der AWS Management Console. Informationen zum programmgesteuerten Ausführen dieser Operationen finden Sie unterAWSReferenz Storage Gateway Speicher-Gateway-aus.

So funktioniert Storage Gateway (Architektur)

Im Folgenden finden Sie eine Übersicht über die Architektur der verfügbaren Storage Gateway Gateway-Lösungen.

Themen

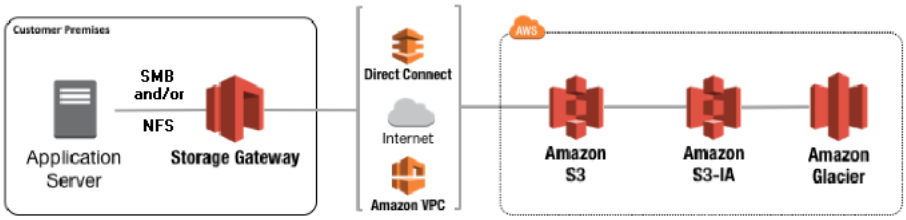
Amazon S3 S3-Datei-Gateways

Um ein S3-File Gateway zu verwenden, laden Sie zunächst ein VM-Abbild für das Gateway herunter. Anschließend aktivieren Sie das Gateway von derAWS Management Consoleoder über die Storage Gateway Gateway-API. Sie können ein S3-File Gateway auch unter Verwendung eines Amazon EC2 EC2-Abbildes erstellen.

Nachdem das S3 File Gateway aktiviert wurde, erstellen und konfigurieren Sie Ihre Dateifreigabe und ordnen diese Freigabe Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket zu. Auf diese Weise wird die Freigabe für Clients unter Verwendung des Network File System (NFS) - oder Server Message Block (SMB) -Protokolls zugänglich. In eine Dateifreigabe geschriebene Dateien werden in Amazon S3 zu Objekten, wobei der Pfad der Schlüssel ist. Es gibt eine 1:1 -Zuweisung zwischen Dateien und Objekten, und die Objekte in Amazon S3 werden asynchron aktualisiert, wenn Sie die Dateien ändern. Vorhandene Objekte im Amazon S3 S3-Bucket werden im Dateisystem als Dateien angezeigt und der Schlüssel wird zum Pfad. Die Objekte werden mit Amazon S3 — serverseitigen Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt. Die gesamte Datenübertragung erfolgt über HTTPS.

Der Service optimiert die Datenübertragung zwischen dem Gateway undAWSUm die verfügbare Bandbreite besser zu nutzen, verwenden Sie mehrteilige Uploads oder Downloads im Byte-Bereich. Lokaler Cache wird beibehalten, damit schneller Zugriff auf die Daten möglich ist, auf die zuletzt zugegriffen wurde, und damit Gebühren für den ausgehenden Datenverkehr reduziert werden. CloudWatch-Metriken bieten Einblicke in die Ressourcennutzung auf der VM und die Datenübertragungen zu und vonAWSaus. CloudTrail verfolgt alle API-Aufrufe.

Mit S3 File Gateway-Speicher kann für Aufgaben wie die Einbeziehung von Cloud-Workloads in Amazon S3, Sicherungen, Archivierungen, Abstufung und die Migration von Speicherdaten zurAWSCloud. Die folgende Abbildung zeigt eine Übersicht über die Bereitstellung von Dateispeicher für Storage Gateway.



S3 File Gateway konvertiert beim Hochladen von Dateien auf Amazon S3 Dateien in S3-Objekte. Die Interaktion zwischen Dateioperationen, die mit Dateifreigaben auf S3 File Gateway- und S3-Objekten durchgeführt werden, erfordert, dass bestimmte Vorgänge beim Konvertieren zwischen Dateien und Objekten sorgfältig abgewogen werden.

Gemeinsame Dateioperationen ändern Datei-Metadaten, was zum Löschen des aktuellen S3-Objekts und zur Erstellung eines neuen S3-Objekts führt. Die folgende Tabelle zeigt Beispiele für Dateioperationen und die Auswirkungen auf S3-Objekte.

Dateivorgängen	Auswirkungen auf S3-Objekte	Auswirkungen auf Speicherk lasse
Datei umbenennen	Ersetzt vorhandenes S3-Objekt und erstellt für jede Datei ein neues S3-Objekt	Es können Gebühren für vorzeitige Löschung und Abrufgebühren anfallen
Ordner umbenennen	Ersetzt alle vorhandenen S3-Objekte und erstellt neue S3-Objekte für jeden Ordner und jede Datei in der Ordnerstr uktur	Es können Gebühren für vorzeitige Löschung und Abrufgebühren anfallen
Datei-/Ordnerberechtigungen ändern	Ersetzt vorhandenes S3-Objekt und erstellt ein neues S3-Objekt für jede Datei oder jeden Ordner	Es können Gebühren für vorzeitige Löschung und Abrufgebühren anfallen
Ändern Sie den Besitz von Datei/Ordnern	Ersetzt vorhandenes S3-Objekt und erstellt ein neues S3-Objekt für jede Datei oder jeden Ordner	Es können Gebühren für vorzeitige Löschung und Abrufgebühren anfallen

Dateivorgängen	Auswirkungen auf S3-Objekte	Auswirkungen auf Speicherklasse
An eine Datei anhängen	Ersetzt vorhandenes S3-Objekt und erstellt für jede Datei ein neues S3-Objekt	Es können Gebühren für vorzeitige Löschung und Abrufgebühren anfallen

Wenn eine Datei von einem NFS- oder SMB-Client in das S3 File Gateway geschrieben wird, lädt das Datei-Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von seinen Metadaten (Eigentümerschaften, Zeitstempel usw.). Durch das Hochladen der Dateidaten wird ein S3-Objekt erstellt, und das Hochladen der Metadaten für die Datei aktualisiert die Metadaten für das S3-Objekt. Dieser Prozess erstellt eine andere Version des Objekts, was zu zwei Versionen eines Objekts führt. Wenn S3-Versioning aktiviert ist, werden beide Versionen gespeichert.

Wenn eine Datei im S3 File Gateway von einem NFS- oder SMB-Client geändert wird, nachdem sie auf Amazon S3 hochgeladen wurde, lädt das S3 File Gateway die neuen oder geänderten Daten hoch, anstatt die gesamte Datei hochzuladen. Die Dateiänderung führt dazu, dass eine neue Version des S3-Objekts erstellt wird.

Wenn das S3 File Gateway größere Dateien hochlädt, muss es möglicherweise kleinere Teile der Datei hochladen, bevor der Client mit dem Schreiben in das S3 File Gateway fertig ist. Einige Gründe dafür sind die Freigabe von Cache-Speicherplatz oder eine hohe Schreibrate in eine Dateifreigabe. Dies kann zu mehreren Versionen eines Objekts im S3-Bucket führen.

Sie sollten Ihren S3-Bucket überwachen, um festzustellen, wie viele Versionen eines Objekts vorhanden sind, bevor Sie Lebenszyklusrichtlinien einrichten, um Objekte in verschiedene Speicherklassen zu verschieben. Sie sollten den Lebenszyklusablauf für frühere Versionen konfigurieren, um die Anzahl der Versionen zu minimieren, die Sie für ein Objekt in Ihrem S3-Bucket haben. Die Verwendung der Replikation derselben Region (SRR) oder regionsübergreifender Replikation (CRR) zwischen S3-Buckets erhöht den verwendeten Speicher.

Einrichten für Amazon S3 File Gateway

In diesem Abschnitt erhalten Sie Anweisungen für die ersten Schritte mit Amazon S3 File Gateway. Um mit den ersten Schritten zu beginnen, registrieren Sie sich zunächst fürAWSaus. Wenn Sie erstmaliger Benutzer sind, empfehlen wir, die-RegionenundVoraussetzungenAbschnitten erstellt

Themen

- Bei Amazon Web Services registrieren
- Erstellen eines IAM-Benutzers
- Setup-Anforderungen für das File
- Zugriff auf AWS Storage Gateway
- Unterstützte AWS-Regionen

Bei Amazon Web Services registrieren

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Sich für ein AWS-Konto (AWS-Konto) registrieren

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Erstellen eines IAM-Benutzers

Nachdem Sie Ihre erstellt habenAWS-Konto: Führen Sie die folgenden Schritte aus, um eineAWS Identity and Access ManagementBenutzer (IAM) für Sie selbst. Dann fügen Sie diesen Benutzer einer Gruppe hinzu, der über Administratorrechte verfügt.

Einen Administratorbenutzer für sich selbst erstellen und einer Administratorengruppe hinzufügen (Konsole)

1. Melden Sie sich bei der IAM console (IAM-Konsole) als Kontoinhaber an, indem Sie Root user (Stammbenutzer) auswählen und die E-Mail-Adresse Ihres AWS-Konto eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   > **Note**
   >
   > Wir empfehlen ausdrücklich, die bewährten Verfahren mithilfe des IAM-**`Administrator`**Benutzers unten zu verwenden und die Anmeldeinformationen des Stammbenutzers an einem sicheren Ort auzubewahren. Melden Sie sich als Stammbenutzer an, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

2. Wählen Sie im Navigationsbereich Users (Benutzer) und dann Add User (Benutzer hinzufügen) aus.
3. Geben Sie unter User Name (Benutzername) den Text **`Administrator`** ein.
4. Aktivieren Sie das Kontrollkästchen neben AWS Management Console access (Konsolenzugriff). Wählen Sie dann Custom password (Benutzerdefiniertes Passwort) aus und geben Sie danach ein neues Passwort in das Textfeld ein.
5. (Optional) Standardmäßig erfordert AWS, dass der neue Benutzer bei der ersten Anmeldung ein neues Passwort erstellt. Sie können das Kontrollkästchen neben User must create a new password at next sign-in (Benutzer muss bei der nächsten Anmeldung ein neues Passwort erstellen) deaktivieren, damit der neue Benutzer sein Kennwort nach der Anmeldung zurücksetzen kann.
6. Wählen Sie Weiter. Berechtigungen.
7. Wählen Sie unter Set permissions (Berechtigungen festlegen) die Option Add user to group (Benutzer der Gruppe hinzufügen) aus.
8. Wählen Sie Gruppe erstellen aus.
9. Geben Sie im Dialogfeld Create group (Gruppe erstellen) unter Group name (Gruppenname) den Wert **`Administrators`** ein.
10. Wählen Sie Filter policies (Filterrichtlinien) und anschließend AWS managed – job function (AWS-verwaltet – Auftragsfunktion) aus, um den Tabelleninhalt zu filtern.
11. Aktivieren Sie in der Richtlinienliste das Kontrollkästchen AdministratorAccess. Wählen Sie dann Create group (Gruppe erstellen) aus.

> **Note**
>
> Sie müssen den Zugriff der IAM-Benutzer und -Rollen auf die Fakturierung aktivieren, bevor Sie die `AdministratorAccess`-Berechtigungen verwenden können, um auf die AWS Fakturierung und Kostenmanagement-Konsole zuzugreifen. Befolgen Sie hierzu die Anweisungen in Schritt 1 des Tutorials zum Delegieren des Zugriffs auf die Abrechnungskonsole.

12. Kehren Sie zur Gruppenliste zurück und aktivieren Sie das Kontrollkästchen der neuen Gruppe. Möglicherweise müssen Sie Refresh (Aktualisieren) auswählen, damit die Gruppe in der Liste angezeigt wird.
13. Wählen Sie Weiter. Tags.
14. (Optional) Fügen Sie dem Benutzer Metadaten hinzu, indem Sie Markierungen als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Markierungen in IAM finden Sie unter Tagging von IAM-Entitäten im IAM-Leitfaden.
15. Wählen Sie Weiter. PrüfenUm eine Liste der Gruppenmitgliedschaften anzuzeigen, die dem neuen Benutzer hinzugefügt werden soll. Wenn Sie bereit sind, fortzufahren, wählen Sie Create user (Benutzer erstellen) aus.

Mit diesen Schritten können Sie weitere Gruppen und Benutzer erstellen und Ihren Benutzern Zugriff auf Ihre AWS-Konto-Ressourcen gewähren. Informationen zur Verwendung von Richtlinien, die die Benutzerrechte auf bestimmte AWS-Ressourcen beschränken, finden Sie unter Zugriffsverwaltung und Beispielrichtlinien.

Setup-Anforderungen für das File

Sofern nicht anders angegeben gelten die folgenden Anforderungen für alle File Gateway-Typen inAWS Storage Gatewayaus. Ihr Setup muss die Anforderungen in diesem Abschnitt erfüllen. Überprüfen Sie die Anforderungen, die für Ihr Gateway-Setup gelten, bevor Sie Ihr Gateway bereitstellen.

Themen

- Unterstützte Hypervisoren und Host-Anforderungen
- Unterstützte NFS-Clients für ein File Gateway
- Unterstützte SMB-Clients für ein File Gateway
- Unterstützte Dateisystemoperationen für ein File Gateway

Erforderliche Voraussetzungen

Bevor Sie ein Amazon FSx File Gateway (FSx File Gateway) verwenden, müssen Sie die folgenden Anforderungen erfüllen:

- Erstellen und konfigurieren Sie ein FSx for Windows File Server-Dateisystem. Detaillierte Anweisungen finden Sie unterSchritt 1: Erstellen Sie Ihr DateisystemimAmazon FSx for Windows File Server Benutzerhandbuchaus.
- Konfigurieren Sie Microsoft Active Directory (AD).
- Stellen Sie sicher, dass zwischen dem Gateway undAWSaus. Zum erfolgreichen Herunterladen, Aktivieren und Aktualisieren des Gateways sind mindestens 100 Mbit/s erforderlich.
- Konfigurieren Sie Ihr privates Netzwerk, VPN oderAWS Direct ConnectZwischen Ihrer Amazon Virtual Private Cloud (Amazon VPC) und der lokalen Umgebung, in der Sie Ihr FSx File Gateway bereitstellen.
- Stellen Sie sicher, dass Ihr Gateway den Namen Ihres Active Directory-Domänencontrollers auflösen kann Sie können DHCP in Ihrer Active Directory-Domäne verwenden, um die Auflösung zu verarbeiten, oder einen DNS-Server manuell über das Menü Einstellungen der Netzwerkkonfiguration in der lokalen Gateway-Konsole angeben.

Hardware- und Speicheranforderungen

In den folgenden Abschnitten erhalten Sie Informationen über die mindestens erforderliche Hardware und Einstellungen für Ihr Gateway sowie den minimalen Festplattenspeicherplatz, der für den erforderlichen Speicher reserviert werden muss.

Informationen zu bewährten Methoden für die Leistung von File Gateways finden Sie unter Leitfaden zur Leistung von Datei-Gateways.

Hardwareanforderungen für lokale VMs

Stellen Sie bei einer lokalen Bereitstellung des Gateways sicher, dass die zugrunde liegende Hardware, auf der Sie die virtuelle Gateway-Maschine (VM) bereitstellen, mindestens die folgenden Ressourcen reservieren können:

- Vier virtuelle Prozessoren für die VM
- 16 GiB reserviertes RAM für File Gateways
- 80 GiB Festplattenspeicher zur Installation des VM-Abbilds sowie für die Systemdaten

Weitere Informationen finden Sie unter Optimieren der Gateway-Leistung. Weitere Informationen zu den Auswirkungen der Hardware auf die Leistung der Gateway-VM finden Sie unter Kontingente für Dateifreigaben.

Anforderungen für Amazon EC2 EC2-Instance-Typen

Bei der Bereitstellung des Gateways in Amazon Elastic Compute Cloud (Amazon EC2) muss die Instance-Größe mindestens betragen**`xlarge`**damit Ihr Gateway funktioniert. Doch für die Instance-Familie, die für die Datenverarbeitung optimiert ist, muss die Größe mindestens**`2xlarge`**aus. Verwenden Sie einen der folgenden für Ihr Gateway empfohlenen Instance-Typen.

Empfohlen für File Gateway-Typen

- Allzweck-Instance-Familie — Instance-Typ m4 oder m5.
- Instance-Familie „Für Datenverarbeitung optimiert“: Instance-Typ c4 oder c5. Wählen Sie die Instance-Größe 2xlarge oder höher aus, um die erforderlichen RAM-Anforderungen zu erfüllen.
- Speicheroptimierte Instance-Familie — Instance-Typen r3.
- Speicheroptimierte Instance-Familie — Instance-Typen i3.

> **Note**
>
> Wenn Sie Ihr Gateway in Amazon EC2 starten und der Instance-Typ, den Sie ausgewählt haben, flüchtigen Speicher unterstützt, werden die Datenträger automatisch aufgelistet. Weitere Informationen zum Amazon EC2 EC2-Instance-Speicher finden Sie unterInstance-SpeicherimAmazon EC2 EC2-Benutzerhandbuch
> Anwendungs-Schreibvorgänge werden im Cache synchron gespeichert und dann asynchron in permanenten Speicher in Amazon S3 hochgeladen. Wenn der flüchtige

Speicher verlorengeht, weil eine -Instance angehalten wird, bevor der Upload abgeschlossen ist, können die Daten verlorengehen, die sich noch im Cache befinden und noch nicht in Amazon Simple Storage Service (Amazon S3) geschrieben wurden. Bevor Sie die Instance anhalten, die das Gateway hostet, stellen Sie sicher, dass die`CachePercentDirty`CloudWatch-Metrik ist`0`aus. Weitere Informationen zum flüchtigen Speicher finden Sie unter Verwenden von kurzlebigem Speicher mit EC2-Gateways. Weitere Informationen zur Überwachung von Metriken für Ihr Speicher-Gateway finden Sie unterÜberwachen Sie Ihr Datei-Gatewayaus.
Wenn Sie über mehr als 5 Millionen Objekte in Ihrem S3-Bucket verfügen und ein Allzweck-SSD-Volume verwenden, ist mindestens ein EBS-Stamm-Volume von 350 GiB notwendig, um eine akzeptable Leistung Ihres Gateways beim Starten zu gewährleisten. Weitere Informationen zum Erhöhen der Volume-Größe finden Sie unterÄndern eines EBS-Volumes mit elastischen Volumes (Konsole)aus.

Speicheranforderungen

Neben 80 GiB Festplattenspeicher für die VM benötigen Sie außerdem zusätzliche Datenträger für das Gateway.

Gateway-Typ	Cache (mindestens)	Cache (maximal)			
File Gateway	150 GiB	64 TiB			

Note

Sie können ein oder mehrere lokale Laufwerke für Ihren Cache bis zur maximalen Kapazität konfigurieren.
Wenn Sie einen Cache zu einem vorhandenen Gateway hinzufügen, müssen neue Datenträger auf Ihrem Host (Hypervisor oder Amazon EC2 EC2-Instance) erstellt werden. Ändern Sie nicht die Größe von vorhandenen Datenträgern, wenn die Datenträger zuvor als Cache zugewiesen wurden.

Informationen zu Gateway-Kontingenten finden Sie unter Kontingente für Dateifreigaben.

Netzwerk- und Firewall-Anforderungen

Das Gateway muss unter anderem auf das Internet, lokale Netzwerke, DNS (Domain Name Service)-Server, Firewalls und Router zugreifen können.

Die Anforderungen an die Netzwerkbandbreite variieren je nach Datenmenge, die vom Gateway hochgeladen und heruntergeladen wird. Es sind mindestens 100 Mbit/s erforderlich, um das Gateway erfolgreich herunterzuladen, zu aktivieren und zu aktualisieren. Ihre Datenübertragungsmuster bestimmen die Bandbreite, die zur Unterstützung Ihrer Arbeitsbelastung erforderlich ist.

Nachfolgend finden Sie Informationen zu den erforderlichen Ports sowie eine Anleitung zur Gewährung von Zugriff über Firewalls und Router.

> **Note**
>
> In einigen Fällen können Sie FSx File Gateway auf Amazon EC2 bereitstellen oder andere Arten von Bereitstellungen (einschließlich lokal) mit Netzwerksicherheitsrichtlinien verwenden, die einschränkenAWSIP-Adressbereiche. In diesen Fällen kann es auf dem Gateway zu Problemen mit der Service-Konnektivität kommen, wennAWSDie Werte im IP-Bereich ändern sich. DieAWSDie zu verwendenden Werte für den IP-Adressbereich befinden sich in der Amazon-Service-Untergruppe für dieAWSRegion, in der Sie Ihr Gateway aktivieren. Die aktuellen Werte für den IP-Bereich finden Sie unterAWSIP-AdressbereicheimAWS– Allgemeine Referenzaus.

Themen

Port-Anforderungen

Storage Gateway erfordert, dass bestimmte Ports für den Betrieb zugelassen werden. Die folgende Abbildung zeigt die erforderlichen Ports, die Sie für jede Art von Gateway zulassen müssen. Einige Ports werden von allen Gateway-Typen und andere Ports von bestimmten Gateway-Typen benötigt. Weitere Informationen zu den Anforderungen für Ports finden Sie unter Port-Anforderungen.

Allgemeine Ports für alle Gateway-Typen

Die folgenden Ports werden von allen Gateway-Typen verwendet und sind für alle Gateway-Typen erforderlich.

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
TCP	443 (HTTPS)	Ausgehend	Storage Gateway	AWS	Für die Kommunikation vom Storage Gateway zumAWSService-Endpunkt. Informationen über Service-Endpunkte finden Sie unter Gewähren von Zugriff über Firewalls und Router für AWS Storage Gateway.
TCP	80 (HTTP)	Eingehend	Der Host, von dem aus Sie sich mit demAWS Management Consoleaus.	Storage Gateway	Durch lokale Systeme zum Abrufen des Speicher-Gateway-Aktivierungsschlüssels. Port

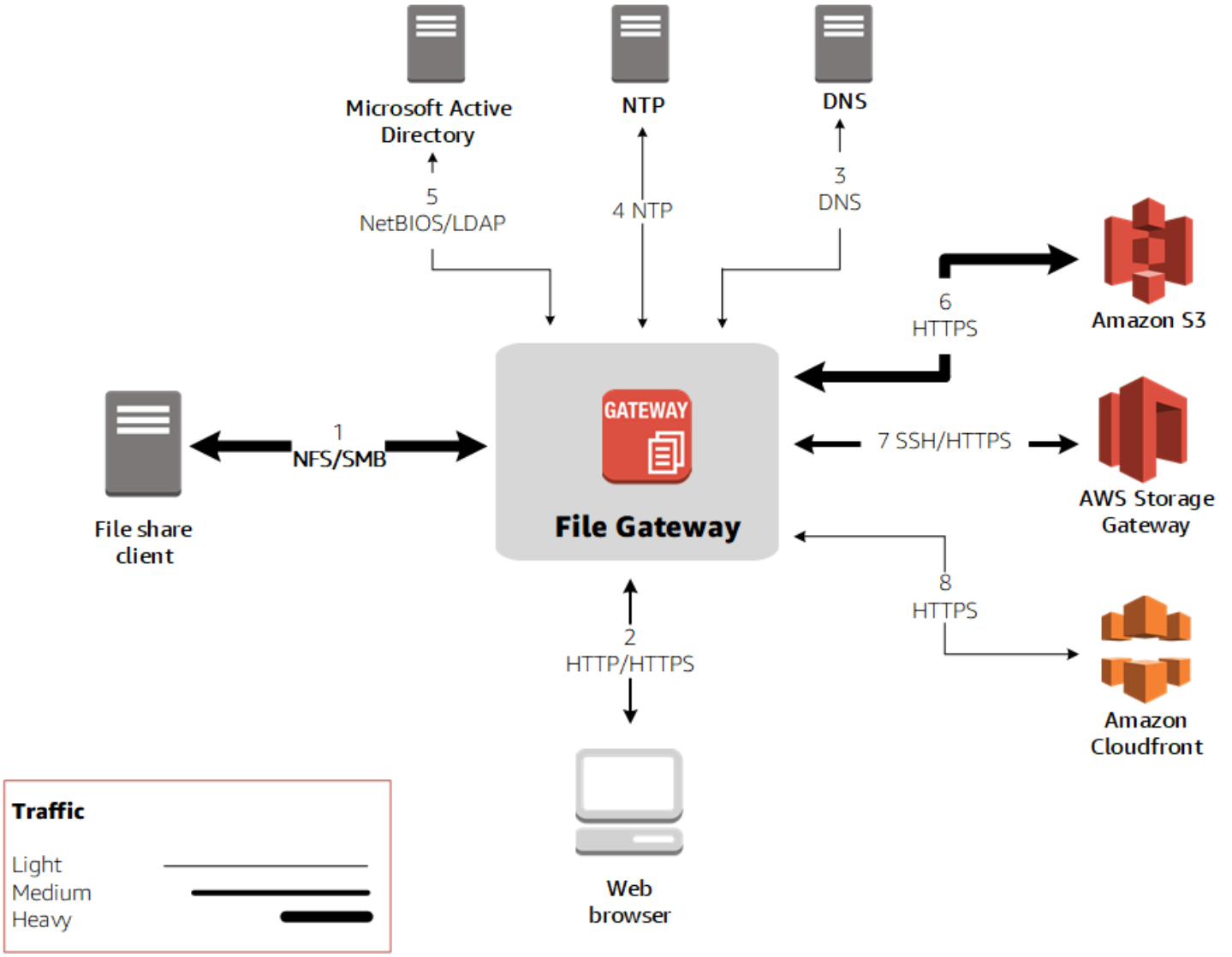
Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
					80 wird nur während der Aktivierung der Storage Gateway Gateway-Appliance verwendet. Storage Gateway erfordert keinen Port 80, um öffentlich zugänglich zu sein. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie das Gateway von der Storage Gateway Gateway-Konsole aus aktivieren, muss der Host, von

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
					dem aus Sie die Verbindung mit der Konsole herstellen, Zugriff auf Port 80 des Gateways haben.
UDP/UDP	53 (DNS)	Ausgehend	Storage Gateway	DNS-Server	Für die Kommunikation zwischen Storage Gateway und DNS-Server

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
TCP	22 (Support-Kanal)	Ausgehend	Storage Gateway	Support	ErlaubtSupportUm auf Ihr Gateway zuzugreifen, um Ihnen bei der Behandlung von Gateway-Problemen zu helfen Dieser Port muss für den normalen Betrieb des Gateways nicht offen sein, für die Fehlerbehebung ist dies jedoch erforderlich.
UDP	123 (NTP)	Ausgehend	NTP-Client	NTP-Server	Verwendet von lokalen Systemen zur Synchronisierung der VM-Zeit mit der Host-Zeit.

Ports für File Gateways

Die folgende Abbildung zeigt die Ports, die für ein S3-Datei-Gateway offen sein müssen.



> **Note**
>
> Weitere Informationen zu spezifischen Port-Anforderungen finden Sie unterPort-Anforderungenaus.

Für S3 File Gateway müssen Sie nur Microsoft Active Directory verwenden, wenn Sie Domänennutzern erlauben möchten, auf eine SMB-Dateifreigabe (Server Message Block) zuzugreifen. Sie können Ihr File Gateway mit jeder gültigen Microsoft Windows-Domäne (aufgelöst durch DNS) verbinden.

Sie können auch dieAWS Directory Serviceum einAWS Managed Microsoft ADIn der Amazon Web Services Cloud erstellt. Für die meistenAWS Managed Microsoft ADBereitstellungen müssen Sie

den DHCP-Service (Dynamic Host Configuration Protocol) für Ihre VPC konfigurieren. Weitere Informationen zum Erstellen eines DHCP-Optionssatzes finden Sie unterErstellen einer DHCP-OptionslisteimAWS Directory ServiceAdministratorhandbuchaus.

Neben den allgemeinen Ports erfordert Amazon S3 File Gateway die folgenden Ports.

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
TCP/UDP	2049 (NFS)	Eingehend	NFS-Kunden	Storage Gateway	Für lokale Systeme zum Herstelle n einer Verbindun g zu vom Gateway verfügbar gemachte NFS-Freig aben.
TCP/UDP	111 (NfsV3)	Eingehend	nfsV3-Kunde	Storage Gateway	Für lokale Systeme zum Herstelle n einer Verbindun g zum vom Gateway verfügbar gezeigten Port-Mapper. **Note** Dieser Port wird nur

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
					für NfsV3 benötigt.
TCP/UDP	20048 (NfsV3)	Eingehend	nfsV3-Kunde	Storage Gateway	Für lokale Systeme zum Herstellen einer Verbindung zu vom Gateway verfügbar gemachte Mounts. **Note** Dieser Port wird nur für NfsV3 benötigt.

Netzwerk- und Firewall-Anforderungen für die Storage Gateway Hardware Appliance

Jede Storage Gateway Gateway-Hardware-Appliance erfordert die folgenden Netzwerkdienste:

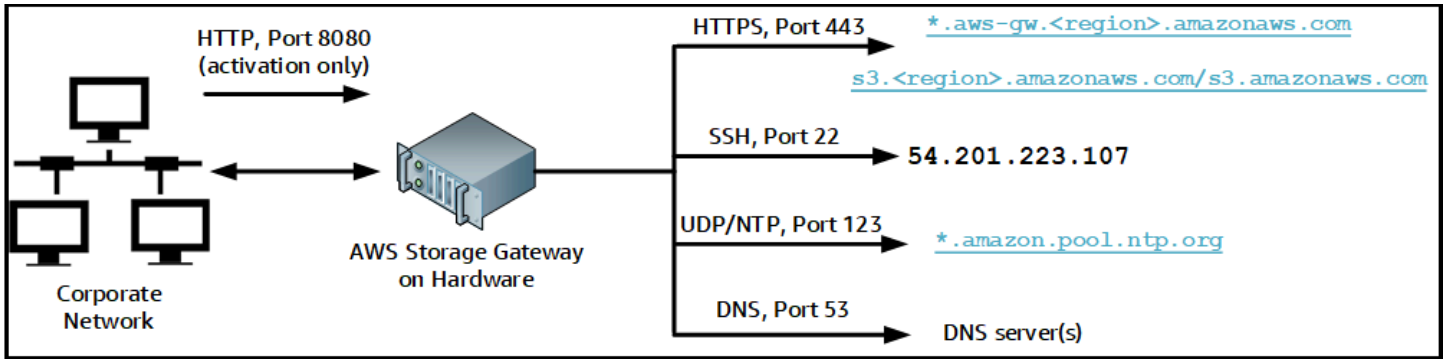
- Internetzugang— eine ständig aktive Verbindung zum Internet über eine Netzwerkschnittstelle auf dem Server.

- DNS-Dienste— DNS-Services für die Kommunikation zwischen der Hardware-Appliance und dem DNS-Server
- Zeitsynchronisierung— Ein automatisch konfigurierter Amazon NTP-Zeitservice muss erreichbar sein.
- IP-Adresse— Eine zugewiesene DHCP- oder statische IPv4-Adresse. Sie können keine IPv6-Adressen zuweisen.

Es gibt fünf physische Netzwerk-Ports auf der Rückseite des Servers Dell PowerEdge R640. Bei diesen Ports handelt es sich von links nach rechts (zur Rückseite des Servers hin) um:

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

Sie können den iDRAC-Port für die Remote-Serververwaltung verwenden.



Eine Hardware-Appliance benötigt die folgenden Ports.

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
SSH	22	Ausgehend	Hardware-Appliance	`54.201.223.107`	Support-Kanal

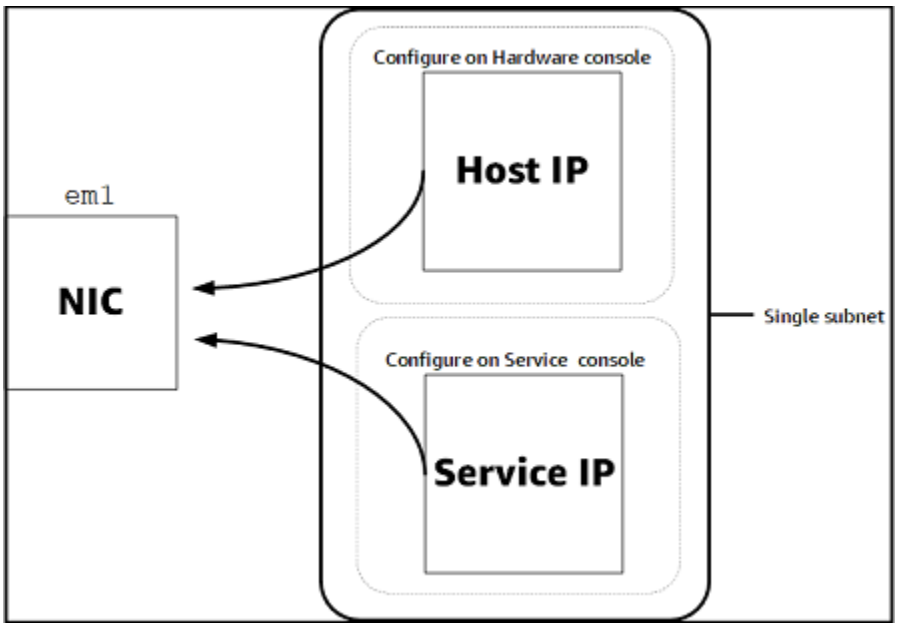
Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
DNS	53	Ausgehend	Hardware-Appliance	DNS-Server	Namensauflösung
UDP/NTP	123	Ausgehend	Hardware-Appliance	`*.amazon.pool.ntp.org`	Zeitsynchronisierung
HTTPS	443	Ausgehend	Hardware-Appliance	`*.amazonaws.com`	Datenübertragung
HTTP	8080	Eingehend	AWS	Hardware-Appliance	Aktivierung (nur kurz)

Eine Hardware-Appliance erfordert die folgenden Netzwerk- und Firewalleinstellungen, um richtig zu funktionieren:

- Konfigurieren Sie alle verbundenen Netzwerkschnittstellen in der Hardwarekonsole.
- Stellen Sie sicher, dass jede Netzwerkschnittstelle sich in einem eindeutigen Subnetz befindet.
- Stellen Sie allen verbundenen Netzwerkschnittstellen Zugriff auf ausgehenden Datenverkehr auf die im vorangehenden Diagramm aufgeführten Endpunkte bereit.
- Konfigurieren Sie mindestens eine Netzwerkschnittstelle zur Unterstützung der Hardware-Appliance. Weitere Informationen finden Sie unter Konfigurieren von Netzwerkparametern.

> **Note**
>
> Eine Abbildung der Rückseite des Servers mit seinen Ports finden Sie unterMontieren Sie Ihre Hardware-Appliance im Rack und verbinden Sie sie mit Stromaus.

Alle IP-Adressen auf derselben Netzwerkschnittstelle (NIC), für ein Gateway und einen Host gleichermaßen, müssen sich im gleichen Subnetz befinden. In der folgenden Abbildung ist das Adressierungsschema dargestellt.



Weitere Informationen zum Aktivieren und Konfigurieren einer Hardware-Appliance finden Sie unterVerwenden der Storage Gateway Hardware Applianceaus.

Gewähren von Zugriff über Firewalls und Router für AWS Storage Gateway

Das Gateway muss Zugriff auf die folgenden Service-Endpunkte haben, um mit kommunizieren zu könnenAWSaus. Wenn Sie eine Firewall oder einen Router verwenden, um den Netzwerkverkehr zu filtern oder zu begrenzen, müssen Sie die Firewall und den Router so konfigurieren, dass diese Service-Endpunkte für die ausgehende Kommunikation inAWSaus.

> **Important**
>
> Abhängig von Ihrem GatewayAWSRegion, ersetzen*Region*im Dienstendpunkt mit der richtigen Regions-Zeichenfolge.

Der folgende Service-Endpunkt ist von allen Gateways für Head-Bucket-Operationen erforderlich.

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

Die folgenden Dienstendpunkte werden von allen Gateways für den Steuerpfad benötigt (`anon-cp`,`client-cp`,`proxy-app`) und Datenpfad (`dp-1`) operationen erstellt.

```
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
```

Der folgende Gateway-Service-Endpunkt ist für API-Aufrufe erforderlich.

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

Das folgende Beispiel ist ein Gateway-Service-Endpunkt in der Region USA West (Oregon) (`us-west-2`) enthalten.

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

Der Amazon S3-Service-Endpunkt unten wird ausschließlich von File Gateways genutzt. Ein File Gateway benötigt diesen Endpunkt, um auf den Amazon S3 S3-Bucket zugreifen zu können, der einer Dateifreigabe zugeordnet ist.

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

Das folgende Beispiel ist ein Amazon S3-Service-Endpunkt in der Region USA Ost (Ohio) (`us-east-2`) enthalten.

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

> **Note**
>
> Wenn Ihr Gateway dieAWSIn der Region, in der sich Ihr S3-Bucket befindet, ist dieser Service-Endpunkt standardmäßig aufs`3.us-east-1.amazonaws.com`aus. Wir empfehlen, den Zugang zur US East (N. Virginia) -Region (`us-east-1`) zusätzlich zu Regionen, in denen Ihr Gateway aktiviert ist und in denen sich Ihr S3-Bucket befindet.

Im Folgenden werden Amazon S3-Service-Endpunkte fürAWS GovCloud (US)Regionen.

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

Das folgende Beispiel ist ein FIPS-Service-Endpunkt für einen S3-Bucket imAWSGovCloud (US-West) Region.

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

Der folgende Amazon CloudFront CloudFront-Endpunkt ist erforderlich, damit Storage Gateway die Liste der verfügbaren abrufen kannAWSRegionen.

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

Eine Storage Gateway Gateway-VM ist so konfiguriert, dass die folgenden NTP-Server verwendet werden.

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

- Storage Gateway — Für unterstützteAWSRegionen und eine Liste vonAWSService-Endpoints, die Sie mit Storage Gateway verwenden können, sieheAWS Storage Gateway-Endpunkte und -KontingenteimAWS– Allgemeine Referenzaus.
- Storage Gateway Gateway-Hardware-Appliance — Für unterstützteAWSRegionen, die Sie mit der Hardware-Appliance verwenden können, finden Sie unterRegionen der Speicher-Gateway-HardwarimAWS– Allgemeine Referenzaus.

Konfigurieren von Sicherheitsgruppen für Ihre Amazon EC2 EC2-Gateway-Instance

In :AWS Storage Gatewaysteuert eine Sicherheitsgruppe den Datenverkehr zu Ihrer Amazon EC2 EC2-Gateway-Instance. Wenn Sie eine Sicherheitsgruppe konfigurieren, empfehlen wir Folgendes:

- Die Sicherheitsgruppe sollte keine eingehenden Verbindungen aus dem externen Internet zulassen. Sie sollte festlegen, dass ausschließlich Instances innerhalb der Gateway-Sicherheitsgruppe mit dem Gateway kommunizieren dürfen.

  Müssen Instances von außerhalb der Gateway-Sicherheitsgruppe eine Verbindung mit dem Gateway herstellen, empfehlen wir, solche Verbindungen ausschließlich auf Port 3260 (iSCSI-Verbindungen) und Port 80 (Aktivierung) zuzulassen.

- Wenn Sie Ihr Gateway von einem Amazon EC2 EC2-Host außerhalb der Gateway-Sicherheitsgruppe aktivieren möchten, müssen Sie auf Port 80 eingehende Verbindungen von der IP-Adresse dieses Hosts zulassen. Falls Sie die IP-Adresse des zur Aktivierung verwendeten Hosts nicht kennen, können Sie Port 80 öffnen, Ihr Gateway aktivieren und Port 80 nach der Aktivierung wieder für Zugriffe schließen.
- Erlauben Sie Zugriffe über Port 22 nur, wenn Sie Support für die Problembehebung verwenden Weitere Informationen finden Sie unter Du willstSupportum bei der Fehlerbehebung bei Ihrem EC2-Gateway zu helfen.

In manchen Fällen können Sie eine Amazon EC2-Instance als Initiator verwenden (um eine Verbindung zu den iSCSI-Zielen auf dem in Amazon EC2 bereitgestellten Gateway herzustellen). In diesem Fall empfehlen wir eine Vorgehensweise in zwei Schritten:

1. Starten Sie die Initiator-Instance in derselben Sicherheitsgruppe wie das Gateway.
2. Konfigurieren Sie den Zugriff so, dass der Initiator mit dem Gateway kommunizieren kann.

Weitere Informationen zu den für das Gateway zu öffnenden Ports finden Sie unter Port-Anforderungen.

Unterstützte Hypervisoren und Host-Anforderungen

Sie können Storage Gateway entweder lokal als VM-Appliance (virtuelle Maschine) oder physische Hardware-Appliance ausführen oder inAWSals Amazon EC2 EC2-Instance erstellt.

Storage Gateway unterstützt die folgenden Hypervisor-Versionen und Hosts:

- VMware ESXi Hypervisor (Version 6.0, 6.5 oder 6.7) — Eine kostenlose Version von VMware finden Sie auf derVMware-Webseiteaus. Für diese Einrichtung benötigen Sie außerdem einen VMware vSphere-Client, um eine Verbindung mit dem Host herstellen zu können.
- Microsoft Hypervisor 2012 Hyper-V (Version 2012 R2 oder 2016) — Eine kostenlose Standalone-Version von Hyper-V finden Sie imMicrosoft-Downloadcenteraus. Um einen Microsoft Windows-basierten Client-Computer mit dem Host verbinden zu können, benötigen Sie für diese Einrichtung einen Microsoft Hyper-V-Manager.
- Linux Kernel-basierte virtuelle Maschine (KVM) — Eine kostenlose Open-Source-Virtualisierungstechnologie. KVM ist in allen Versionen der Linux-Version 2.6.20 und neuer enthalten. Storage Gateway wird für die Centos/Rhel 7.7-, Ubuntu 16.04 LTS- und Ubuntu 18.04 LTS-Distributionen getestet und unterstützt. Jede andere moderne Linux-Verteilung kann

funktionieren, aber weder Funktion noch Leistung werden garantiert. Wir empfehlen diese Option, wenn Sie bereits über eine KVM-Umgebung verfügen und bereits mit der Funktionsweise von KVM vertraut sind.

- Amazon EC2 EC2-Instance: Storage Gateway stellt ein Amazon Machine Image (AMI) mit dem Abbild der Gateway-VM bereit. Weitere Informationen zur Bereitstellung von Gateways auf Amazon EC2 finden Sie unterBereitstellen eines File Gateways auf einem Amazon EC2 EC2-Hostaus.
- Storage Gateway-Hardware-Appliance: Storage Gateway bietet eine physische Hardware-Appliance als lokale Bereitstellungsoption für Standorte mit eingeschränkter Infrastruktur für virtuelle Maschinen.

> **Note**
>
> Storage Gateway unterstützt nicht die Wiederherstellung eines Gateways von einer VM, die aus einem Snapshot oder Klon einer anderen Gateway-VM oder aus Ihrem Amazon EC2 EC2-AMI erstellt wurde. Wenn Ihre Gateway-VM nicht funktioniert, aktivieren Sie ein neues Gateway und stellen Sie Ihre Daten zu diesem Gateway wieder her. Weitere Informationen finden Sie unter Wiederherstellen von einem unerwarteten Shutdown der virtuellen Maschine. Storage Gateway unterstützt keinen dynamischen Speicher und virtuelle Speicherballonierung.

Unterstützte NFS-Clients für ein File Gateway

File Gateways unterstützen die folgenden Network File System (NFS)-Clients:

- Amazon Linux
- MacOS X

> **Note**
>
> Wir empfehlen die`rsize`und`wsize`Bereitstellen von Optionen auf 64 KB, um die Leistung beim Einhängen von NFS-Dateifreigaben unter Mac OS X zu verbessern.

- RHEL 7
- SUSE Linux Enterprise Server 11 und SUSE Linux Enterprise Server 12
- Ubuntu 14.04

- Microsoft Windows 10 Enterprise, Windows Server 2012 und Windows Server 2016. Native Clients unterstützen ausschließlich NFS Version 3.
- Windows 7 Enterprise und Windows Server 2008.

  Native Clients unterstützen ausschließlich NFS Version 3. Die maximal unterstützte Größe von NFS-E/A-Operationen liegt bei 32 KB. Daher kann es unter diesen Windows-Versionen zu Leistungseinbrüchen kommen.

> **Note**
>
> Sie können jetzt SMB-Dateifreigaben verwenden, wenn der Zugriff über Windows (SMB)-Clients anstelle von Windows-NFS-Clients erfolgen muss.

Unterstützte SMB-Clients für ein File Gateway

File Gateways unterstützen die folgenden Service Message Block (SMB)-Clients:

- Microsoft Windows Server 2008 und höher
- Windows Desktop-Versionen: 10, 8 und 7.
- Windows Terminal Server unter Windows Server 2008 und neuer

> **Note**
>
> Für die Verschlüsselung des Server-Nachrichtenblocks sind Clients erforderlich, die SMB v2.1 unterstützen.

Unterstützte Dateisystemoperationen für ein File Gateway

Der NFS- oder SMB-Client kann Dateien schreiben, lesen, löschen und kürzen. Wenn Kunden Schreibvorgänge sendenAWS Storage Gatewayschreibt es synchron in den lokalen Cache. Dann schreibt es unter Verwendung von optimierten Übertragungen synchron in Amazon S3. Lesevorgänge werden zunächst über den lokalen Cache ausgeliefert. Sind dort keine Daten verfügbar, werden sie per Read-Through-Cache aus S3 abgerufen.

Dabei werden sowohl Schreib- als auch Lesevorgänge optimiert: Es werden nur die geänderten oder angeforderten Teile über das Gateway weitergeleitet. Löscht Entfernungsobjekte aus Amazon S3.

Verzeichnisse werden als Ordnerobjekte in S3 verwaltet. Dabei wird dieselbe Syntax verwendet wie in der Amazon S3 S3-Konsole.

HTTP-Operationen wie `GET`, `PUT`, `UPDATE` und `DELETE` können Dateien in einer Dateifreigabe ändern. Diese Operationen entsprechen den atomaren CRUD-Funktionen (Erstellen, Lesen, Aktualisieren, Löschen).

Zugriff auf AWS Storage Gateway

Sie können dasAWS Storage GatewayKonsoleUm verschiedene Gateway-Konfigurations- und -Verwaltungsaufgaben auszuführen. Im Abschnitt „Erste Schritte“ und verschiedenen anderen Abschnitten dieses Handbuchs werden Gateway-Funktionen anhand der Konsole erläutert.

Zudem können Sie mit der AWS Storage Gateway-API Ihre Gateways programmgesteuert konfigurieren und verwalten. Weitere Informationen zur API finden Sie unter API-Referenz für Storage Gateway.

Sie können auch dieAWSSDKs zur Entwicklung von Anwendungen, die mit Storage Gateway interagieren. DieAWSSDKs für Java, .NET und PHP umfassen die zugrunde liegende Storage Gateway Gateway-API, um Ihre Programmieraufgaben zu vereinfachen. Weitere Informationen zum Herunterladen der SDK-Bibliotheken finden Sie unterAWSEntwickler-Centeraus.

Informationen zu Preisen finden Sie unter AWS Storage Gateway-Preise.

Unterstützte AWS-Regionen

- Storage Gateway — Für unterstützteAWSRegionen und eine Liste vonAWSService-Endpoints, die Sie mit Storage Gateway verwenden können, sieheAWS Storage Gateway-Endpunkte und -KontingenteimAWS– Allgemeine Referenzaus.
- Storage Gateway Hardware Appliance — Informationen zu unterstützten Regionen, die Sie mit der Hardware-Appliance verwenden können, finden SieAWS Storage GatewayHardware-Appliance-RegionenimAWS– Allgemeine Referenzaus.

Verwenden der Storage Gateway Hardware Appliance

Bei der Storage Gateway Gateway-Hardware-Appliance handelt es sich um eine physische Hardware-Appliance, bei der die Storage Gateway Gateway-Software auf einer val Sie können Ihre Hardware-Appliance über dieHardware (Hardware)angezeigtenAWS Storage Gatewayconsole.

Bei der Hardware-Appliance handelt es sich um einen hoch leistungsfähigen 1U-Server, den Sie in Ihrem Rechenzentrum oder vor Ort in Ihrer Unternehmens-Firewall bereitstellen können. Wenn Sie Ihre Hardware-Appliance kaufen und aktivieren, wird während des Aktivierungsvorgangs Ihre Hardware-Appliance mit Ihrer verknüpftAWSKonto. Nach der Aktivierung wird Ihre Hardware-Appliance in der Konsole als Gateway auf derHardware (Hardware)angezeigten. Sie können Ihre Hardware-Appliance als File Gateway, Tape Gateway oder Volume Gateway konfigurieren. Das Verfahren, mit dem Sie die diese Gateway-Typen auf einer Hardware-Appliance bereitstellen und aktivieren, ist dasselbe wie auf einer virtuellen Plattform.

Die Storage Gateway Hardware Appliance kann direkt über dieAWS Storage Gatewayconsole.

So bestellen Sie eine Hardware-Appliance

1. Die Storage Gateway Gateway-Konsole unterhttps://console.aws.amazon.com/storagegateway/homeund wähle dasAWSRegion, in der Sie Ihr Appliance haben möchten.
2. Klicken Sie aufHardware (Hardware)Über den Navigationsbereich.
3. Klicken Sie aufBestellen ApplianceKlicken Sie auf und danach aufFortfahrenaus. Sie werden zur weitergeleitetAWSElementar Appliances und Software Management Console, um ein Verkaufsangebot anzufordern.
4. Füllen Sie die notwendigen Informationen aus und wählen SieAbsendenaus.

Sobald die Informationen überprüft wurden, wird ein Verkaufsangebot erstellt, und Sie können mit dem Bestellvorgang fortfahren und eine Bestellung abgeben oder eine Vorauszahlung veranlassen.

So zeigen Sie ein Verkaufsangebot oder eine Bestellhistorie für die Hardware-Appliance an

1. Die Storage Gateway Gateway-Konsole unterhttps://console.aws.amazon.com/storagegateway/homeaus.
2. Klicken Sie aufHardware (Hardware)Über den Navigationsbereich.

3. Klicken Sie aufAngebote und BestellungenKlicken Sie auf und danach aufFortfahrenaus. Sie werden zur weitergeleitetAWSElementar Appliances und Software Management Console zur Überprüfung von Verkaufsangeboten und Bestellhistorie.

In den folgenden Abschnitten finden Sie Anleitungen für die Einrichtung, Konfiguration, das Aktivieren, das Starten und die Verwendung einer Storage Gateway Gateway-Hardware-Appliance.

Themen

Unterstützte AWS-Regionen

Die Storage Gateway Hardware Appliance ist weltweit für den Versand verfügbar, wo sie gesetzlich von der US-Regierung erlaubt und zum Export zugelassen ist. Weitere Informationen zu unterstütztenAWSRegionen sieheRegionen der Storage Gateway Gateway-HardimAWS– Allgemeine Referenzaus.

Einrichten Ihrer Hardware-Appliance

Nachdem Sie Ihre Storage Gateway Hardware Appliance erhalten haben, konfigurieren Sie mithilfe der Hardware-Appliance-Konsole das Netzwerk für die Bereitstellung einer ständigen Verbindung zu konfigurierenAWSund aktiviere dein Gerät. Die Aktivierung verknüpft Ihre Appliance mitAWS-Konto, das während des Aktivierungsvorgangs verwendet wird. Nach der Aktivierung der Appliance können Sie eine Datei, ein Volume oder ein Tape Gateway von der Storage Gateway Gateway-Konsole aus starten.

So installieren und konfigurieren Sie Ihre Hardware-Appliance

1. Mounten Sie die Appliance in einem Rack und schließen Sie Strom- und Netzwerkkabel an. Weitere Informationen finden Sie unter Montieren Sie Ihre Hardware-Appliance im Rack und verbinden Sie sie mit Strom.
2. Legen Sie die IPv4-Adressen für die Hardware-Appliance (den Host) und das Storage Gateway (den Service) fest. Weitere Informationen finden Sie unter Konfigurieren von Netzwerkparametern.
3. Aktivieren Sie die Hardware-Appliance auf der KonsoleHardware (Hardware)angezeigtenAWSRegion Ihrer Wahl. Weitere Informationen finden Sie unter Aktivieren Ihrer Hardware-Appliance.
4. Installieren Sie das Storage Gateway auf Ihrer Hardware-Appliance. Weitere Informationen finden Sie unter Konfigurieren Ihres Gateways.

   Sie richten Gateways auf Ihrer Hardware-Appliance auf die gleiche Weise ein, wie Sie Gateways auf VMware ESXi, Microsoft Hyper-V, Linux Kernel-basierter virtueller Maschine (KVM) oder Amazon EC2 einrichten.

Erweiterung des nutzbaren Cache-Speichers

Sie können den nutzbaren Speicher auf der Hardware-Appliance von 5 TB auf 12 TB erhöhen. Dies bietet einen größeren Cache für den schnellen Zugriff auf die Daten inAWSaus. Wenn Sie das 5-TB-Modell bestellt haben, können Sie den nutzbaren Speicher auf 12 TB erhöhen, indem Sie fünf 1,92-TB-SSDs (Solid State Drives) kaufen, die auf der Konsole bestellt werden könnenHardware (Hardware)angezeigten. Sie können die zusätzlichen SSDs bestellen, indem Sie denselben Bestellvorgang wie die Bestellung einer Hardware-Appliance befolgen und ein Verkaufsangebot von der Storage Gateway Gateway-Konsole anfordern.

Sie können sie dann zur Hardware-Appliance hinzufügen, bevor Sie sie aktivieren. Wenn Sie die Hardware-Appliance bereits aktiviert haben und den nutzbaren Speicher auf der Appliance auf 12 TB erhöhen möchten, gehen Sie wie folgt vor:

1. Setzen Sie die Hardware Appliance auf die Werkseinstellungen zurück. KontaktAWSSupport für Anweisungen hierfür.
2. Fügen Sie der Appliance fünf 1,92-TB-SSDs hinzu.

Optionen für Netzwerkschnittstellenkarten

Je nach Modell der von Ihnen bestellten Appliance kann es mit einer 10G-Base-T Kupfer-Netzwerkkarte oder einer 10G DA/SFP+-Netzwerkkarte geliefert werden.

- 10G-Base-T NIC-Konfiguration:
  - Verwenden Sie CAT6-Kabel für 10G oder CAT5 (e) für 1G
- 10G DA/SFP+NIC-Konfiguration:
  - Verwenden Sie Twinax Copper Direct Attach Kabel bis zu 5 Meter
  - Dell/Intel-kompatible optische SFP+-Module (SR oder LR)
  - SFP/SFP+ Kupfer-Transceiver für 1G-Base-T oder 10G-Base-T

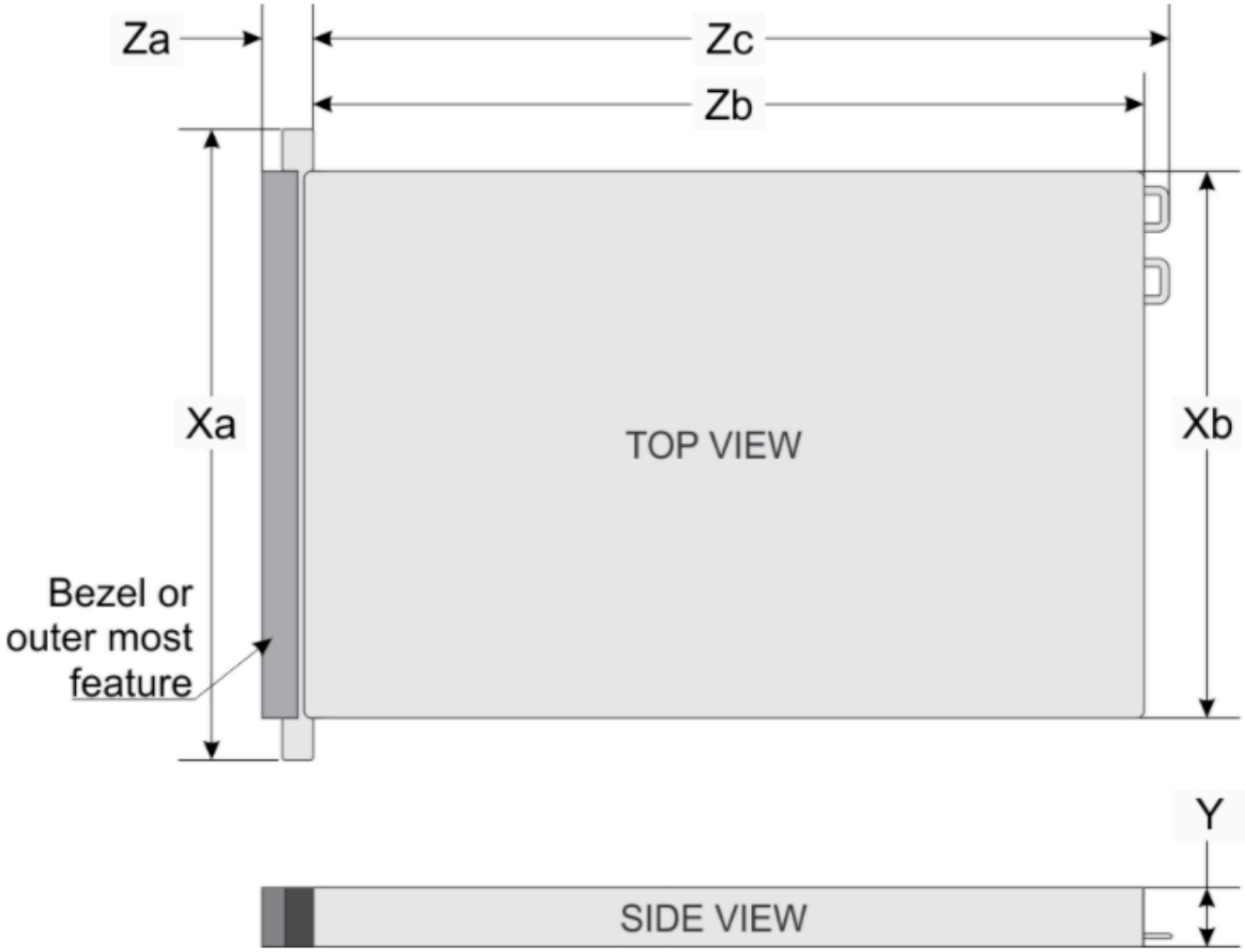
Montieren Sie Ihre Hardware-Appliance im Rack und verbinden Sie sie mit Strom

Folgen Sie nach dem Entpacken Ihrer Storage Gateway Hardware Appliance den im Lieferumfang enthaltenen Anleitungen für das Mounten des Servers im Rack. Bei Ihrer Appliance handelt es sich um einen 1U-Server, der in ein standardmäßiges 19-Zoll-Rack der International Electrotechnical Commission (IEC) konform ist.

Um Ihre Hardware-Appliance zu installieren, benötigen Sie die folgenden Komponenten:

- Stromkabel: Benötigt wird ein Stromkabel. empfohlen werden zwei Stromkabel.
- Unterstützte Netzwerkverkabelung (abhängig davon, welche Netzwerkschnittstellenkarte (NIC) in der Hardware-Appliance enthalten ist). Twinax Copper DAC, optisches SFP+-Modul (Intel-kompatibel) oder SFP zu Base-T Kupfer-Transceiver.
- Tastatur und Monitor oder eine Switch-Lösung mit Tastatur, Anzeige und Maus (Keyboard, Video and Mouse, KVM).

-Hardware-Appliance



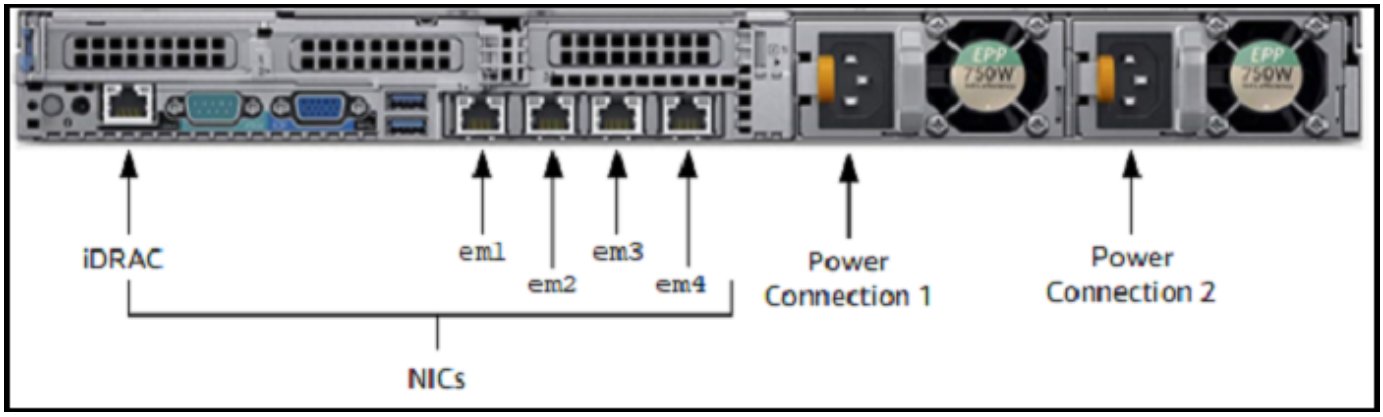
System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

So schließen Sie die Hardware-Appliance an die Stromversorgung an

> **Note**
>
> Stellen Sie vor Ausführung der folgenden Schritte sicher, dass Sie alle Anforderungen für die Storage Gateway Hardware Appliance erfüllen wie in beschriebenNetzwerk- und Firewall-Anforderungen für die Storage Gateway Hardware Applianceaus.

1. Schließen Sie an beide Netzteile ein Stromkabel an. Es ist möglich, nur ein Stromkabel anzuschließen. Es wird jedoch empfohlen, beide Netzteile an die Stromversorgung anzuschließen.

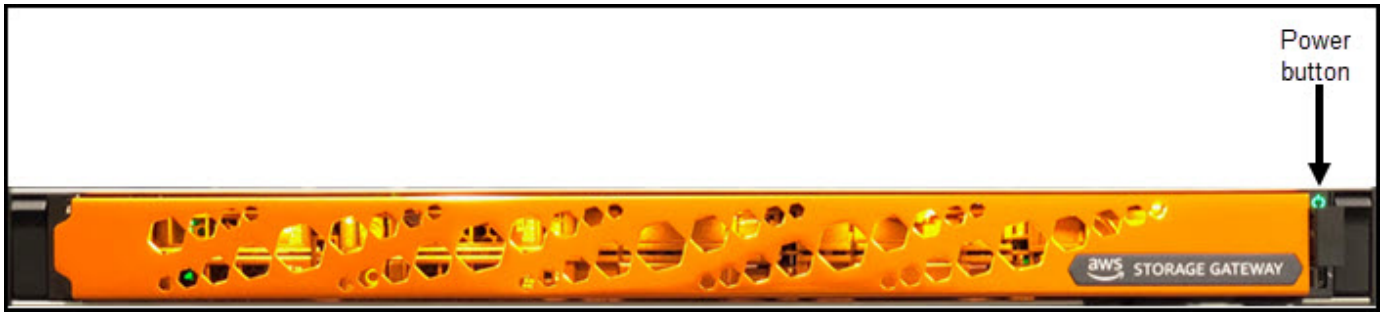
   Im folgenden Bild werden die verschiedenen Anschlüsse der Hardware-Appliance gezeigt.

2. Schließen Sie ein Ethernet-Kabel an den em1-Port an, um eine stets verfügbare Internetverbindung bereitzustellen. Der em1-Port ist der erste der vier physischen Netzwerkports an der Rückseite, von links nach rechts betrachtet.

   > **Note**
   >
   > Die Hardware-Appliance unterstützt kein VLAN-Trunking. Richten Sie den Switch-Port, mit dem Sie die Hardware-Appliance verbinden, als VLAN-Port ohne Trunking ein.

3. Schließen Sie die Tastatur und den Monitor an.
4. Schalten Sie den Server durch Drücken der Taste Power (Ein/Aus) an der Vorderseite ein wie im folgenden Bild gezeigt.



Nach dem Starten des Servers wird die Hardwarekonsole auf dem Monitor angezeigt. Die Hardwarekonsole besitzt eine spezifische BenutzeroberflächeAWSkönnen Sie verwenden, um anfängliche Netzwerkparameter zu konfigurieren. Sie konfigurieren diese Parameter, um die Appliance zu verbindenAWSund öffnen Sie einen Support-Kanal zur Fehlerbehebung durchAWSSupport.

Um mit der Hardwarekonsole zu arbeiten, geben Sie über die Tastatur Text ein und verwenden die Tasten `Up`, `Down`, `Right` und `Left Arrow`, um in der angegebenen Richtung durch den Bildschirm zu navigieren. Durchlaufen Sie die Elemente auf dem Bildschirms der Reihe nach vorwärts mit der Taste `Tab`. In einigen Fällen können Sie mittels der Tastenkombination `Shift+Tab` rückwärts durch Optionen navigieren, eine nach der anderen. Mittels der Taste `Enter` können Sie Ihre Auswahl speichern oder eine Schaltfläche auf dem Bildschirm auswählen.

So legen Sie zum ersten Mal ein Passwort ein

1. Geben Sie in Set Password (Passwort festlegen) ein Passwort ein und drücken Sie anschließend `Down arrow`.
2. Geben Sie das Passwort in Confirm (Bestätigen) erneut ein und wählen Sie dann Save Password (Passwort speichern) aus.

An diesem Punkt befinden Sie sich in der Hardwarekonsole wie im Folgenden gezeigt.

Nächster Schritt

Konfigurieren von Netzwerkparametern

Konfigurieren von Netzwerkparametern

Nach dem Starten des Servers können Sie das erste Passwort in der Hardwarekonsole eingeben wie in Montieren Sie Ihre Hardware-Appliance im Rack und verbinden Sie sie mit Strom beschrieben.

Führen Sie als Nächstes in der Hardwarekonsole die folgenden Schritte aus, um Netzwerkparameter zu konfigurieren, damit Ihre Hardware-Appliance eine Verbindung herstellen kannAWSaus.

So richten Sie eine Netzwerkadresse ein

1. Wählen Sie Configure Network (Netzwerk konfigurieren) aus und drücken Sie die Taste `Enter`. Anschließend wird der im Folgenden gezeigte Bildschirm Configure Network (Netzwerk konfigurieren) angezeigt.

2. Geben Sie in IP address (IP-Adresse) eine gültige IPv4-Adresse aus einer der folgenden Quellen ein:

   - Verwenden Sie die IPv4-Adresse, die Ihrem physischen Netzwerkport von Ihrem Dynamic Host Configuration Protocol (DHCP)-Server zugewiesen wurde.

     Notieren Sie diese IPv4-Adresse, da Sie diese später während des Aktivierungsschritts benötigen werden.

   - Weisen Sie eine statische IPv4-Adresse zu. Wählen Sie hierzu Static (Statisch) im Abschnitt `em1` aus und drücken Sie `Enter`, um den Bildschirm „Configure Static IP (Statische IP-Adresse konfigurieren)“ anzuzeigen wie im Folgenden gezeigt.

     Der Abschnitt `em1` befindet sich oben links in der Gruppe der Porteinstellungen.

   Drücken Sie nach der Eingabe einer gültigen IPv4-Adresse `Down arrow` oder `Tab`.

> **Note**
>
> Wenn Sie eine andere Schnittstelle konfigurieren, muss diese dieselbe stets verfügbare Verbindung zur bereitstellenAWSEndpunkte, die in den Anforderungen aufgeführt sind.

3. Geben Sie in Subnet (Subnetz) eine gültige Subnetzmaske ein und drücken Sie dann `Down arrow`.
4. Geben Sie in Gateway (Gateway) die IPv4-Adresse Ihres Netzwerk-Gateways ein und drücken Sie dann `Down arrow`.
5. Geben Sie in DNS1 die IPv4-Adresse für Ihren Domain Name Service (DNS)-Server ein und drücken Sie dann `Down arrow`.
6. (Optional) Geben Sie in DNS2 eine zweite IPv4-Adresse ein und drücken Sie dann `Down arrow`. Die Zuweisung eines zweiten DNS-Servers sorgt für zusätzliche Redundanz für den Fall, dass der erste DNS-Server nicht mehr verfügbar ist.

7. Wählen Sie Save (Speichern) aus und drücken Sie dann `Enter`, um Ihre Einstellung für eine statische IPv4-Adresse für die Appliance zu speichern.

So melden Sie sich von der Hardwarekonsole ab

1. Wählen Sie Back (Zurück) aus, um zum Hauptbildschirm zurückzukehren.
2. Wählen Sie Logout (Abmelden) aus, um zum Anmeldebildschirm zurückzukehren.

Nächster Schritt

Aktivieren Ihrer Hardware-Appliance

Aktivieren Ihrer Hardware-Appliance

Nach der Konfigurierung der IP-Adresse geben Sie diese IP-Adresse auf der Seite Hardware der Konsole ein wie im Folgenden beschrieben. Während des Aktivierungsvorgangs wird überprüft, ob Ihre Hardware-Appliance die nötigen Sicherheitsanmeldeinformationen besitzt, wird die Appliance bei Ihrer registriertAWSKonto.

Sie können Ihre Hardware-Appliance in jeder der unterstützten aktivierenAWSRegionen. Eine Liste der unterstütztenAWSRegionen siheRegionen der Storage Gateway Gateway-HardimAWS–Allgemeine Referenzaus.

So aktivieren Sie Ihre Appliance zum ersten Mal oder in einemAWSRegion, in der Sie keine Gateways bereitgestellt haben

1. Melden Sie sich beim anAWS Management Consoleund öffnen Sie die Storage Gateway Gateway-Konsole unterAWS Storage Gateway-Managementkonsolemit den Kontoanmeldeinformationen, die für die Aktivierung Ihrer Hardware verwendet werden.

   Wenn dies Ihr erstes Gateway in einemAWSRegion sehen Sie einen Begrüßungsbildschirm. Nachdem Sie in diesem ein Gateway erstellt habenAWSRegion wird der Bildschirm nicht mehr angezeigt.

   > **Note**
   >
   > Die folgenden Anforderungen müssen erfüllt sein, um die Hardware-Appliance aktivieren zu können:

- Ihr Browser muss sich im selben Netzwerk wie Ihre Hardware-Appliance befinden.
- Ihre Firewall muss eingehenden HTTP-Datenverkehr zur Appliance auf Port 8080 zulassen.

2. Wählen Sie Get started (Erste Schritte) aus, um den Assistenten für die Erstellung von Gateways anzuzeigen. Wählen Sie anschließend auf der Seite Select host platform (Host-Plattform auswählen) die Option Hardware Appliance (Hardware-Appliance) aus wie im Folgenden gezeigt.
3. Wählen Sie Next (Weiter) aus, um den Bildschirm Connect to hardware (Mit Hardware verbinden) anzuzeigen wie im Folgenden gezeigt.
4. FürIP-AdresseimMit Hardware-Appliance Connectgeben Sie die IPv4-Adresse Ihrer Appliance ein.VerbindenUm zum Bildschirm Hardware aktivieren zu wechseln wie im Folgenden gezeigt.
5. Geben Sie in Hardware name (Name der Hardware) einen Namen für Ihre Appliance ein. Namen können bis zu 255 Zeichen enthalten. Sie dürfen keinen Schrägstrich enthalten.
6. FürHardware-ZeitzoneGeben Sie Ihre lokalen Einstellungen ein.

   Die Zeitzone legt fest, wann Hardware-Updates ausgeführt werden. Updates werden um 2 Uhr morgens lokaler Zeit ausgeführt.

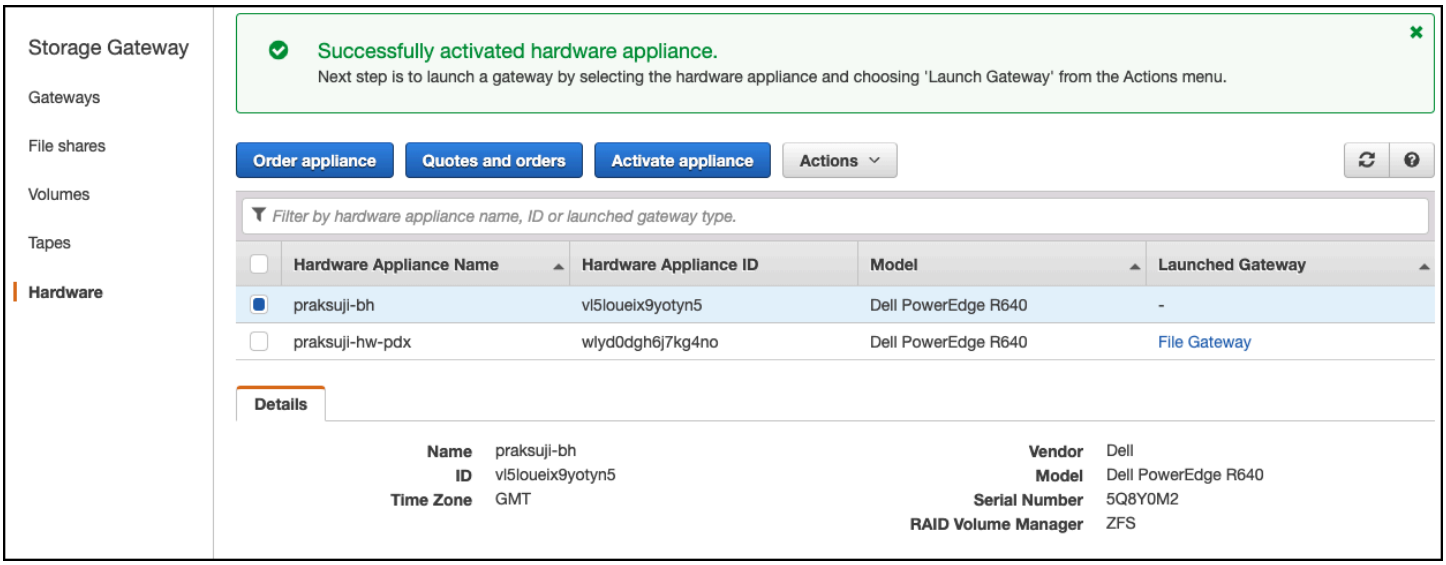
   > **Note**
   >
   > Die Einrichtung einer Zeitzone für Ihre Appliance wird empfohlen, da hierdurch ein Standardzeitpunkt für Updates festgelegt wird, der außerhalb der normalen Arbeitszeiten liegt.

7. (Optional) Behalten Sie die Festlegung von RAID Volume Manager (RAID-Volume-Manager) als ZFS (ZFS) bei.

   ZFS wird als RAID-Volume-Manager auf der Hardware-Appliance verwendet, um eine bessere Leistung und einen besseren Datenschutz zu bieten. ZFS ist ein softwarebasiertes Open-Source-Dateisystem und ein logischer, optischer, offener Dateis Die Hardware-Appliance ist spezifisch auf ZFS RAID ausgelegt. Weitere Informationen zu ZFS RAID finden Sie auf der Wikipedia-Seite für ZFS.
8. Wählen Sie Next (Weiter) aus, um die Aktivierung zu beenden.

Anschließend wird auf der Seite Hardware ein Konsolenbanner angezeigt, das die erfolgreiche Aktivierung der Hardware-Appliance bestätigt wie im Folgenden gezeigt.

An diesem Punkt ist die Appliance mit Ihrem Konto verknüpft. Der nächste Schritt besteht im Starten eines Datei-, Band- oder Cached-Volume-Gateways auf Ihrer Appliance.



Nächster Schritt

Starten eines Gateways

Starten eines Gateways

Sie können jedes der drei Speicher-Gateways auf der Appliance starten - File-Gateway, Volume Gateway (zwischengespeichert) oder Band-Gateway.

So starten Sie einen Gateway auf Ihrer Hardware-Appliance

1. Melden Sie sich beim anAWS Management Consoleund öffnen Sie die Storage Gateway Gateway-Konsole unterhttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie Hardware (Hardware) aus.
3. Wählen Sie in Actions (Aktionen) die Option Launch Gateway (Gateway starten) aus.
4. Wählen Sie in Gateway Type (Gateway-Typ) File Gateway (Datei-Gateway), Tape Gateway (Band-Gateway) oder Volume Gateway ((Cached-)Volume-Gateway) aus.
5. Geben Sie in Gateway name (Gateway-Name) einen Namen für Ihren Gateway ein. Namen können 255 Zeichen enthalten. Sie dürfen keinen Schrägstrich enthalten.
6. Wählen Sie Launch Gateway (Gateway starten) aus.

Die Storage Gateway Gateway-Software für den von Ihnen gewählten Gateway-Typ wird auf der Appliance installiert. Es kann 5 bis 10 Minuten dauern, bis ein Gateway als angezeigt wirdonlinein der Konsole.

Um dem installierten Gateway eine statische IP-Adresse zuzuweisen, konfigurieren Sie als Nächstes die Netzwerkschnittstellen des Gateways, damit Ihre Anwendungen diesen verwenden können.

Nächster Schritt

Konfigurieren einer IP-Adresse für das Gateway

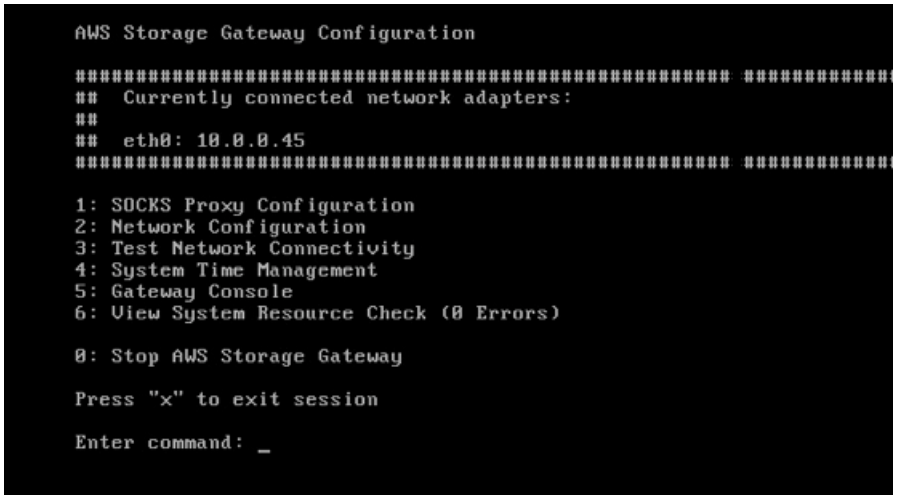
Konfigurieren einer IP-Adresse für das Gateway

Bevor Sie Ihre Hardware-Appliance aktiviert haben, haben Sie ihrer physischen Netzwerkschnittstelle eine IP-Adresse zugewiesen. Nachdem Sie die Appliance aktiviert und Ihr Storage Gateway darauf gestartet haben, müssen Sie der virtuellen Storage Gateway Gateway-Maschine, die auf der Hardware-Appliance ausgeführt wird, eine andere IP-Adresse zuweisen. Um einem auf Ihrer Hardware-Appliance installierten Gateway eine statische IP-Adresse zuzuweisen, konfigurieren Sie die IP-Adresse auf der lokalen Konsole für dieses Gateway. Ihre Anwendungen (wie Ihr NFS- oder SMB-Client, Ihr iSCSI-Initiator usw.) stellen Verbindungen mit dieser IP-Adresse her. Sie können über die Konsole der Hardware-Appliance auf die lokale Konsole des Gateways zugreifen.

So konfigurieren Sie eine IP-Adresse auf Ihrer Appliance, damit Ihre Anwendungen diese verwenden können

1. Wählen Sie auf der Hardwarekonsole Open Service Console (Service-Konsole öffnen) aus, um einen Anmeldebildschirm für die lokale Konsole des Gateways zu öffnen.
2. Geben Sie das localhost-Passwort in Login (Anmeldung) ein und drücken Sie anschließend `Enter`.

   Das Standardkonto ist `admin` und das Standardpasswort ist `password`.
3. Ändern Sie das Standardpasswort. Wählen Sie Actions (Aktionen) und dann Set Local Password (Lokales Passwort festlegen) aus. Geben Sie dann die neuen Anmeldeinformationen in das Dialogfeld Set Local Password (Lokales Passwort festlegen) ein.
4. (Optional) Konfigurieren Sie die Proxyeinstellungen. Detaillierte Anweisungen finden Sie unter Montieren Sie Ihre Hardware-Appliance im Rack und verbinden Sie sie mit Strom.
5. Navigieren Sie zur Seite „Network Settings (Netzwerkeinstellungen)“ der lokalen Konsole des Gateways wie im Folgenden gezeigt.



6. Geben Sie 2 ein, um zur Seite Network Configuration (Netzwerkkonfiguration) zu wechseln wie im Folgenden gezeigt.

7. Konfigurieren Sie eine statische oder DHCP-IP-Adresse für den Netzwerkport auf Ihrer Hardware-Appliance, um Anwendungen einen Datei-, Volume- und Band-Gateway bereitzustellen. Diese IP-Adresse muss sich im selben Subnetz wie die IP-Adresse befinden, die während der Aktivierung der Hardware-Appliance verwendet wurde.

So verlassen Sie die lokale Konsole des Gateways

- Drücken Sie die Tastenkombination `Crtl+]` (schließende Klammer). Anschließend wird die Hardwarekonsole angezeigt.

> **Note**
>
> Die eben angegebene Tastenkombination stellt die einzige Möglichkeit dar, wie Sie die lokale Konsole des Gateways verlassen können.

Nächster Schritt

Konfigurieren Ihres Gateways

Konfigurieren Ihres Gateways

Mach der Aktivierung und Konfigurierung Ihrer Hardware-Appliance wird Ihre Appliance in der Konsole angezeigt. Nun können Sie den gewünschten Gateway-Typ konfigurieren. Sie setzen die Installation Ihres Gateway-Typs fort. Anweisungen finden Sie unter Konfigurieren Sie Ihr Amazon S3 File Gateway.

Entfernen eines Gateways von der Hardware-Appliance

Um Gateway-Software von Ihrer Hardware-Appliance zu entfernen, führen Sie die folgenden Schritte aus. Anschließend ist die Gateway-Software nicht länger auf Ihrer Hardware-Appliance installiert.

So entfernen Sie einen Gateway von einer Hardware-Appliance

1. Wählen Sie das Kontrollkästchen für das Gateway.
2. Wählen Sie für Actions (Aktionen) die Option Remove Gateway (Gateway entfernen).
3. Wählen Sie im Dialogfeld Remove gateway from hardware appliance (Gateway von Hardware-Appliance entfernen) Confirm (Bestätigen).

> **Note**
>
> Wenn Sie ein Gateway löschen, können Sie die Aktion nicht rückgängig machen. Bei bestimmten Gateway-Typen können Daten beim Löschen verlorengehen, insbesondere zwischengespeicherte Daten. Weitere Informationen zum Löschen eines Gateways finden Sie unter Löschen des Gateways über die AWS Storage Gateway-Konsole und Bereinigen zugehöriger Ressourcen.

Durch das Löschen eines Gateways wird nicht die Hardware-Appliance von der Konsole gelöscht. Die Hardware-Appliance bleibt für zukünftige Gateway-Bereitstellungen erhalten.

Löschen Ihrer Hardware-Appliance

Nachdem Sie Ihre Hardware-Appliance in IhremAWSkönnen Sie es in einem anderen verschieben und aktivieren.AWSKonto. In diesem Fall müssen Sie zuerst die Appliance imAWSAccount und aktiviere es in einem anderenAWSKonto. Möglicherweise möchten Sie auch die Appliance vollständig aus Ihrer löschenAWS-Konto, weil Sie es nicht mehr benötigen. Befolgen Sie die folgenden Anweisungen zum Löschen Ihrer Hardware-Appliance.

So löschen Sie Ihre Hardware-Appliance

1. Wenn Sie ein Gateway auf der Hardware-Appliance installiert haben, müssen Sie zunächst das Gateway entfernen, bevor Sie die Appliance löschen können. Anweisungen zum Entfernen eines Gateways von der Hardware-Appliance finden Sie unterEntfernen eines Gateways von der Hardware-Applianceaus.
2. Wählen Sie auf der Hardware-Seite die Hardware-Appliance aus, die Sie löschen möchten.
3. Wählen Sie für Actions (Aktionen) die Option Delete Appliance (Appliance löschen) aus.
4. Wählen Sie im Dialogfeld Confirm deletion of resource(s) (Löschen von Ressource(n) bestätigen) das Kontrollkästchen zur Bestätigung aus, und klicken Sie anschließend auf Delete (Löschen). Es wird eine Meldung zur Bestätigung der erfolgreichen Löschung angezeigt.

   Wenn Sie die Hardware-Appliance löschen, werden alle Ressourcen im Zusammenhang mit dem Gateway, das auf der Appliance installiert ist, ebenfalls gelöscht, jedoch nicht die Daten auf der Hardware-Appliance.

Erste Schritte mit AWS Storage Gateway

In diesem Abschnitt finden Sie Anweisungen zum Erstellen und Aktivieren eines File GatewaysAWS Storage Gatewayaus. Bevor Sie beginnen, stellen Sie sicher, dass Ihr Setup die erforderlichen Voraussetzungen und andere Anforderungen erfüllt, die unterEinrichten für Amazon S3 File Gatewayaus.

Themen

- Erstellen und aktivieren Sie ein Amazon S3 File Gateway

Erstellen und aktivieren Sie ein Amazon S3 File Gateway

In diesem Abschnitt finden Sie Anweisungen zum Erstellen, Bereitstellen und Aktivieren eines File GatewaysAWS Storage Gatewayaus.

Themen

- So richten Sie ein Amazon S3 S3-Datei-Gateway ein
- Connect Sie Ihr Amazon S3 File Gateway mitAWS
- Überprüfen Sie die Einstellungen und aktivieren Sie Ihr Amazon S3 File Gateway
- Konfigurieren Sie Ihr Amazon S3 File Gateway

So richten Sie ein Amazon S3 S3-Datei-Gateway ein

So richten Sie ein neues S3 File Gateway ein

1. Öffnen SieAWS Management Consolebeimhttps://console.aws.amazon.com/storagegateway/home/, und wählen Sie dasAWS-Regionwo Sie Ihr Gateway erstellen möchten.
2. Klicken Sie aufCreate gatewaySo öffnen Sie denEinrichten eines Gatewaysangezeigten.
3. In derGateway Einstellungenwie folgt:

    a. Geben Sie in Gateway name (Gateway-Name) einen Namen für Ihren Gateway ein. Nachdem Ihr Gateway erstellt wurde, können Sie nach diesem Namen suchen, um Ihr Gateway auf den Listenseiten imAWS Storage Gatewayconsole.

    b. FürGateway-Zeitzone, wählen Sie die lokale Zeitzone für den Teil der Welt aus, in dem Sie Ihr Gateway bereitstellen möchten.

4. In derGateways OptionenAbschnitts fürGateway-Typ, wählenAmazon S3 S3-Datei-Gatewayaus.
5. In derOptionen für die Plattformwie folgt:

   a. FürHost-Plattformwählen Sie die Plattform aus, auf der Sie Ihr Gateway bereitstellen möchten. Folgen Sie dann den plattformspezifischen Anweisungen auf der Storage Gateway Gateway-Konsolenseite, um Ihre Host-Plattform einzurichten. Sie können aus den folgenden Optionen auswählen:

      - VMware ESXi— Laden Sie die virtuelle Gateway-Maschine mit VMware ESXi herunter, stellen Sie sie bereit und konfigurieren Sie sie.
      - Microsoft Hyper-V— Laden Sie die virtuelle Gateway-Maschine mit Microsoft Hyper-V herunter, stellen Sie sie bereit und konfigurieren Sie sie.
      - Linux-KVM— Laden Sie die virtuelle Maschine des Gateways herunter, stellen Sie sie bereit und konfigurieren Sie sie mit Linux Kernel-basierten virtuellen Maschine (KVM).
      - Amazon EC2— Konfigurieren und starten Sie eine Amazon EC2 EC2-Instance zum Hosten Ihres Gateways.
      - Hardware-Appliance- Bestellen Sie eine dedizierte physische HardwareAWSHosten Ihres Gateways.

   b. FürBestätigen Sie einrichten Gateway, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Bereitstellungsschritte für die von Ihnen gewählte Host-Plattform ausgeführt haben. Dieser Schritt gilt nicht für dieHardware-ApplianceHost-Plattform.
6. Nachdem Ihr Gateway eingerichtet ist, müssen Sie wählen, wie es eine Verbindung herstellen und kommunizieren sollAWSaus. Klicken Sie aufWeiterSo fahren Sie mit.

Connect Sie Ihr Amazon S3 File Gateway mitAWS

So verbinden Sie ein neues S3 File Gateway mitAWS

1. Wenn Sie dies noch nicht getan haben, führen Sie das unterSo richten Sie ein Amazon S3 S3-Datei-Gateway einaus. Wenn Sie fertig sind, wählen SieWeiterSo öffnen Sie denVerbinden mitAWSangezeigter imAWS Storage Gatewayconsole.
2. In derEndpunkt-OptionenAbschnitts fürService-Endpunktwählen Sie den Endpunkttyp aus, mit dem Ihr Gateway verwendet, mit dem Ihr Gateway kommunizieren sollAWSaus. Sie können aus den folgenden Optionen auswählen:

- Publicly accessible (Öffentlich zugänglich)— Ihr Gateway kommuniziert mitAWSüber das öffentliche Internet. Wenn Sie diese Option auswählen, verwenden Sie dieFIPS-aktivierter Endpunkt-Kontrollkästchen, um anzugeben, ob die Verbindung Federal Information Processing Standards (FIPS) erfüllen muss.

  > **Note**
  >
  > Wenn Sie für den Zugriff auf FIPS 140-2 validierte kryptografische Module benötigenAWSVerwenden Sie über eine Befehlszeilenschnittstelle oder eine API einen FIPS-konformen Endpunkt. Weitere Informationen finden Sie unter Federal Information Processing Standard (FIPS) 140-2.
  > Der FIPS-Service-Endpunkt ist nur in einigen verfügbarAWSRegionen. Weitere Informationen finden Sie unterAWS Storage Gateway-Endpunkte und -KontingenteimAWS– Allgemeine Referenzaus.

- VPC gehostet— Ihr Gateway kommuniziert mitAWSüber eine private Verbindung mit Ihrer Virtual Private Cloud (VPC), mit der Sie Ihre Netzwerkeinstellungen steuern können. Wenn Sie diese Option auswählen, müssen Sie einen vorhandenen VPC-Endpunkt angeben, indem Sie die VPC-Endpunkt-ID aus der Dropdown-Liste auswählen. Sie können auch den DNS-Namen oder die IP-Adresse des VPC-Endpunkts (Domain Name System) angeben.

3. In derVerbindungsoptionenAbschnitts fürVerbindungsoptionen, wählen Sie, wie Sie Ihr Gateway zu identifizierenAWSaus. Sie können aus den folgenden Optionen auswählen:

   - IP-Adresse— Geben Sie die IP-Adresse Ihres Gateways in das entsprechende Feld ein. Diese IP-Adresse muss öffentlich oder von Ihrem aktuellen Netzwerk aus zugänglich sein und Sie müssen in der Lage sein, über Ihren Webbrowser eine Verbindung zu ihr herzustellen.

     Sie können die Gateway-IP-Adresse abrufen, indem Sie sich von Ihrem Hypervisor-Client bei der lokalen Konsole des Gateways anmelden oder sie von der Detailseite Ihrer Amazon EC2 EC2-Instance kopieren.

   - Aktivierungsschlüssel— Geben Sie den Aktivierungsschlüssel für das Gateway in das entsprechende Feld ein. Sie können mit der lokalen Konsole des Gateways einen Aktivierungsschlüssel generieren. Wenn die IP-Adresse Ihres Gateways nicht verfügbar ist, wählen Sie diese Option.

4. Nachdem Sie sich entschieden haben, wie Ihr Gateway eine Verbindung herstellen sollAWS, müssen Sie das Gateway aktivieren. Klicken Sie aufWeiterSo fahren Sie mit.

Überprüfen Sie die Einstellungen und aktivieren Sie Ihr Amazon S3 File Gateway

So aktivieren Sie ein neues S3 File Gateway

1. Wenn Sie dies noch nicht getan haben, führen Sie die in den folgenden Themen beschriebenen Verfahren aus:

   - So richten Sie ein Amazon S3 S3-Datei-Gateway ein
   - Connect Sie Ihr Amazon S3 File Gateway mitAWS

   Wenn Sie fertig sind, wählen SieWeiterSo öffnen Sie denPrüfen und aktivierenangezeigter imAWS Storage Gatewayconsole.
2. Überprüfen Sie die ersten Gateway-Details für jeden Abschnitt auf der Seite.
3. Wenn ein Abschnitt Fehler enthält, wählen SieBearbeitenum zur entsprechenden Einstellungsseite zurückzukehren und Änderungen vorzunehmen.

   > **Important**
   >
   > Sie können die Gateway-Optionen oder Verbindungseinstellungen nicht ändern, nachdem Ihr Gateway aktiviert wurde.
4. Nachdem Sie Ihr Gateway aktiviert haben, müssen Sie die Erstkonfiguration durchführen, um lokale Speicherfestplatten zuzuweisen und die Protokollierung zu konfigurieren. Klicken Sie aufWeiterSo fahren Sie mit.

Konfigurieren Sie Ihr Amazon S3 File Gateway

So führen Sie die Erstkonfiguration auf einem neuen S3 File Gateway durch

1. Wenn Sie dies noch nicht getan haben, führen Sie die in den folgenden Themen beschriebenen Verfahren aus:

   - So richten Sie ein Amazon S3 S3-Datei-Gateway ein
   - Connect Sie Ihr Amazon S3 File Gateway mitAWS
   - Überprüfen Sie die Einstellungen und aktivieren Sie Ihr Amazon S3 File Gateway

Wenn Sie fertig sind, wählen SieWeiterSo öffnen Sie denKonfigurieren des Gangezeigter imAWS Storage Gatewayconsole.

2. In derKonfigurieren des Cache-verwenden Sie die Dropdown-Listen, um mindestens eine lokale Festplatte mit mindestens 150 Gibibyte (GiB) Kapazität zuzuweisenCacheaus. Die in diesem Abschnitt aufgeführten lokalen Festplatten entsprechen dem physischen Speicher, den Sie auf Ihrer Host-Plattform bereitgestellt haben.
3. In derCloudWatch-Protokollgruppewählen Sie aus, wie Amazon CloudWatch Logs eingerichtet werden soll, um den Zustand Ihres Gateways zu überwachen. Sie können aus den folgenden Optionen auswählen:

   - Eine neue Protokollgruppe erstellen— Rufen Sie eine neue Protokollgruppe ein, um Ihr Gateway zu überwachen.
   - Verwenden einer vorhandenen Protokollgruppe— Wählen Sie eine vorhandene Protokollgruppe aus der entsprechenden Dropdown-Liste aus.
   - Protokollierung deaktivieren— Verwenden Sie Amazon CloudWatch Logs nicht, um Ihr Gateway zu überwachen.
4. In derCloudWatch-Alarmewählen Sie aus, wie Amazon CloudWatch CloudWatch-Alarme eingerichtet werden sollen, um Sie zu benachrichtigen, wenn die Metriken Ihres Gateways von definierten Grenzwerten abweichen. Sie können aus den folgenden Optionen auswählen:

   - Alarme deaktivieren— Verwenden Sie keine CloudWatch-Alarme, um über die Metriken Ihres Gateways informiert zu werden.
   - Erstellen eines benutzerdefinierten CloudWatch-Alarms— Konfigurieren Sie einen neuen CloudWatch-Alarm, der über die Metriken Ihres Gateways informiert wird. Klicken Sie aufAlarm erstellenzum Definieren von Metriken und zur Festlegung von Alarmaktionen in der Amazon CloudWatch CloudWatch-Konsole. Detaillierte Anweisungen finden Sie unterVerwenden von Amazon CloudWatch CloudWatch-AlarmenimAmazon CloudWatch-Benutzerhandbuchaus.
5. (Optional) ImTags-Abschnitt auswählen, wählen SieNeues Tag hinzufügenund geben Sie ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung ein, das Ihnen das Suchen und Filtern Ihres Gateways erleichtert.AWS Storage Gatewayconsole. Wiederholen Sie diesen Schritt, um so viele Tags hinzuzufügen, wie Sie benötigen.
6. (Optional) ImÜberprüfen der Konfiguration von VMware High AvailabilityWenn Ihr Gateway auf einem VMware-Host als Teil eines Clusters bereitgestellt wird, der für VMware High Availability

(HA) aktiviert ist, wählen SieÜberprüfen von VMware HAum zu testen, ob die HA-Konfiguration ordnungsgemäß funktioniert.

> **Note**
>
> Dieser Abschnitt wird nur für Gateways angezeigt, die auf der VMware-Hostplattform ausgeführt werden.
> Dieser Schritt ist nicht erforderlich, um den Gateway-Konfigurationsprozess abzuschließen. Sie können die HA-Konfiguration Ihres Gateways jederzeit testen. Die Überprüfung dauert einige Minuten und startet die virtuelle Maschine (VM) von Storage Gateway neu.

7. Klicken Sie aufKonfigurationUm die Erstellung Ihres Gateways abzuschließen.

   Um den Status Ihres neuen Gateways zu überprüfen, suchen Sie danach auf der-Gatewaysangezeigter derAWS Storage Gatewayconsole.

Nachdem Sie das Gateway erstellt haben, müssen Sie eine Dateifreigabe erstellen, die es verwenden kann. Detaillierte Anweisungen finden Sie unterErstellen Sie eine Dateifreigabeaus.

Erstellen Sie eine Dateifreigabe

Im diesem Abschnitt finden Sie eine Anleitung zur Erstellung einer Dateifreigabe. Sie können eine Dateifreigabe erstellen, auf die unter Verwendung des NFS (Network File System)- oder SMB (Server Message Block)-Protokolls zugegriffen werden kann.

> **Note**
>
> Wenn eine Datei von einem NFS- oder SMB-Client in das Datei-Gateway geschrieben wird, lädt das Datei-Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von seinen Metadaten (Eigentümerschaften, Zeitstempel usw.). Durch das Hochladen der Dateidaten wird ein S3-Objekt erstellt, und das Hochladen der Metadaten für die Datei aktualisiert die Metadaten für das S3-Objekt. Dieser Prozess erstellt eine andere Version des Objekts, was zu zwei Versionen eines Objekts führt. Wenn die S3-Versioning aktiviert ist, werden beide Versionen gespeichert.
> Wenn Sie die Metadaten einer in Ihrem Datei-Gateway gespeicherten Datei ändern, wird ein neues S3-Objekt erstellt und ersetzt das vorhandene S3-Objekt. Dieses Verhalten unterscheidet sich vom Bearbeiten einer Datei in einem Dateisystem, wobei das Bearbeiten einer Datei nicht dazu führt, dass eine neue Datei erstellt wird. Testen Sie alle Dateioperationen, mit denen Sie verwenden möchtenAWSStorage Gateway, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.
> Berücksichtigen Sie sorgfältig die Verwendung von S3-Versionierung und regionsübergreifender Replikation (CRR) in Amazon S3, wenn Sie Daten von Ihrem Datei-Gateway hochladen. Das Hochladen von Dateien von Ihrem Datei-Gateway auf Amazon S3 bei aktivierter S3-Versionierung führt zu mindestens zwei Versionen eines S3-Objekts. Bestimmte Workflows mit großen Dateien und Dateischreibmustern wie Datei-Uploads, die in mehreren Schritten ausgeführt werden, können die Anzahl der gespeicherten S3-Objektversionen erhöhen. Wenn der Datei-Gateway-Cache aufgrund hoher Dateischreibraten Speicherplatz freigeben muss, werden möglicherweise mehrere S3-Objektversionen erstellt. Diese Szenarien erhöhen den S3-Speicher, wenn die S3-Versionierung aktiviert ist, und erhöhen die mit CRR verbundenen Transferkosten. Testen Sie alle Dateioperationen, die Sie mit Storage Gateway verwenden möchten, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.
> Die Verwendung des Rsync-Dienstprogramms mit Ihrem Datei-Gateway führt zur Erstellung temporärer Dateien im Cache und zur Erstellung temporärer S3-Objekte in Amazon S3. Diese

Situation führt zu frühen Löschgebühren in den Speicherklassen S3 Standard-Infrequent Access (S3 Standard-IA) und S3 Intelligent-Tiering.

Wenn Sie eine NFS-Freigabe erstellen, kann standardmäßig jeder, der Zugriff auf den NFS-Server hat, auf die NFS-Dateifreigabe zugreifen. Sie können den Zugriff auf Clients über die IP-Adresse einschränken.

Für SMB können Sie eine von drei verschiedenen Authentifizierungsarten verwenden:

- Eine Dateifreigabe mit Microsoft Active Directory (AD)-Zugriff. Jeder authentifizierte Microsoft AD-Benutzer erhält Zugriff auf diesen Dateifreigabetyp.
- Eine SMB-Dateifreigabe mit eingeschränktem Zugriff. Nur bestimmte Domänenbenutzer und -gruppen, die Sie angeben, dürfen darauf zugreifen (über eine Zulassungsliste). Benutzern und Gruppen kann der Zugriff auch verweigert werden (durch eine Verweigerungsliste).
- Eine SMB-Dateifreigabe mit Gastzugriff. Alle Benutzer, die das Gast-Passwort angeben können, erhalten Zugriff auf diese Dateifreigabe.

> **Note**
>
> Dateifreigaben, die über das Gateway für NFS-Dateifreigaben exportiert wurden, unterstützen POSIX-Berechtigungen. Für SMB-Dateifreigaben können Sie Zugriffskontrolllisten (Access Control Lists, ACLs) zum Verwalten von Berechtigungen für Dateien und Ordner in Ihrer Dateifreigabe verwenden. Weitere Informationen finden Sie unter Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe.

Ein File Gateway kann eine oder mehrere Dateifreigaben unterschiedlicher Typen hosten. Sie können mehrere NFS- und SMB-Dateifreigaben auf einem Datei-Gateway haben.

> **Important**
>
> Um eine Dateifreigabe für ein File Gateway zu erstellen, müssen Sie AWS Security Token Service (AWS STS) aktivieren. Stellen Sie Folgendes sicherAWS STSist imAWS-RegionIn dem Sie Ihr File Gateway erstellen möchten. WennAWS STSist darin nicht aktiviertAWS-Region, aktiviere es. Weitere Informationen zur AktivierungAWS STSfinden Sie

unter,Aktivieren und DeaktivierenAWS STSin einemAWS-RegionimAWS Identity and Access Management-Benutzerhandbuchaus.

> **Note**
>
> Sie können verwenden.AWS Key Management Service(AWS KMS) um Objekte zu verschlüsseln, die Ihr File Gateway in Amazon S3 speichert. Informationen dazu, wie Sie dies mithilfe der Storage Gateway Gateway-Konsole tun,Erstellen Sie eine NFS-DateifreigabeoderErstellen Sie eine SMB-Dateifreigabeaus. Sie können dies mithilfe der Storage Gateway -API tun. Detaillierte Anweisungen finden Sie unterCreateNFSFileShareoderCreateSmbFileShareimAWSStorage Gateway Gateway-APIaus.
>
> Standardmäßig verwendet ein Datei-Gateway eine serverseitige Verschlüsselung, die mit Amazon S3 (SSE-S3) verwaltet wird, wenn es Daten in einen S3-Bucket schreibt. Wenn Sie SSE-KMS (serverseitige Verschlüsselung mitAWS KMS— verwaltete Schlüssel) Die Standardverschlüsselung für Ihren S3-Bucket, werden Objekte, die ein Datei-Gateway dort speichert, mit SSE-KMS verschlüsselt.
>
> Um SSE-KMS mit Ihrem eigenen AWS KMS-Schlüssel zu verschlüsseln, müssen Sie die SSE-KMS-Verschlüsselung aktivieren. Dabei geben Sie den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels an, wenn Sie Ihre Dateifreigabe erstellen. Sie können die KMS-Einstellungen für Ihre Dateifreigabe auch mithilfe der API-Operation UpdateNFSFileShare oder UpdateSMBFileShare aktualisieren. Diese Aktualisierung gilt für Objekte, die nach der Aktualisierung in den Amazon S3 S3-Buckets gespeichert sind.
>
> Wenn Sie Ihr Datei-Gateway für die Verwendung von SSE-KMS für die Verschlüsselung konfigurieren, müssen Sie manuell hinzufügen`kms:Encrypt`,`kms:Decrypt`,`kms:ReEncrypt`,`kms:GenerateDataKey`, und`kms:DescribeKey`Berechtigungen für die IAM-Rolle, die der Dateifreigabe zugeordnet ist. Weitere Informationen finden Sie unterVerwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für Storage Gatewayaus.

Themen

- Erstellen Sie eine NFS-Dateifreigabe
- Erstellen Sie eine SMB-Dateifreigabe

Erstellen Sie eine NFS-Dateifreigabe

Führen Sie die folgenden Schritte durch, um eine Network File System (NFS) -Dateifreigabe zu erstellen.

> **Note**
>
> Wenn eine Datei von einem NFS-Client in das Datei-Gateway geschrieben wird, lädt das Datei-Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von seinen Metadaten (Eigentümer, Zeitstempel usw.). Durch das Hochladen der Dateidaten wird ein S3-Objekt erstellt, und das Hochladen der Metadaten für die Datei aktualisiert die Metadaten für das S3-Objekt. Dieser Prozess erstellt eine andere Version des Objekts, was zu zwei Versionen eines Objekts führt. Wenn die S3-Versioning aktiviert ist, werden beide Versionen gespeichert.
>
> Wenn Sie die Metadaten einer in Ihrem Datei-Gateway gespeicherten Datei ändern, wird ein neues S3-Objekt erstellt und ersetzt das vorhandene S3-Objekt. Dieses Verhalten unterscheidet sich vom Bearbeiten einer Datei in einem Dateisystem, wobei das Bearbeiten einer Datei nicht dazu führt, dass eine neue Datei erstellt wird. Testen Sie alle Dateioperationen, mit denen Sie verwenden möchtenAWSStorage Gateway, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.
>
> Berücksichtigen Sie sorgfältig die Verwendung von S3-Versionierung und regionsübergreifender Replikation (CRR) in Amazon S3, wenn Sie Daten von Ihrem Datei-Gateway hochladen. Das Hochladen von Dateien von Ihrem Datei-Gateway auf Amazon S3 bei aktivierter S3-Versionierung führt zu mindestens zwei Versionen eines S3-Objekts. Bestimmte Workflows mit großen Dateien und Dateischreibmustern wie Datei-Uploads, die in mehreren Schritten ausgeführt werden, können die Anzahl der gespeicherten S3-Objektversionen erhöhen. Wenn der Datei-Gateway-Cache aufgrund hoher Dateischreibraten Speicherplatz freigeben muss, werden möglicherweise mehrere S3-Objektversionen erstellt. Diese Szenarien erhöhen den S3-Speicher, wenn die S3-Versionierung aktiviert ist, und erhöhen die mit CRR verbundenen Transferkosten. Testen Sie alle Dateioperationen, die Sie mit Storage Gateway verwenden möchten, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.
>
> Die Verwendung des Rsync-Dienstprogramms mit Ihrem Datei-Gateway führt zur Erstellung temporärer Dateien im Cache und zur Erstellung temporärer S3-Objekte in Amazon S3. Diese Situation führt zu frühen Löschgebühren in den Speicherklassen S3 Standard-Infrequent Access (S3 Standard-IA) und S3 Intelligent-Tiering.

Erstellen Sie wie folgt eine NFS-Dateifreigabe

1. Öffnen SieAWSStorage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/home/aus.
2. Klicken Sie aufErstellen einer DateifreigabeSo öffnen Sie denDateifreigabeeinstellungenangezeigten.
3. FürGatewayWählen Sie Ihr Amazon S3 File Gateway aus der Liste aus.
4. FürAmazon S3 S3-SpeicherortFühren Sie einen der folgenden Schritte aus:

   - Um die Dateifreigabe direkt mit einem S3-Bucket zu verbinden, wählen SieName eines S3-Bucketsund geben Sie dann den S3-Bucket-Namen und optional einen Präfixnamen für Objekte ein, die von der Dateifreigabe erstellt wurden. Ihr Gateway verwendet diesen Bucket zum Speichern und Abrufen von Dateien. Weitere Hinweise zum Erstellen eines neuen Buckets finden Sie unterWie erstelle ich einen S3 Bucket?imAmazon-S3-Benutzerhandbuchaus.
   - Um die Dateifreigabe über einen Zugriffspunkt mit einem S3-Bucket zu verbinden, wählen SieS3-Zugriffspunktund geben Sie dann den Namen des S3-Zugangspunkts und optional einen Präfixnamen für Objekte ein, die von der Dateifreigabe erstellt wurden. Ihre Bucket-Richtlinie muss so konfiguriert sein, dass sie die Zugriffssteuerung an den Access Point delegiert. Weitere Hinweise zu Zugriffspunkten finden Sie unterVerwalten des Datenzugriffs mit Amazon S3-ZugangspunktenundDelegieren der Zugangskontrolle an ZugriffspunkteimAmazon-S3-Benutzerhandbuchaus.
   - Um die Dateifreigabe über einen Access Point-Alias mit einem S3-Bucket zu verbinden, wählen SieAlias für S3-Zugriffspunkteund geben Sie dann den Aliasnamen des S3-Zugangspunkts und optional einen Präfixnamen für Objekte ein, die von der Dateifreigabe erstellt wurden. Wenn Sie diese Option wählen, kann das Datei-Gateway kein neues erstellenAWS Identity and Access Management(IAM) -Rolle und -Zugriffsrichtlinie in Ihrem Namen. Sie müssen eine vorhandene IAM-Rolle auswählen und eine Zugriffsrichtlinie imZugriff auf Ihren S3-BucketAbschnitt, der folgt. Weitere Hinweise zu Zugriffspunkt-Aliasen finden Sie unterVerwenden eines Alias im Bucket-Stil für Ihren Zugriffspunkt.imAmazon-S3-Benutzerhandbuchaus.

> **Note**
>
> - Wenn Sie einen Präfixnamen eingeben oder eine Verbindung über einen Access Point oder Access Point-Alias herstellen möchten, müssen Sie einen Namen für die Dateifreigabe eingeben.
> - Der Präfixname muss mit einem Schrägstrich enden (/) enthalten.
> - Nachdem die Dateifreigabe erstellt wurde, kann der Präfixname nicht geändert oder gelöscht werden.
> - Weitere Hinweise zur Nutzung von Präfixnamen finden Sie unterOrganisieren von Objekten mit PräfixenimAmazon-S3-Benutzerhandbuchaus.

5. FürAWS-Region, wähle dasAWS-Regiondes S3-Buckets.
6. FürName der Dateifreigabeein, geben Sie einen Namen für die Dateifreigabe ein. Der Standardname ist der S3-Bucket-Name oder der Name des Zugriffspunkts.

> **Note**
>
> - Wenn Sie einen Präfixnamen eingegeben haben oder sich für eine Verbindung über einen Access Point oder Access Point-Alias entschieden haben, müssen Sie einen Namen für die Dateifreigabe eingeben.
> - Nachdem die Dateifreigabe erstellt wurde, kann der Name der Dateifreigabe nicht gelöscht werden.

7. (Optional) FürAWS PrivateLinkfür S3wie folgt:

    1. So konfigurieren Sie die Dateifreigabe für die Verbindung zu S3 über einen Interface-Endpunkt in Ihrer Virtual Private Cloud (VPC), die vonAWS PrivateLink, wählenVerwenden von VPC-Endpunktenaus.
    2. Um den Endpunkt der VPC-Schnittstelle zu identifizieren, über den die Dateifreigabe eine Verbindung herstellen soll, wählen Sie entweder-VPC-Endpunkt-IDoderDNS-Name des VPC-Endpunktsund geben Sie dann die erforderlichen Informationen in das entsprechende Feld ein.

> **Note**
>
> - Dieser Schritt ist erforderlich, wenn die Dateifreigabe über einen VPC-Zugriffspunkt oder über einen Alias, der mit einem VPC-Zugriffspunkt verknüpft ist, mit S3 verbunden ist.
> - Dateifreigabe-VerbindungenAWS PrivateLinkwerden auf FIPS-Gateways nicht unterstützt.
> - Weitere Informationen zu finden Sie unterAWS PrivateLinkfinden Sie unter,AWS PrivateLinkfür Amazon S3imAmazon-S3-Benutzerhandbuchaus.

8. Wählen Sie in Access objects using (Zugriff auf Objekte unter Verwendung von) die Option Network File System (NFS) aus.
9. Wählen Sie unter Audit logs (Prüfungsprotokolle) eine der folgenden Optionen aus:

   - Wählen Sie zum Deaktivieren der ProtokollierungDisable logging (Protokollierung deaktivieren)aus.
   - Wählen Sie zum Erstellen eines neuen PrüfungsprotokollsEine neue Protokollgruppe erstellenaus.
   - Um ein vorhandenes Audit-Log zu verwenden, wählen SieVerwenden einer vorhandenen Protokollgruppeund wählen Sie dann ein Prüfungsprotokoll aus der Liste aus.

   Weitere Informationen zu Auditprotokollen finden Sie unter Verstehen von Datei-Gateway-Audit.
10. FürAutomatisierte Cache-Aktualisierung von S3, wählenAktualisierungsintervall einstellenund legen Sie die Zeit in Tagen, Stunden und Minuten fest, um den Cache der Dateifreigabe mit Time To Live (TTL) zu aktualisieren. TTL ist die Zeitspanne seit der letzten Aktualisierung. Nach Ablauf des TTL-Intervalls führt der Zugriff auf das Verzeichnis dazu, dass das Datei-Gateway den Inhalt dieses Verzeichnisses zuerst aus dem Amazon S3 S3-Bucket aktualisiert.
11. FürDatei-Upload, wählenEinstellungszeit (Sekunden)um benachrichtigt zu werden, wenn eine Datei vom Datei-Gateway vollständig auf S3 hochgeladen wurde. Legen Sie den Wert fürZeit eingleichenin Sekunden, um die Anzahl der Sekunden zu steuern, die nach dem letzten Zeitpunkt gewartet werden müssen, den ein Client in eine Datei geschrieben hat, bevor ein`ObjectUploaded`-Benachrichtigung. Da Clients viele kleine Schreibvorgänge in Dateien vornehmen können, legen Sie diesen Parameter am besten so lange wie möglich fest, um zu

vermeiden, dass mehrere Benachrichtigungen für dieselbe Datei in einem kleinen Zeitraum generiert werden. Weitere Informationen finden Sie unter Benachrichtigung zum Hochladen von Dateien.

> **Note**
>
> Diese Einstellung hat keinen Einfluss auf den Zeitpunkt des Hochladens des Objekts auf S3, nur auf den Zeitpunkt der Benachrichtigung.

12. (Optional) Geben Sie im Abschnitt Add tags (Tags hinzufügen) einen Schlüssel und Wert ein, um Tags zu Ihrer Dateifreigabe hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen Ihrer Dateifreigabe erleichtert.
13. Wählen Sie Next (Weiter). DieKonfigurieren Sie, wie Dateien in Amazon S3 gespeichert werdenDie Seite wird angezeigt.
14. FürSpeicherklasse für neue ObjekteWählen Sie eine Speicherklasse aus, die für neue Objekte verwendet werden soll, die in Ihrem Amazon S3 Bucket erstellt werden:

    - Um Ihre häufig aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind, wählen SieS3 Standardaus. Weitere Hinweise zur S3-Speicherklasse Standard finden Sie unterSpeicherklassen für Objekte mit häufigem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
    - Um die Speicherkosten zu optimieren, indem Sie Daten automatisch in die kostengünstigste Speicherzugriffsstufe verschieben möchten, wählen SieS3 Intelligent-Tieringaus. Weitere Informationen zur S3-Intelligent-Tiering-Speicherklasse finden Sie unterSpeicherklasse, die häufig und weniger häufig verwendete Objekte optimiertimAmazon Simple Storage Service — Benutzerhandbuchaus.
    - Um Ihre selten aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind, wählen SieS3 Standard-IAaus. Weitere Hinweise zur S3-Speicherklasse Standard finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
    - Um Ihre selten aufgerufenen Objektdaten in einer einzigen Availability Zone zu speichern, wählen SieS3 One Zone-IAaus. Weitere Hinweise zur S3 One Zone-IA-Speicherklasse finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.

Um Ihre S3-Abrechnung zu überwachen, verwenden SieAWS Trusted Advisoraus. Weitere Informationen finden Sie unterÜberwachungstoolsimAmazon Simple Storage Service — Benutzerhandbuchaus.

15. Wählen Sie in Object metadata (Objektmetadaten) die Metadaten aus, die Sie verwenden möchten:

    - Um die Bestimmung des MIME-Typs für hochgeladene Objekte basierend auf Dateierweiterungen zu aktivieren, wählen SieGuess MIME-Typaus.
    - Um dem Eigentümer des S3-Buckets, der der NFS-Dateifreigabe zugeordnet ist, volle Kontrolle zu gewähren, wählen SieGeben Sie Bucket-Besitzer die volle Kontrolleaus. Weitere Informationen dazu, wie Sie mit Ihrer Dateifreigabe auf Objekte in einem Bucket eines anderen Kontos zugreifen, finden Sie unterVerwenden einer Dateifreigabe für kontoübergreifenden Zugriffaus.
    - Wenn Sie diese Dateifreigabe in einem Bucket verwenden, bei dem der Anforderer oder Reader anstelle des Bucket-Eigentümers für den Zugriff bezahlt, wählen SieAnforderer aktivieren zahltaus. Weitere Informationen finden Sie unter Buckets mit Bezahlung durch den Anforderer.

16. FürZugriff auf Ihren S3-Bucket, wähle dasAWS Identity and Access Management(IAM) -Rolle, die Ihr Datei-Gateway für den Zugriff auf Ihren Amazon S3 S3-Bucket verwenden soll:

    - Um das File Gateway in Ihrem Namen eine neue IAM-Rolle und -Zugriffsrichtlinie zu aktivieren, wählen SieErstellen Sie eine neue IAM-Rolleaus. Diese Option ist nicht verfügbar, wenn die Dateifreigabe über einen Access Point-Alias mit Amazon S3 verbunden ist.
    - Um eine vorhandene IAM-Rolle auszuwählen und die Zugriffsrichtlinie manuell zu erstellen, wählen SieVerwenden Sie eine vorhandene IAM-Rolleaus. Sie müssen diese Option verwenden, wenn Ihre Dateifreigabe über einen Access Point-Alias mit Amazon S3 verbunden ist. In derIAM-RolleGeben Sie den Amazon-Ressourcennamen (ARN) für die Rolle ein, die für den Zugriff auf Ihren Bucket verwendet wird. Weitere Informationen zu IAM-Rollen finden Sie unterIAM rolesimAWS Identity and Access Management-Benutzerhandbuchaus.

    Weitere Informationen zum Zugriff auf Ihren S3-Bucket finden Sie unter Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket.

17. FürVerschlüsselungWählen Sie die Art der Verschlüsselungsschlüssel aus, die zum Verschlüsseln von Objekten verwendet werden sollen, die Ihr File Gateway in Amazon S3 speichert:

    - Um die serverseitige Verschlüsselung zu verwenden, die mit Amazon S3 (SSE-S3) verwaltet wird, wählen SieS3-verwaltete Schlüssel (SSE-S3)aus.
    - So verwenden Sie serverseitige Verschlüsselung mitAWS Key Management Service(SSE-KMS), wählen SieVon KMS verwaltete Schlüssel (SSE-KMS)aus. In derPrimärschlüsseleine vorhandeneAWS KMS keyoder wählenErstellen Sie einen neuen KMS-SchlüsselErstellen Sie im Feld einen neuen KMS-SchlüsselAWS Key Management Service(AWS KMS) - Konsole. Weitere Informationen zuAWS KMSfinden Sie unter,Was ist ?AWS Key Management Service?imAWS Key Management ServiceEntwicklerhandbuchaus.

    > **Note**
    >
    > So geben Sie einAWS KMSSchlüssel mit einem Alias, der nicht aufgeführt ist oder um einenAWS KMSSchlüssel von einem anderenAWS-KontoSie müssen verwenden.AWS Command Line Interface(AWS CLI) enthalten. Weitere Informationen finden Sie unterCreateNFSFileShareimAWSStorage Gateway Gateway-APIaus. Asymmetrische KMS-Schlüssel werden nicht unterstützt.

18. Klicken Sie aufWeiterum Einstellungen für den Dateizugriff zu konfigurieren.

So konfigurieren Sie Dateizugriffs-Einstellungen

1. FürZulässige Clientsangeben, ob Sie den Zugriff jedes Clients auf Ihre Dateifreigabe zulassen oder einschränken möchten. Geben Sie die IP-Adresse oder CIDR-Notation für die Clients an, die Sie zulassen möchten. Weitere Informationen zu unterstützten NFS-Clients finden Sie unter Unterstützte NFS-Clients für ein File Gateway.
2. FürMount-Optionendie Optionen an, die Sie wünschenSquash-LevelundExportieren alsaus.

   Wählen Sie für Squash-Level eine der folgenden Optionen aus:

   - Alle Squash: Der gesamte Benutzerzugriff wird der Benutzer-ID (UID) (65534) und der Gruppen-ID (GID) (65534) zugeordnet.
   - Kein Root-Squash: Der Remote-Superuser (Root) erhält Zugriff als Root.

- Root-Squash (Standardeinstellung): Der Zugriff für den Remote-Superuser (Root) wird UID (65534) und GID (65534) zugeordnet.

Wählen Sie unter Exportieren als eine der folgenden Optionen aus:

- Schreib- und Leseberechtigung
- Read-only

> **Note**
>
> Für Dateifreigaben, die auf einem Microsoft Windows-Client bereitgestellt sind, wenn Sie wählenRead-onlywird Ihnen möglicherweise ein unerwarteter Fehler angezeigt, sodass Sie den Ordner nicht erstellen können. Sie können diese Meldung ignorieren.

3. Unter Standardeinstellungen für Datei-Metadaten können Sie die Verzeichnisberechtigungen, Dateiberechtigungen, Benutzer-ID und Gruppen-ID bearbeiten. Weitere Informationen finden Sie unter Bearbeiten der Metadaten-Standardwerte für Ihre NFS-Dateifreigabe.
4. Wählen Sie Next (Weiter).
5. Überprüfen Sie die Konfigurationseinstellungen für Ihre Dateifreigabe und wählen Sie dannFinishaus.

   Nach der Erstellung Ihrer NFS-Dateifreigabe können Sie die Einstellungen für Ihre Dateifreigabe auf der Registerkarte Details (Details) der Dateifreigabe anzeigen.

Nächster Schritt

So mounten Sie Ihre NFS-Dateifreigabe auf Ihrem Client

Erstellen Sie eine SMB-Dateifreigabe

Bevor Sie eine Server-Dateifreigabe (SMB) erstellen, stellen Sie sicher, dass Sie die SMB-Sicherheitseinstellungen für Ihr File Gateway konfigurieren. Außerdem müssen Sie entweder Microsoft Active Directory (AD) oder den Gastzugriff für die Authentifizierung konfigurieren. Eine Dateifreigabe bietet nur eine Art von SMB-Zugriff. Detaillierte Anweisungen finden Sie unterBearbeiten von SMB-Einstellungen für ein Gatewayaus.

> **Note**
>
> Eine SMB-Dateifreigabe funktioniert nicht ordnungsgemäß, wenn nicht die erforderlichen Ports in Ihrer Sicherheitsgruppe geöffnet sind. Weitere Informationen finden Sie unter Port-Anforderungen.

> **Note**
>
> Wenn eine Datei von einem SMB-Client in das Datei-Gateway geschrieben wird, lädt das Datei-Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von seinen Metadaten (Eigentümer, Zeitstempel usw.). Durch das Hochladen der Dateidaten wird ein S3-Objekt erstellt, und das Hochladen der Metadaten für die Datei aktualisiert die Metadaten für das S3-Objekt. Dieser Prozess erstellt eine andere Version des Objekts, was zu zwei Versionen eines Objekts führt. Wenn die S3-Versioning aktiviert ist, werden beide Versionen gespeichert.
>
> Wenn Sie die Metadaten einer in Ihrem Datei-Gateway gespeicherten Datei ändern, wird ein neues S3-Objekt erstellt und ersetzt das vorhandene S3-Objekt. Dieses Verhalten unterscheidet sich vom Bearbeiten einer Datei in einem Dateisystem, wobei das Bearbeiten einer Datei nicht dazu führt, dass eine neue Datei erstellt wird. Testen Sie alle Dateioperationen, mit denen Sie verwenden möchtenAWSStorage Gateway, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.
>
> Berücksichtigen Sie sorgfältig die Verwendung von S3-Versionierung und regionsübergreifender Replikation (CRR) in Amazon S3, wenn Sie Daten von Ihrem Datei-Gateway hochladen. Das Hochladen von Dateien von Ihrem Datei-Gateway auf Amazon S3 bei aktivierter S3-Versionierung führt zu mindestens zwei Versionen eines S3-Objekts. Bestimmte Workflows mit großen Dateien und Dateischreibmustern wie Datei-Uploads, die in mehreren Schritten ausgeführt werden, können die Anzahl der gespeicherten S3-Objektversionen erhöhen. Wenn der Datei-Gateway-Cache aufgrund hoher Dateischreibraten Speicherplatz freigeben muss, werden möglicherweise mehrere S3-Objektversionen erstellt. Diese Szenarien erhöhen den S3-Speicher, wenn die S3-Versionierung aktiviert ist, und erhöhen die mit CRR verbundenen Transferkosten. Testen Sie alle Dateioperationen, die Sie mit Storage Gateway verwenden möchten, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.
>
> Die Verwendung des Rsync-Dienstprogramms mit Ihrem Datei-Gateway führt zur Erstellung temporärer Dateien im Cache und zur Erstellung temporärer S3-Objekte in Amazon S3. Diese

Situation führt zu frühen Löschgebühren in den Speicherklassen S3 Standard-Infrequent Access (S3 Standard-IA) und S3 Intelligent-Tiering.

Erstellen einer SMB-Dateifreigabe

Erstellen Sie wie folgt eine SMB-Dateifreigabe

1. Öffnen SieAWSStorage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/home/aus.
2. Klicken Sie aufErstellen einer DateifreigabeSo öffnen Sie denDateifreigabeeinstellungenangezeigten.
3. FürGatewayWählen Sie Ihr Amazon S3 File Gateway aus der Liste aus.
4. FürAmazon S3 S3-SpeicherortFühren Sie einen der folgenden Schritte aus:

   - Um die Dateifreigabe direkt mit einem S3-Bucket zu verbinden, wählen SieName eines S3-Bucketsund geben Sie dann den Bucket-Namen und optional einen Präfixnamen für Objekte ein, die von der Dateifreigabe erstellt wurden. Ihr Gateway verwendet diesen Bucket zum Speichern und Abrufen von Dateien. Weitere Hinweise zum Erstellen eines neuen Buckets finden Sie unterWie erstelle ich einen S3 Bucket?imAmazon-S3-Benutzerhandbuchaus.
   - Um die Dateifreigabe über einen Zugriffspunkt mit einem S3-Bucket zu verbinden, wählen SieS3-Zugriffspunktund geben Sie dann den Namen des S3-Zugangspunkts und optional einen Präfixnamen für Objekte ein, die von der Dateifreigabe erstellt wurden. Ihre Bucket-Richtlinie muss so konfiguriert sein, dass sie die Zugriffssteuerung an den Access Point delegiert. Weitere Hinweise zu Zugriffspunkten finden Sie unterVerwalten des Datenzugriffs mit Amazon S3-ZugangspunktenundDelegieren der Zugangskontrolle an ZugriffspunkteimAmazon-S3-Benutzerhandbuchaus.
   - Um die Dateifreigabe über einen Access Point-Alias mit einem S3-Bucket zu verbinden, wählen SieAlias des S3-Zugriffspunktsund geben Sie dann den Aliasnamen des S3-Zugangspunkts und optional einen Präfixnamen für Objekte ein, die von der Dateifreigabe erstellt wurden. Wenn Sie diese Option wählen, kann das Datei-Gateway kein neues erstellenAWS Identity and Access Management(IAM) -Rolle und -Zugriffsrichtlinie in Ihrem Namen. Sie müssen eine vorhandene IAM-Rolle auswählen und eine Zugriffsrichtlinie imZugriff auf Ihren S3-BucketAbschnitt, der folgt. Weitere Hinweise zu Zugriffspunkt-Aliasen finden Sie unterVerwenden eines Alias im Bucket-Stil für Ihren Zugriffspunkt.imAmazon-S3-Benutzerhandbuchaus.

> **Note**
>
> - Wenn Sie einen Präfixnamen eingeben oder eine Verbindung über einen Access Point oder Access Point-Alias herstellen möchten, müssen Sie einen Namen für die Dateifreigabe eingeben.
> - Der Präfixname muss mit einem Schrägstrich enden (/) enthalten.
> - Nachdem die Dateifreigabe erstellt wurde, kann der Präfixname nicht geändert oder gelöscht werden.
> - Weitere Hinweise zur Nutzung von Präfixnamen finden Sie unterOrganisieren von Objekten mit PräfixenimAmazon-S3-Benutzerhandbuchaus.

5. FürAWS-Region, wähle dasAWS-Regiondes S3-Buckets.
6. FürName der Dateifreigabeein, geben Sie einen Namen für die Dateifreigabe ein. Der Standardname ist der S3-Bucket-Name oder der Name des Zugriffspunkts.

> **Note**
>
> - Wenn Sie einen Präfixnamen eingegeben haben oder sich für eine Verbindung über einen Access Point oder Access Point-Alias entschieden haben, müssen Sie einen Namen für die Dateifreigabe eingeben.
> - Nachdem die Dateifreigabe erstellt wurde, kann der Name der Dateifreigabe nicht gelöscht werden.

7. (Optional) FürAWS PrivateLinkfür S3wie folgt:

    1. So konfigurieren Sie die Dateifreigabe für die Verbindung zu S3 über einen Interface-Endpunkt in Ihrer Virtual Private Cloud (VPC), die vonAWS PrivateLink, wählenVerwenden von VPC-Endpunktenaus.
    2. Um den Endpunkt der VPC-Schnittstelle zu identifizieren, über den die Dateifreigabe eine Verbindung herstellen soll, wählen Sie entweder-VPC-Endpunkt-IDoderDNS-Name des VPC-Endpunktsund geben Sie dann die erforderlichen Informationen in das entsprechende Feld ein.

> **Note**
>
> - Dieser Schritt ist erforderlich, wenn die Dateifreigabe über einen VPC-Zugriffspunkt oder über einen Alias, der mit einem VPC-Zugriffspunkt verknüpft ist, mit S3 verbunden ist.
> - Dateifreigabe-VerbindungenAWS PrivateLinkwerden auf FIPS-Gateways nicht unterstützt.
> - Weitere Informationen zu finden Sie unterAWS PrivateLinkfinden Sie unter,AWS PrivateLinkfür Amazon S3imAmazon Simple Storage Service — Benutzerhandbuchaus.

8. Wählen Sie in Access Objects using (Zugriff auf Objekte mit) die Option Server Message Block (SMB) (Servernachrichtenblock) aus.
9. Wählen Sie unter Audit logs (Prüfungsprotokolle) eine der folgenden Optionen aus:

   - Wählen Sie zum Deaktivieren der ProtokollierungDisable logging (Protokollierung deaktivieren)aus.
   - Wählen Sie zum Erstellen eines neuen PrüfungsprotokollsEine neue Protokollgruppe erstellenaus.
   - Wählen Sie zur Verwendung einer vorhandenen ProtokollgruppeVerwenden einer vorhandenen Protokollgruppeund wählen Sie dann ein Prüfungsprotokoll aus der Liste aus.

   Weitere Informationen zu Auditprotokollen finden Sie unter Verstehen von Datei-Gateway-Audit.
10. FürAutomatisierte Cache-Aktualisierung von S3, wählenAktualisierungsintervall einstellen, und legen Sie dann die Zeit in Tagen, Stunden und Minuten fest, um den Cache der Dateifreigabe mit Time To Live (TTL) zu aktualisieren. TTL ist die Zeitspanne seit der letzten Aktualisierung. Nach Ablauf des TTL-Intervalls führt der Zugriff auf das Verzeichnis dazu, dass das Datei-Gateway den Inhalt dieses Verzeichnisses zuerst aus dem Amazon S3 S3-Bucket aktualisiert.
11. FürDatei-Upload, wählenEinstellungszeit (Sekunden)um benachrichtigt zu werden, wenn eine Datei vom Datei-Gateway vollständig auf S3 hochgeladen wurde. Legen Sie den Wert fürZeit eingleichenin Sekunden, um die Anzahl der Sekunden zu steuern, die nach dem letzten Zeitpunkt gewartet werden müssen, den ein Client in eine Datei geschrieben hat, bevor ein`ObjectUploaded`-Benachrichtigung. Da Clients viele kleine Schreibvorgänge in Dateien

vornehmen können, legen Sie diesen Parameter am besten so lange wie möglich fest, um zu vermeiden, dass mehrere Benachrichtigungen für dieselbe Datei in einem kleinen Zeitraum generiert werden. Weitere Informationen finden Sie unter Benachrichtigung zum Hochladen von Dateien.

> **Note**
>
> Diese Einstellung hat keinen Einfluss auf den Zeitpunkt des Hochladens des Objekts auf S3, nur auf den Zeitpunkt der Benachrichtigung.

12. (Optional) ImTagsAbschnitt auswählenNeues Tag hinzufügenund geben Sie dann einen Schlüssel und einen Wert ein, um Tags zu Ihrer Dateifreigabe hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen Ihrer Dateifreigabe erleichtert.
13. Wählen Sie Next (Weiter). DieAmazon S3 S3-SpeichereinstellungenDie Seite wird angezeigt.
14. FürSpeicherklasse für neue ObjekteWählen Sie eine Speicherklasse aus, die für neue Objekte verwendet werden soll, die in Ihrem Amazon S3 Bucket erstellt werden:

    - Um Ihre häufig aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind, wählen SieS3 Standardaus. Weitere Hinweise zur S3-Speicherklasse Standard finden Sie unterSpeicherklassen für Objekte mit häufigem ZugriffimBenutzerhandbuch für Amazon Simple Storage Serviceaus.
    - Um die Speicherkosten zu optimieren, indem Sie Daten automatisch in die kostengünstigste Speicherzugriffsstufe verschieben möchten, wählen SieS3 Intelligent-Tieringaus. Weitere Informationen zur S3-Intelligent-Tiering-Speicherklasse finden Sie unterSpeicherklasse, die häufig und weniger häufig verwendete Objekte optimiertimBenutzerhandbuch für Amazon Simple Storage Serviceaus.
    - Um Ihre selten aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind, wählen SieS3 Standard-IAaus. Weitere Hinweise zur S3-Speicherklasse Standard finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
    - Um Ihre selten aufgerufenen Objektdaten in einer einzigen Availability Zone zu speichern, wählen SieS3 One Zone-IAaus. Weitere Hinweise zur S3 One Zone-IA-Speicherklasse finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.

Um Ihre S3-Abrechnung zu überwachen, verwenden SieAWS Trusted Advisoraus. Weitere Informationen finden Sie unterÜberwachungstoolsimAmazon Simple Storage Service — Benutzerhandbuchaus.

15. Wählen Sie in Object metadata (Objektmetadaten) die Metadaten aus, die Sie verwenden möchten:

    - Um die Bestimmung des MIME-Typs für hochgeladene Objekte basierend auf Dateierweiterungen zu aktivieren, wählen SieGuess MIME-Typaus.
    - Um dem Eigentümer des S3-Buckets, der der SMB-Dateifreigabe zugeordnet ist, volle Kontrolle zu gewähren, wählen SieGeben Sie Bucket-Besitzer die volle Kontrolleaus. Weitere Informationen dazu, wie Sie mit Ihrer Dateifreigabe auf Objekte in einem Bucket eines anderen Kontos zugreifen, finden Sie unterVerwenden einer Dateifreigabe für kontoübergreifenden Zugriffaus.
    - Um dem Eigentümer des S3-Buckets, der der SMB-Dateifreigabe zugeordnet ist, volle Kontrolle zu gewähren, wählen SieAnforderer aktivieren zahltaus. Weitere Informationen finden Sie unter Buckets mit Bezahlung durch den Anforderer.

16. FürZugriff auf Ihren S3-Bucket, wähle dasAWS Identity and Access Management(IAM) -Rolle, die Ihr Datei-Gateway für den Zugriff auf Ihren Amazon S3 S3-Bucket verwenden soll:

    - Um das File Gateway in Ihrem Namen eine neue IAM-Rolle und -Zugriffsrichtlinie zu aktivieren, wählen SieErstellen Sie eine neue IAM-Rolleaus. Diese Option ist nicht verfügbar, wenn die Dateifreigabe über einen Access Point-Alias mit Amazon S3 verbunden ist.
    - Um eine vorhandene IAM-Rolle auszuwählen und die Zugriffsrichtlinie manuell zu erstellen, wählen SieVerwenden Sie eine vorhandene IAM-Rolleaus. Sie müssen diese Option verwenden, wenn Ihre Dateifreigabe über einen Access Point-Alias mit Amazon S3 verbunden ist. In derIAM-RolleGeben Sie den Amazon-Ressourcennamen (ARN) für die Rolle ein, die für den Zugriff auf Ihren Bucket verwendet wird. Weitere Informationen zu IAM-Rollen finden Sie unterIAM rolesimAWS Identity and Access Management-Benutzerhandbuchaus.

    Weitere Informationen zum Zugriff auf Ihren S3-Bucket finden Sie unter Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket.

17. FürVerschlüsselungWählen Sie die Art der Verschlüsselungsschlüssel aus, die zum Verschlüsseln von Objekten verwendet werden sollen, die Ihr File Gateway in Amazon S3 speichert:

- Um die serverseitige Verschlüsselung zu verwenden, die mit Amazon S3 (SSE-S3) verwaltet wird, wählen SieS3-verwaltete Schlüssel (SSE-S3)aus.
- So verwenden Sie serverseitige Verschlüsselung mitAWS Key Management Service(SSE-KMS), wählen SieVon KMS verwaltete Schlüssel (SSE-KMS)aus. In derPrimärschlüsseleine vorhandeneAWS KMS keyoder wählenErstellen Sie einen neuen KMS-SchlüsselErstellen Sie im Feld einen neuen KMS-SchlüsselAWS Key Management Service(AWS KMS) - Konsole. Weitere Informationen zuAWS KMSfinden Sie unter,Was ist ?AWS Key Management Service?imAWS Key Management ServiceEntwicklerhandbuchaus.

> **Note**
>
> So geben Sie einAWS KMSSchlüssel mit einem Alias, der nicht aufgeführt ist oder um einenAWS KMSSchlüssel von einem anderenAWS-KontoSie müssen verwenden.AWS Command Line Interface(AWS CLI) enthalten. Weitere Informationen finden Sie unterCreateNFSFileShareimAWSStorage Gateway Gateway-APIaus. Asymmetrische KMS-Schlüssel werden nicht unterstützt.

18. Wählen Sie Next (Weiter). DieDateizugriffseinstellungenDie Seite wird angezeigt.
19. FürAuthentifizierungsmethodeWählen Sie die Authentifizierungsmethode aus, die Sie verwenden möchten.

    - Um Ihr Unternehmen Microsoft AD für den benutzerauthentifizierten Zugriff auf Ihre SMB-Dateifreigabe zu verwenden, wählen SieActive Directoryaus. Ihr File Gateway muss mit einer Domäne verbunden sein.
    - Um nur Gastzugriff zu gewähren, wählen SieZugriff auf Gästeaus. Wenn Sie sich für diese Authentifizierungsmethode entscheiden, muss Ihr Datei-Gateway nicht Teil einer Microsoft AD-Domäne sein. Sie können auch ein File Gateway verwenden, das ein Mitglied einer AD-Domäne ist, um Dateifreigaben mit Gastzugriff zu erstellen. Sie müssen ein Gastpasswort für Ihren SMB-Server im entsprechenden Feld festlegen.

    > **Note**
    >
    > Beide Zugriffstypen sind gleichzeitig verfügbar.

20. In derSMB-FreigabeeinstellungenWählen Sie Ihre Einstellungen aus.

Wählen Sie unter Exportieren als eine der folgenden Optionen aus:

- Schreib- und Leseberechtigung (Standardwert)
- Read-only

> **Note**
>
> Für Dateifreigaben, die auf einem Microsoft Windows-Client bereitgestellt sind, wenn Sie wählenRead-onlywird Ihnen möglicherweise ein unerwarteter Fehler angezeigt, sodass Sie den Ordner nicht erstellen können. Sie können diese Meldung ignorieren.

Für File/directory access controlled by (Datei-/Verzeichniszugriff kontrolliert von) wählen Sie eine der folgenden Optionen aus:

- Um fein abgestimmte Berechtigungen für Dateien und Ordner in Ihrer SMB-Dateifreigabe festzulegen, wählen SieListe der Windows-Zugriffskontrolleaus. Weitere Informationen finden Sie unter Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe.
- Um POSIX-Berechtigungen zu verwenden, um den Zugriff auf Dateien und Verzeichnisse zu verwenden, die über eine NFS- oder eine SMB-Dateifreigabe gespeichert werden, wählen SiePOSIX-Berechtigungenaus.

Wenn Ihre Authentifizierungsmethode lautetActive Directory, fürAdmin-Benutzer/GruppenGeben Sie eine durch Komma getrennte Liste der AD-Benutzer und -Gruppen ein. Tun Sie dies, wenn Sie möchten, dass der Admin-Benutzer zum Aktualisieren von Zugriffssteuerungslisten (ACLs) für alle Dateien und Ordnern in der Dateifreigabe berechtigt ist. Diese Benutzer und Gruppen haben dann Administratorrechte für die Dateifreigabe. Einer Gruppe muss das Präfix@Charakter zum Beispiel`@group1`aus.

FürGroß-/KleinschreibungWählen Sie eine der folgenden Optionen aus:

- Damit das Gateway die Groß- und Kleinschreibung steuern kann, wählen SieKunde spezifiziertaus.
- Damit der Client die Groß- und Kleinschreibung steuern kann, wählen SieKleinschreibung erzwingenaus.

> **Note**
>
> - Bei Auswahl dieser Option gilt diese Einstellung sofort für neue SMB-Clientverbindungen. Bestehende SMB-Clientverbindungen müssen sich von der Dateifreigabe trennen und erneut verbinden, damit die Einstellung wirksam wird.

FürZugriffs-basierte AufzählungWählen Sie eine der folgenden Optionen aus:

- Um die Dateien und Ordner auf der Freigabe nur für Benutzer sichtbar zu machen, die Lesezugriff haben, wählen SieDeaktiviert für Dateien und Verzeichnisseaus.
- Um die Dateien und Ordner auf der Freigabe während der Verzeichnisaufzählung für alle Benutzer sichtbar zu machen, wählen SieAktiviert für Dateien und Verzeichnisseaus.

> **Note**
>
> Die zugriffsbasierte Aufzählung ist ein System, das die Aufzählung von Dateien und Ordnern auf einer SMB-Dateifreigabe basierend auf den Zugriffskontrolllisten (ACLs) der Freigabe filtert.

FürOpportunistisches Schloss (Oplock)Wählen Sie eine der folgenden Optionen aus:

- Damit die Dateifreigabe das opportunistische Sperren verwenden kann, um die Dateipufferungsstrategie zu optimieren, wählen SieEnabledaus. In den meisten Fällen verbessert die Aktivierung opportunistischer Sperren die Leistung, insbesondere im Hinblick auf Windows-Kontextmenüs.
- Um die Verwendung von opportunistischer Sperre zu verhindern, wählen SieDisabledaus. Wenn mehrere Windows-Clients in Ihrer Umgebung häufig dieselben Dateien gleichzeitig bearbeiten, kann das Deaktivieren der opportunistischen Sperre manchmal die Leistung verbessern.

> **Note**
>
> Die Aktivierung des opportunistischen Sperren von Shares mit Berücksichtigung von Groß- und Kleinschreibung wird nicht für Workloads empfohlen, die in einem anderen Fall Zugriff auf Dateien mit demselben Namen beinhalten.

21. (Optional) ImZugriff auf Benutzer- und Gruppen-DateifreigabeWählen Sie Ihre Einstellungen aus.

    FürZulässige Benutzer und Gruppen, wählenZugelassenen Benutzer hinzufügenoderZugelassene Gruppe hinzufügenund geben Sie einen AD-Benutzer oder eine Gruppe ein, die den Zugriff auf die Dateifreigabe zulassen soll. Wiederholen Sie diesen Vorgang, um so viele Benutzer und Gruppen wie nötig zuzulassen.

    FürBenutzer und Gruppen verweigert, wählenBenutzer hinzufügenoderHinzufügen einer abgelehnten Gruppeund geben Sie einen AD-Benutzer oder eine Gruppe ein, der der Zugriff auf die Dateifreigabe verweigern soll. Wiederholen Sie diesen Vorgang, um so viele Benutzer und Gruppen wie nötig abzulehnen.

    > **Note**
    >
    > DieZugriff auf Benutzer- und Gruppen-Dateifreigabewird nur angezeigt, wennActive Directoryausgewählt ist.
    > Geben Sie nur den AD-Benutzernamen oder -Gruppennamen ein. Der Domänenname für das spezifische AD, mit dem das Gateway verbunden wird, geht aus der Mitgliedschaft des Gateways hervor.
    > Wenn Sie keine zulässigen oder verweigerten Benutzer oder Gruppen angeben, kann jeder authentifizierte AD-Benutzer die Dateifreigabe exportieren.

22. Wählen Sie Next (Weiter).
23. Überprüfen Sie die Konfigurationseinstellungen für Ihre Dateifreigabe und wählen Sie dannFinishaus.

    Nachdem Ihre SMB-Dateifreigabe erstellt wurde, können Sie die Einstellungen für die Dateifreigabe auf der Registerkarte Details der Dateifreigabe anzeigen.

Nächster Schritt

So mounten Sie Ihre SMB-Dateifreigabe auf Ihrem Client

So mounten und verwenden Sie Ihre Dateifreigabe

Im Folgenden finden Sie Anweisungen dazu, wie Sie Ihre Dateifreigabe auf dem Client mounten, die Freigabe verwenden und Ihr File Gateway testen und bei Bedarf Ressourcen bereinigen können. Weitere Informationen über unterstützte NFS-Clients (Network File System) finden Sie unter Unterstützte NFS-Clients für ein File Gateway. Weitere Informationen über unterstützte SMB-Clients (Service Message Block) finden Sie unter Unterstützte SMB-Clients für ein File Gateway.

Beispielbefehle zum Mounten Ihrer Dateifreigabe finden Sie auf der AWS Management Console. In den folgenden Abschnitten erfahren Sie, wie Sie Ihre Dateifreigabe auf Ihrem Client mounten, Ihre Freigabe verwenden, Ihr File Gateway testen und bei Bedarf Ressourcen bereinigen können.

Themen

So mounten Sie Ihre NFS-Dateifreigabe auf Ihrem Client

Jetzt mounten Sie Ihre NFS-Dateifreigabe auf einem Laufwerk auf dem Client und weisen es Ihrem Amazon S3 S3-Bucket zu.

So mounten Sie eine Dateifreigabe und weisen sie einem Amazon S3 S3-Bucket zu

1. Wenn Sie einen Microsoft Windows-Client verwenden, sollten Sie eine SMB-Dateifreigabe erstellen und über einen SMB-Client, der bereits auf einem Windows-Client installiert ist, auf diese zugreifen. Wenn Sie NFS verwenden, aktivieren Sie Services für NFS in Windows.
2. Mounten Sie Ihre NFS-Dateifreigabe:

   - Geben Sie für Linux-Clients den folgenden Befehl in die Befehlszeile ein.

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

   - Geben Sie für MacOS-Clients den folgenden Befehl in die Befehlszeile ein.

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

- Geben Sie für Windows-Clients den folgenden Befehl in die Befehlszeile ein.

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

Angenommen, auf einem Windows-Client lautet die IP-Adresse Ihrer VM 123.123.1.2 und der Name Ihres Amazon S3 S3-Buckets ist`test-bucket`aus. Gehen wir außerdem davon aus, dass Sie Laufwerk T zuordnen möchten. In diesem Fall sieht Ihr Befehl wie folgt aus.

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

> **Note**
>
> Beachten Sie beim Mounten von Dateifreigaben Folgendes:
>
> - Möglicherweise haben Sie einen Fall, in dem ein Ordner und ein Objekt in einem Amazon S3 S3-Bucket vorhanden sind und den gleichen Namen haben. Wenn der Objektname keinen abschließenden Schrägstrich enthält, ist nur der Ordner in einem File Gateway sichtbar. Wenn ein Bucket beispielsweise ein Objekt mit dem Namen enthält`test`oder`test/`und ein Ordner mit dem Name`test/test1`, nur`test/`und`test/test1`sind in einem Datei-Gateway sichtbar.
> - Möglicherweise müssen Sie die Dateifreigabe nach einem Client-Neustart erneut mounten.
> - Standardmäßig verwendet Windows ein zeitweiliges Mounten für Ihre NFS-Freigabe. Bei einem zeitweiligen Mounten kommt es bei Verbindungsprobleme schneller zu einer Zeitüberschreitung. Wir empfehlen das dauerhafte Mounten, da dieses sicherer ist und Ihre Daten besser erhalten bleiben. Der Befehl für ein zeitweiliges Mounten lässt den Schalter **`-o mtype=hard`** aus. Der Windows-Befehl für ein dauerhaftes Mounten verwendet den Schalter `-o mtype=hard`.
> - Wenn Sie Windows-Clients verwenden, sollten Sie nach dem Mounten Ihre `mount`-Optionen überprüfen, indem Sie den Befehl `mount` ohne Optionen ausführen. Die Antwort sollte bestätigen, dass die Dateifreigabe mit den letzten von Ihnen angegebenen Optionen gemountet wurde. Sie sollte auch bestätigen, dass Sie keine

zwischengespeicherten alten Einträge verwenden. Für das Löschen solcher Einträge werden mindestens 60 Sekunden benötigt.

Nächster Schritt

[Testen Sie Ihr S3 File Gateway]

So mounten Sie Ihre SMB-Dateifreigabe auf Ihrem Client

Jetzt mounten Sie Ihre SMB-Dateifreigabe und ordnen sie einem Laufwerk zu, auf das Ihr Client Zugriff hat. Der Abschnitt File Gateway der Konsole zeigt die unterstützten Mounting-Befehle für SMB-Clients. Im Folgenden finden Sie einige zusätzliche Optionen, die Sie ausprobieren können.

Sie können mehrere verschiedene Methoden zum Mounten von SMB-Dateifreigaben verwenden, wie beispielsweise:

- Eingabeaufforderung`cmdkey`und`net use`) — Mit der Eingabeaufforderung mounten Sie Ihre Dateifreigabe. Speichern Sie Ihre Anmeldeinformationen mit`cmdkey`, montieren Sie dann das Laufwerk mit`net use`Schließen Sie das mit ein`/persistent:yes`und`/savecred`Wenn die Verbindung über einen Systemneustart hinweg beibehalten soll. Die spezifischen Befehle, die Sie verwenden, unterscheiden sich je nachdem, ob Sie das Laufwerk für Microsoft Active Directory (AD) -Zugriff oder Gastbenutzerzugriff mounten möchten. Beispiele finden Sie unten.
- Datei-Explorer (Netzlaufwerk zuordnen) — Verwenden Sie den Windows-Datei-Explorer, um Ihre Dateifreigabe einzuhängen Konfigurieren Sie Einstellungen, um anzugeben, ob die Verbindung über Systemneustarts hinweg bestehen bleiben soll, und fordern Sie zur Eingabe von Netzwerkanmeldeinformationen auf.
- PowerShell-Skript — Erstellen Sie ein benutzerdefiniertes PowerShell-Skript zum Einhängen Ihrer Dateifreigabe Abhängig von den Parametern, die Sie im Skript angeben, kann die Verbindung über einen Systemneustart hinweg persistent sein und die Freigabe kann für das Betriebssystem sichtbar oder unsichtbar sein, während es gemountet ist.

> **Note**
>
> Wenn Sie ein Microsoft AD-Benutzer sind, wenden Sie sich an Ihren Administrator, um sicherzustellen, dass Sie Zugriff auf die SMB-Dateifreigabe haben, bevor Sie die Dateifreigabe auf Ihrem lokalen System mounten.

Wenn Sie ein Gastbenutzer sind, stellen Sie sicher, dass Sie das Passwort für das Gastbenutzerkonto besitzen, bevor Sie versuchen, die Dateifreigabe zu aktivieren.

So mounten Sie Ihre SMB-Dateifreigabe für autorisierte Microsoft AD-Benutzer über die Eingabeaufforderung:

1. Stellen Sie sicher, dass der Microsoft AD-Benutzer über die erforderlichen Berechtigungen für die SMB-Dateifreigabe verfügt, bevor Sie die Dateifreigabe auf dem System des Benutzers mounten.
2. Geben Sie an der Eingabeaufforderung Folgendes ein, um die Dateifreigabe einzuhängen:

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

So mounten Sie Ihre SMB-Dateifreigabe mit einer bestimmten Kombination aus Benutzernamen und Kennwort über die Eingabeaufforderung:

1. Stellen Sie sicher, dass das Benutzerkonto Zugriff auf die SMB-Dateifreigabe hat, bevor Sie die Dateifreigabe auf dem System mounten.
2. Geben Sie an der Eingabeaufforderung Folgendes ein, um die Benutzeranmeldeinformationen in Windows Credential Manager zu speichern:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. Geben Sie an der Eingabeaufforderung Folgendes ein, um die Dateifreigabe einzuhängen:

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

So mounten Sie Ihre SMB-Dateifreigabe für Gastbenutzer mit der Eingabeaufforderung:

1. Stellen Sie sicher, dass Sie das Passwort für das Gastbenutzerkonto besitzen, bevor Sie die Dateifreigabe mounten.
2. Geben Sie an der Eingabeaufforderung Folgendes ein, um die Gastanmeldeinformationen im Windows Credential Manager zu speichern:

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

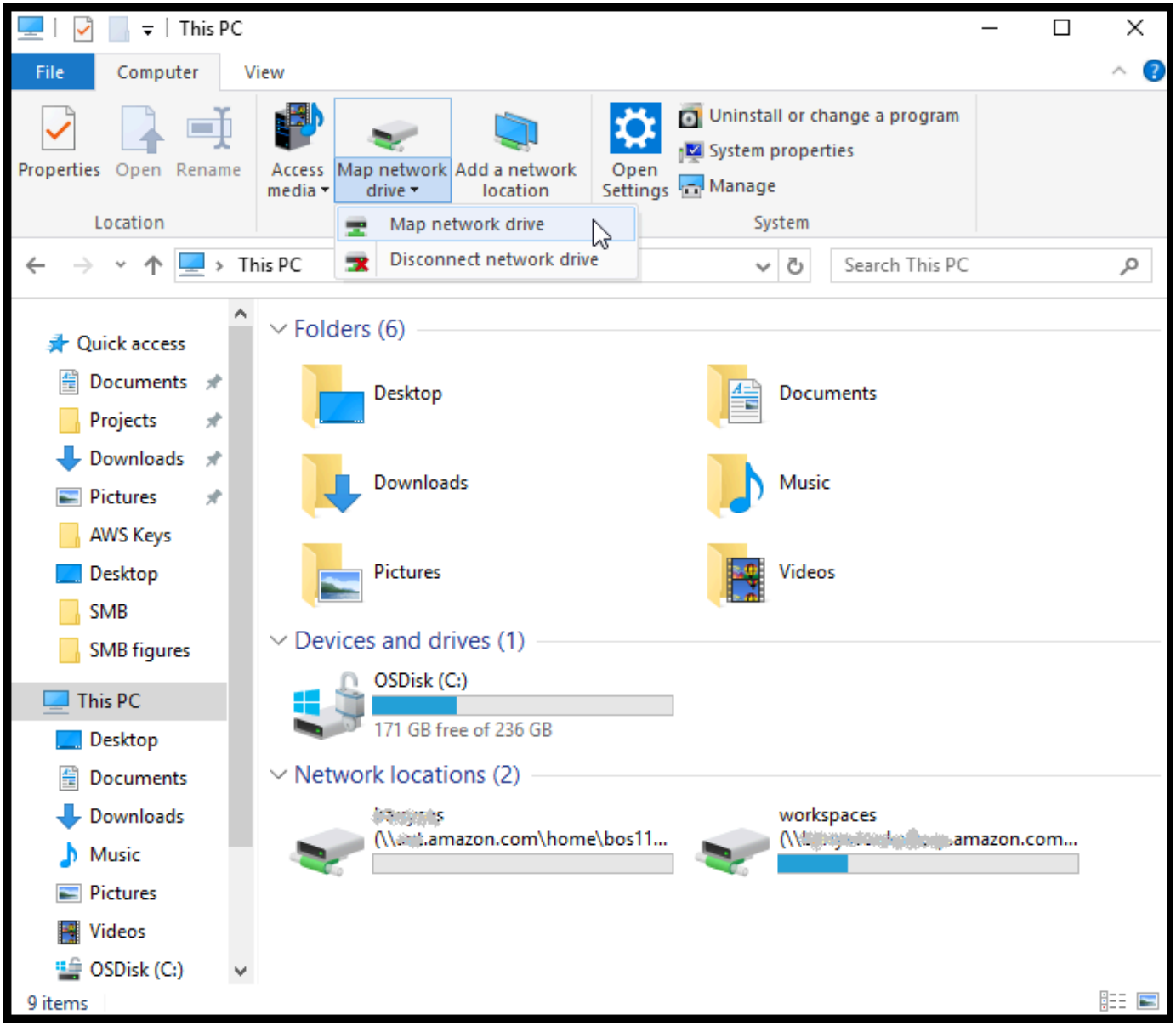
3. Geben Sie an der Eingabeaufforderung Folgendes ein.

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

> **Note**
>
> Beachten Sie beim Mounten von Dateifreigaben Folgendes:
>
> - Möglicherweise haben Sie einen Fall, in dem ein Ordner und ein Objekt in einem Amazon S3 S3-Bucket vorhanden sind und den gleichen Namen haben. Wenn der Objektname keinen abschließenden Schrägstrich enthält, ist nur der Ordner in einem File Gateway sichtbar. Wenn ein Bucket beispielsweise ein Objekt mit dem Namen enthält`test`oder`test/`und ein Ordner mit dem Namen`test/test1`, nur`test/`und`test/test1`sind in einem Datei-Gateway sichtbar.
> - Sofern Sie Ihre Dateifreigabeverbindung nicht so konfigurieren, dass Ihre Benutzeranmeldeinformationen gespeichert und bei Systemneustarts bestehen bleiben, müssen Sie Ihre Dateifreigabe möglicherweise jedes Mal neu starten, wenn Sie Ihr Clientsystem neu starten.

So mounten Sie eine Dateifreigabe mit dem Windows Datei-Explorer

1. Drücken Sie die Windows-Taste und geben Sie **`File Explorer`** in das Feld Search Windows (Windows durchsuchen) ein oder drücken Sie **`Win+E`**.
2. Wählen Sie im Navigationsbereich die Option This PC (Dieser PC) und dann Map Network Drive (Netzwerklaufwerk zuordnen) in Map Network Drive (Netzwerklaufwerk zuordnen) auf der Registerkarte Computer (Computer) aus wie im folgenden Screenshot gezeigt.



3. Wählen Sie im Dialogfeld Map Network Drive (Netzwerklaufwerk zuordnen) einen Laufwerksbuchstaben für Drive (Laufwerk) aus.
4. Geben Sie in Folder (Ordner) ***[File Gateway IP]**[SMB File Share Name]*** ein oder wählen Sie Browse (Durchsuchen) aus, um die SMB-Dateifreigabe im Dialogfeld auszuwählen.
5. (Optional) Wählen Sie Reconnect at sign-up (Beim Anmelden erneut verbinden) aus, wenn der Mountingpunkt nach dem Neustart beibehalten werden soll.
6. (Optional) Wählen Sie Connect using different credentials (Mit anderen Anmeldeinformationen verbinden) aus, wenn Benutzer Microsoft AD-Anmeldeinformationen oder ein Gastkontobenutzer-Passwort eingeben sollen.
7. Klicken Sie auf Finish (Beenden), um den Mounting-Punkt fertigzustellen.

Sie können die Einstellungen für die Dateifreigabe bearbeiten, zulässige und abgelehnte Benutzer und Gruppen bearbeiten und das Gastzugriffspasswort in der Storage Gateway-Managementkonsole ändern. Sie können auch die Daten im Cache der Dateifreigabe aktualisieren und eine Dateifreigabe von der Konsole löschen.

So ändern Sie Ihre SMB-Dateifreigabeeigenschaften

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie im Navigationsbereich File Shares (Dateifreigaben) aus.
3. Wählen Sie auf der Seite File Share (Dateifreigabe) das Kontrollkästchen neben der SMB-Dateifreigabe aus, die Sie ändern möchten.
4. Wählen Sie in Actions (Aktionen) die gewünschte Aktion aus:

   - Wählen Sie Edit file share settings (Dateifreigabeeinstellungen bearbeiten) aus, um den Freigabezugriff zu ändern.
   - Wählen Sie Edit allowed/denied users (Zugelassene/abgelehnte Benutzer bearbeiten) aus, um Benutzer und Gruppen hinzuzufügen oder zu löschen, und geben Sie dann die zugelassenen oder abgelehnten Benutzer und Gruppen in die Felder Allowed Users (Zugelassene Benutzer), Denied Users (Abgelehnte Benutzer), Allowed Groups (Zugelassene Gruppen) und Denied Groups (Abgelehnte Gruppen) ein. Verwenden Sie die Schaltflächen Add Entry (Eintrag hinzufügen), um neue Zugriffsrechte zu erstellen, und die Schaltfläche (X), um den Zugriff zu entfernen.
5. Wenn Sie fertig sind, wählen Sie Speichern.

   Wenn Sie zugelassene Benutzer und Gruppen eingeben, erstellen Sie eine Zulassungsliste. Ohne Zulassungsliste können alle authentifizierten Microsoft AD-Benutzer auf die SMB-Dateifreigabe zugreifen. Alle Benutzer und Gruppen, die als abgelehnt markiert sind, werden einer Verweigerungsliste hinzugefügt und können nicht auf die SMB-Dateifreigabe zugreifen. In Fällen, in denen sich Benutzer oder Gruppen auf der Ablehnungsliste und der Zulassungsliste befinden, hat die Verweigerungsliste Vorrang.

   Sie können auf Ihrer SMB-Dateifreigabe Zugriffskontrolllisten (Access Control Lists, ACLs) aktivieren. Weitere Informationen darüber, wie ACLs aktiviert werden, finden Sie unter Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe.

Nächster Schritt

Testen Sie Ihr S3 File Gateway

Arbeiten mit Dateifreigaben in einem Bucket mit Pre-Exisiting-Objekten

Sie können eine Dateifreigabe in einen Amazon S3 S3-Bucket exportieren, der Objekte enthält, die außerhalb des File Gateways mit NFS oder SMB erstellt wurden. Objekte im Bucket, die außerhalb des Gateways erstellt wurden, werden im NFS- oder SMB-Dateisystem als Dateien angezeigt, wenn Ihre Dateisystem-Clients darauf zugreifen. POSIX (Standard Portable Operating System Interface)-Zugriff und -Berechtigungen werden in der Dateifreigabe verwendet. Wenn Dateien in einen Amazon S3 S3-Bucket zurückschreiben, nehmen die Dateien die Eigenschaften und Zugriffsrechte an, die Sie ihnen geben.

Sie können Objekte jederzeit in einen S3-Bucket hochladen. Damit die Dateifreigabe diese neu hinzugefügten Objekte als Dateien anzeigt, müssen Sie zuerst S3-Bucket aktualisieren. Weitere Informationen finden Sie unter the section called “Aktualisieren von Objekten in Ihrem Amazon S3 S3-Bucket”.

> **Note**
>
> Wir raten davon ab, mehrere Autoren für einen Amazon S3 S3-Bucket zuzulassen. Wenn Sie dies tun, lesen Sie unbedingt den Abschnitt „Kann ich mehrere Autoren für meinen Amazon S3 S3-Bucket haben?“ imFAQ Storage Gatewayaus.

Weitere Informationen dazu, wie Sie Objekten, auf die unter Verwendung von NFS zugegriffen wird, Metadaten zuweisen, finden Sie unter Bearbeiten von Metadaten-Standardwerten in Verwalten Ihres Amazon S3 S3-Datei-Gateways.

Für SMB können Sie eine Freigabe mit Microsoft AD- oder Gast-Zugriff für einen Amazon S3 S3-Bucket mit vorhandenen Objekten exportieren. Objekte, die über eine SMB-Dateifreigabe exportiert werden, erben POSIX-Eigentümerschaft und Berechtigungen aus dem unmittelbar übergeordneten Verzeichnis. Für Objekte unter dem Root-Ordner werden Root-Zugriffskontrolllisten (Access Control Lists, ACL) geerbt. Für Root-ACLs ist der Eigentümer `smbguest` und die Berechtigungen für Dateien sind 666 und für Verzeichnisse 777. Dies gilt für alle Formen des authentifizierten Zugriffs (Microsoft AD und Gast)

Testen Sie Ihr S3 File Gateway

Sie können Dateien und Ordner zum zugeordneten Laufwerk kopieren. Die Dateien werden automatisch in Ihren Amazon S3 S3-Bucket hochgeladen.

So laden Sie Dateien von Ihrem Windows-Client auf Amazon S3 hoch

1. Navigieren Sie auf dem Windows-Client zu dem Laufwerk, auf dem Sie Ihre Dateifreigabe gemountet haben. Dem Namen des Laufwerks ist der Name Ihres S3-Buckets vorangestellt.
2. Kopieren Sie Dateien oder einen Ordner auf das Laufwerk.
3. Navigieren Sie in der Amazon S3 Management Console zum zugewiesenen Bucket. Sie sollten die Dateien und Ordner sehen, die Sie in den angegebenen Amazon S3 S3-Bucket kopiert haben.

   Sie können die erstellte Dateifreigabe in derDateifreigabenRegisterkarte (Registerkarte) in derAWSStorage Gateway Management Console.

Ihr NFS- oder SMB-Client kann Dateien schreiben, lesen, löschen, umbenennen und kürzen.

> **Note**
>
> Ein File Gateway unterstützt das Erstellen von harten oder symbolischen Links für eine Dateifreigabe nicht.

Beachten Sie folgende Punkte im Hinblick auf die Funktionsweise von File Gateways mit S3:

- Lesevorgänge werden vom Read-Through-Cache verarbeitet. Mit anderen Worten: Wenn keine Daten verfügbar ist, werden sie aus S3 abgerufen und zum Cache hinzugefügt.
- Schreibvorgänge werden über optimierte mehrteilige Uploads über einen Zurückschreib-Cache an S3 gesendet.
- Dabei werden sowohl Schreib- als auch Lesevorgänge optimiert: Es werden nur die angeforderten oder geänderten Teile über das Netzwerk übertragen.
- Mit Löschvorgängen werden Objekte aus S3 entfernt.
- Verzeichnisse werden als Ordnerobjekte in S3 verwaltet. Dabei wird dieselbe Syntax verwendet wie in der Amazon S3 S3-Konsole. Sie können leere Verzeichnisse umbenennen.

- Die rekursive Dateisystem-Operationsleistung (z. B. `ls -l`) hängt von der Anzahl der Objekte in Ihrem Bucket ab.

Nächster Schritt

Wie geht es weiter?

Wie geht es weiter?

In den vorhergehenden Abschnitten haben Sie ein File Gateway erstellt und verwendet. Sie haben eine Dateifreigabe gemountet und Ihre Einrichtung getestet.

Andere Abschnitte dieses Handbuchs enthalten Informationen darüber, wie Sie die folgenden Aufgaben ausführen:

- Informationen zum Verwalten Ihres File Gateways finden Sie unter Verwalten Ihres Amazon S3 S3-Datei-Gateways.
- Informationen zum Optimieren Ihres File Gateways finden Sie unter Optimieren der Gateway-Leistung.
- Informationen zum Beheben von Gateway-Problemen finden Sie unter Fehlerbehebung bei Ihrem Gateway.
- Informationen zu Storage Gateway Gateway-Metriken und zur Überwachung der Leistung Ihres Gateways finden Sie unter.

So bereinigen Sie nicht benötigte Ressourcen

Wenn Sie das Gateway als Beispielübung oder Test erstellt haben, sollten Sie es bereinigen, um unerwartete oder unnötige Gebühren zu vermeiden.

So bereinigen Sie nicht benötigte Ressourcen

1. Falls Sie das Gateway nicht weiterhin verwenden möchten, löschen Sie es. Weitere Informationen finden Sie unter Löschen des Gateways über die AWS Storage Gateway-Konsole und Bereinigen zugehöriger Ressourcen.
2. Löschen Sie die Storage Gateway Gateway-VM von Ihrem lokalen Host. Wenn Sie Ihr Gateway auf einer Amazon EC2 EC2-Instance erstellt haben, beenden Sie die Instance.

Aktivieren eines Gateways in einer Virtual Private Cloud

Sie können eine private Verbindung zwischen Ihrer lokalen Software-Appliance und der Cloud-basierten Speicherinfrastruktur herstellen. Anschließend können Sie die Software-Appliance verwenden, um Daten anAWSSpeicher ohne dass Ihr Gateway kommuniziertAWSSpeicher-Services über das öffentliche Internet. Mithilfe des Amazon VPC-Dienstes können Sie startenAWS-Ressourcen in einem benutzerdefinierten virtuellen Netzwerk. Mit einer Virtual Private Cloud (VPC) können Sie Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways, steuern. Weitere Informationen über VPCs finden Sie unterWas ist Amazon VPC?imAmazon VPC User Guideaus.

Um ein Gateway mit einem Storage Gateway -VPC-Endpunkt in Ihrer VPC zu verwenden, gehen Sie wie folgt vor:

- Mit der VPC-Konsole können Sie einen VPC-Endpunkt für Storage Gateway erstellen und die VPC-Endpunkt-ID abrufen. Geben Sie diese VPC-Endpunkt-ID an, wenn Sie das Gateway erstellen und aktivieren.
- Wenn Sie ein File Gateway aktivieren, erstellen Sie einen VPC-Endpunkt für Amazon S3. Geben Sie diesen VPC-Endpunkt an, wenn Sie Dateifreigaben für Ihr Gateway erstellen.
- Wenn Sie ein File Gateway aktivieren, richten Sie einen HTTP-Proxy ein und konfigurieren Sie ihn in der lokalen VM-Konsole des File Gateways. Sie benötigen diesen Proxy für lokale File Gateways, die hypervisorbasiert sind, z. B. solche, die auf VMware, Microsoft HyperV und Linux KVM (Kernel-basierte virtuelle Maschine) basieren. In diesen Fällen benötigen Sie den Proxy, um den Zugriff Ihres Gateways auf private Amazon-S3-Endpunkte außerhalb Ihrer VPC zu ermöglichen. Weitere Informationen zum Konfigurieren eines HTTP-Proxys finden Sie unter Konfigurieren eines HTTP-Proxys

> **Note**
>
> Ihr Gateway muss in derselben Region aktiviert werden, in der Ihr VPC-Endpunkt erstellt wurde.
> Für das File Gateway muss sich der Amazon S3-Speicher, der für die Dateifreigabe konfiguriert ist, in derselben Region befinden, in der Sie den VPC-Endpunkt für Amazon S3 erstellt haben.

Themen

Erstellen eines VPC-Endpunkts für Storage Gateway

Befolgen Sie diese Anweisungen zum Erstellen eines VPC-Endpunkts. Wenn Sie bereits über einen VPC-Endpunkt für Storage Gateway verfügen, können Sie ihn verwenden.

So erstellen Sie einen VPC-Endpunkt für Storage Gateway

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoints (Endpunkte) und anschließend Create Endpoint (Endpunkt erstellen) aus.
3. Auf derErstellen eines Endpunkts-Seite wählenAWSServiceszumServicekategorieaus.
4. Wählen Sie für Service Name (Servicename) `com.amazonaws.`*`region`*`.storagegateway` aus. Beispiel `com.amazonaws.us-east-2.storagegateway`.
5. Wählen Sie in VPC (VPC) Ihre VPC aus und notieren Sie ihre Availability Zones und Subnetze.
6. Stellen Sie sicher, dass Enable Private DNS Name (Privaten DNS-Namen aktivieren) ausgewählt ist.
7. Wählen Sie in Security group (Sicherheitsgruppe) die Sicherheitsgruppe aus, die Sie für Ihre VPC verwenden möchten. Sie können die Standardsicherheitsgruppe akzeptieren. Stellen Sie sicher, dass alle der folgenden TCP-Ports in Ihrer Sicherheitsgruppe zulässig sind:

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

8. Wählen Sie Create endpoint (Endpunkt erstellen). Der Anfangsstatus des Endpunkts ist pending (ausstehend). Wenn der Endpunkt erstellt wurde, notieren Sie die ID des VPC-Endpunkts, den Sie gerade erstellt haben.
9. Wenn der Endpunkt erstellt wurde, wählen Sie Endpoints (Endpunkte) und dann den neuen VPC-Endpunkt aus.
10. Suchen Sie den Abschnitt DNS Names (DNS-Namen) und verwenden Sie den ersten DNS-Namen, der keine Availability Zone angibt. Ihr DNS-Name sieht ungefähr wie folgt aus: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Da Sie nun über einen VPC-Endpunkt verfügen, können Sie Ihr Gateway erstellen.

> **Important**
>
> Wenn Sie ein File Gateway erstellen, müssen Sie auch einen Endpunkt für Amazon S3 erstellen. Führen Sie dieselben Schritte wie im obigen Abschnitt So erstellen Sie einen VPC-Endpunkt für Storage Gateway durch, aber wählen Sie`com.amazonaws.us-east-2.s3`stattdessen unter Dienstname. Anschließend wählen Sie die Routing-Tabelle aus, die dem S3-Endpunkt zugeordnet sein soll, anstelle der Subnetz-/Sicherheitsgruppe. Detaillierte Anweisungen finden Sie unterErstellen eines Gateway-Endpunktsaus.

Einrichten und Konfigurieren eines HTTP-Proxys (nur lokale Datei-Gateways)

Wenn Sie ein File Gateway aktivieren, müssen Sie einen HTTP-Proxy einrichten und ihn in der lokalen VM-Konsole des File Gateways konfigurieren. Sie benötigen diesen Proxy für ein lokales File Gateway, um auf private Amazon S3 S3-Endpunkte von außerhalb Ihrer VPC zuzugreifen. Wenn Sie bereits über einen HTTP-Proxy in Amazon EC2 verfügen, können Sie ihn verwenden. Sie müssen allerdings überprüfen, ob alle der folgenden TCP-Ports in Ihrer Sicherheitsgruppe zulässig sind:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028

- TCP 1031
- TCP 2222

Wenn Sie keinen Amazon EC2 Proxy haben, verwenden Sie das folgende Verfahren, um einen HTTP-Proxy einzurichten und zu konfigurieren.

So richten Sie einen Proxyserver ein

1. Starten Sie ein Amazon EC2 Linux AMI. Wir raten zur Verwendung einer Instance-Familie, die für Netzwerke optimiert ist, z. B. die c5n.large.
2. Mit dem folgenden Befehl können Sie Squid installieren: **`sudo yum install squid`**aus. Dadurch wird eine Standardkonfigurationsdatei in erstellt`/etc/squid/squid.conf`aus.
3. Ersetzen Sie den Inhalt dieser Konfigurationsdatei durch den folgenden Inhalt:

```
#
# Recommended minimum configuration:
#

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

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

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

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

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

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

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

# Squid normally listens to port 3128
http_port 3128

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

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

4. Wenn Sie keine Notwendigkeit haben, den Proxy-Server zu sperren, und keine Änderungen mehr erforderlich sind, aktivieren und starten Sie den Proxy-Server mithilfe der folgenden Befehle. Diese Befehle starten den Server, wenn hochfährt.

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

Sie können jetzt den HTTP-Proxy für das Storage Gateway konfigurieren, um es zu verwenden. Bei der Konfiguration des Gateways für die Verwendung eines Proxys verwenden Sie den Standard-Squid-Port 3128. Die generierte squid.conf-Datei deckt standardmäßig die folgenden erforderlichen TCP-Ports ab:

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

So konfigurieren Sie den HTTP-Proxy mithilfe der lokalen VM-Konsole

1. Melden Sie sich bei der lokalen VM-Konsole des Gateways an. Informationen zum Anmelden finden Sie unter Anmelden an der lokalen Konsole des File Gateways.
2. Wählen Sie im Hauptmenü die Option Configure HTTP proxy (HTTP-Proxy konfigurieren) aus.
3. In derKonfigurationMenü wählenKonfigurieren von HTTP-Proxyaus.
4. Geben Sie den Host-Namen und Port für Ihren Proxy-Server ein.

Detaillierte Informationen zum Konfigurieren eines HTTP-Proxys finden Sie unter Konfigurieren eines HTTP-Proxys.

Zulassen von Datenverkehr zu erforderlichen Ports in Ihrem HTTP-Proxy

Wenn Sie einen HTTP-Proxy verwenden, stellen Sie sicher, dass Sie Datenverkehr von Storage Gateway zu den folgenden aufgelisteten Zielen und Ports zulassen.

Wenn Storage Gateway über die öffentlichen Endpunkte kommuniziert, kommuniziert es mit den folgenden Storage Gateway -Services.

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

> **Important**
>
> Abhängig von Ihrem GatewayAWSRegion, ersetzen*Region*Im Endpunkt mit der entsprechenden Regionszeichenfolge für die Region. Wenn Sie beispielsweise ein Gateway in der Region US-West (Oregon) erstellen, würde der Endpunkt wie folgt aussehen:`storagegateway.us-west-2.amazonaws.com:443`aus.

Wenn Storage Gateway über den VPC-Endpunkt kommuniziert, kommuniziert es mitAWS-Services über mehrere Ports auf dem Storage Gateway VPC-Endpunkt und Port 443 auf dem privaten Amazon S3 S3-Endpunkt.

- TCP-Ports auf dem Storage Gateway-VPC-Endpunkt
  - 443, 1026, 1027, 1028, 1031 und 2222
- TCP-Port auf dem privaten S3-Endpunkt
  - 443

Verwalten Ihres Amazon S3 S3-Datei-Gateways

In den folgenden Abschnitten erhalten Sie Informationen zum Verwalten Ihrer Amazon S3 File Gateway-Ressourcen.

Themen

Hinzufügen einer Dateifreigabe

Nachdem das S3-File Gateway aktiviert wurde und ausgeführt wird, können Sie weitere Dateifreigaben hinzufügen und Zugriff auf Amazon S3 S3-Buckets gewähren. Sie können den Zugriff gewähren, um Buckets in einem anderenAWS-Kontoals Ihre Dateifreigabe. Weitere Informationen zum Hinzufügen einer Dateifreigabe finden Sie unter Erstellen Sie eine Dateifreigabe.

Themen

Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket

Wenn Sie eine Dateifreigabe erstellen, benötigt Ihr Datei-Gateway Zugriff, um Dateien in Ihren Amazon S3 S3-Bucket hochzuladen und Aktionen für alle Access Points oder Virtual Private Cloud (VPC) -Endpunkte auszuführen, die es für die Verbindung mit dem Bucket verwendet. Um diesen Zugriff zu gewähren, geht Ihr Datei-Gateway vonAWS Identity and Access Management(IAM) -Rolle, die mit einer IAM-Richtlinie verknüpft ist, die diesen Zugriff gewährt.

Für die Rolle ist diese IAM-Richtlinie und eine Vertrauensbeziehung zum Security Token Service (STS) erforderlich. Die Richtlinie bestimmt, welche Aktionen die Rolle ausführen kann. Darüber hinaus müssen der S3-Bucket und alle zugehörigen Access Points oder VPC-Endpoints über eine Zugriffsrichtlinie verfügen, mit der die IAM-Rolle darauf zugreifen kann.

Sie können die Rollen- und Zugriffsrichtlinie selbst erstellen oder dies File Gateway überlassen. Erstellt das File Gateway die Richtlinie für Sie, enthält die Richtlinie eine Liste von S3-Aktionen. Weitere Informationen zu -Rollen und Berechtigungen finden Sie unterErstellen einer Rolle zum Delegieren von Berechtigungen an eineAWS-ServiceimIAM User Guideaus.

Im folgenden Beispiel sehen Sie eine Vertrauensrichtlinie, mit der Sie dem File Gateway das Übernehmen einer IAM-Rolle gestatten.

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

Soll keine Richtlinie in Ihrem Namen erstellen, können Sie eine eigene Richtlinie erstellen und diese Richtlinie der Dateifreigabe anfügen. Weitere Information dazu finden Sie unter Erstellen Sie eine Dateifreigabe.

Die folgende Beispielrichtlinie ermöglicht Ihrem File Gateway, alle in der Richtlinie aufgeführten Amazon S3 S3-Aktionen auszuführen. Der erste Teil der Anweisung definiert, dass alle aufgeführten

Aktionen auf den S3-Bucket `TestBucket` angewendet werden dürfen. Der zweite Teil legt fest, dass die aufgeführten Aktionen auf alle Objekte in `TestBucket` angewendet werden dürfen.

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

Die folgende Beispielrichtlinie ähnelt der vorherigen, ermöglicht es Ihrem Datei-Gateway jedoch, Aktionen auszuführen, die für den Zugriff auf einen Bucket über einen Access Point erforderlich sind.

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

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

> **Note**
>
> Wenn Sie Ihre Dateifreigabe über einen VPC-Endpunkt mit einem S3-Bucket verbinden müssen, lesen SieEndpunktrichtlinien für Amazon S3imAWS PrivateLink-Benutzerhandbuchaus.

Dienstübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann der dienstübergreifende Identitätswechsel zu Confused-Deputy-Problem führen. Ein serviceübergreifender Identitätswechsel kann auftreten, wenn ein Service (der aufrufende Service) einen anderen Service aufruft (der aufgerufene Service). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen die Verwendung der globalen Bedingungskontext-Schlüsseln `aws:SourceArn` und `aws:SourceAccount` in ressourcenbasierten Richtlinien, um die Berechtigungen, die AWS Storage Gateway einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken. Wenn Sie

beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der Wert von`aws:SourceArn`muss der ARN des Storage Gateway sein, mit dem Ihre Dateifreigabe verknüpft ist.

Der effektivste Weg, um sich vor dem verwirrten Stellvertreterproblem zu schützen, ist die Verwendung des`aws:SourceArn`globaler Kontextschlüssel mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht wissen oder mehrere Ressourcen angeben, verwenden Sie die Option`aws:SourceArn`globaler Kontextbedingungsschlüssel mit Platzhaltern (*) für die unbekannten Teile des ARN. Zum Beispiel, `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`.

Das folgende Beispiel zeigt, wie Sie`aws:SourceArn`und`aws:SourceAccount`Schlüssel zum globalen Zustandskontext in Storage Gateway, um das verwirrte Deputy Problem zu verhindern.

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

Verwenden einer Dateifreigabe für kontoübergreifenden Zugriff

KontoübergreifendDer Zugriff erfolgt, wenn ein Amazon Web Services Services-Konto und die Benutzer dieses Kontos Zugriff auf Ressourcen eines anderen Amazon Web Services Services-Kontos erhalten. Für File Gateways können Sie eine Dateifreigabe in einem Amazon Web Services Services-Konto verwenden, um auf Objekte in einem Amazon S3 S3-Bucket zuzugreifen, der zu einem anderen Amazon Web Services Services-Konto gehört.

So verwenden Sie eine Dateifreigabe eines Amazon Web Services Services-Kontos, um auf einen S3-Bucket in einem anderen Amazon Web Services Services-Konto zuzugreifen

1. Stellen Sie sicher, dass der S3-Bucket-Besitzer Ihrem Amazon Web Services Services-Konto Zugriff auf den S3-Bucket gewährt hat, auf den Sie zugreifen müssen, und auf die Objekte in diesem Bucket. Weitere Informationen über die Gewährung dieses Zugriffs finden Sie unterBeispiel 2: Bucket-Eigentümer gewährt kontoübergreifende Bucket-imAmazon Simple Storage Service — Benutzerhandbuchaus. Eine Liste der erforderlichen Berechtigungen finden Sie unter Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket.
2. Stellen Sie sicher, dass die von der Dateifreigabe für den Zugriff auf den S3-Bucket verwendete IAM-Rolle über Berechtigungen für Operationen wie `s3:GetObjectAcl` und `s3:PutObjectAcl` verfügt. Stellen Sie außerdem sicher, dass die IAM-Rolle eine Vertrauensrichtlinie enthält, die es dem Konto ermöglicht, diese IAM-Rolle zu übernehmen. Ein Beispiel für eine solche Vertrauensrichtlinie finden Sie unter Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket.

   Wenn die Dateifreigabe für den Zugriff auf den S3-Bucket eine vorhandene Rolle verwendet, sollten Sie Berechtigungen für die Operationen `s3:GetObjectAc` und `s3:PutObjectAcl` einschließen. Außerdem benötigt die Rolle eine Vertrauensrichtlinie, die es dem Konto ermöglicht, diese Rolle anzunehmen. Ein Beispiel für eine solche Vertrauensrichtlinie finden Sie unter Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket.
3. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
4. Wählen Sie Give bucket owner full control (Bucket-Eigentümer volle Kontrolle gewähren) in den Object metadata (Objektmetadaten)-Einstellungen im Dialogfeld Configure file share setting (Dateifreigabeeinstellungen konfigurieren).

Wenn Sie die Dateifreigabe für kontoübergreifenden Zugriff erstellt oder aktualisiert und die Dateifreigabe lokal eingebunden haben, empfehlen wir dringend, die Konfiguration zu testen. Listen

Sie hierzu den Verzeichnisinhalt auf oder schreiben Sie Testdateien und stellen Sie sicher, dass die Dateien als Objekte im S3-Bucket angezeigt werden.

> **Important**
>
> Sie müssen die Richtlinien so einrichten, dass kontoübergreifender Zugriff auf das von der Dateifreigabe verwendete Konto gewährt wird. Wenn Sie dies nicht tun, werden Aktualisierungen der Dateien über lokale Anwendungen nicht auf den Amazon S3 S3-Bucket weitergeleitet, mit dem Sie arbeiten.

Ressourcen

Weitere Informationen zu Zugriffsrichtlinien und Zugriffskontrolllisten finden Sie unter:

Orientierungshilfen für die Verwendung der unterstützten Zugriffsrichtlinienoptionenim Amazon Simple Storage Service — Benutzerhandbuch

Zugriffskontrolllisten (ACL) — Übersichtim Amazon Simple Storage Service — Benutzerhandbuch

Löschen einer Dateifreigabe

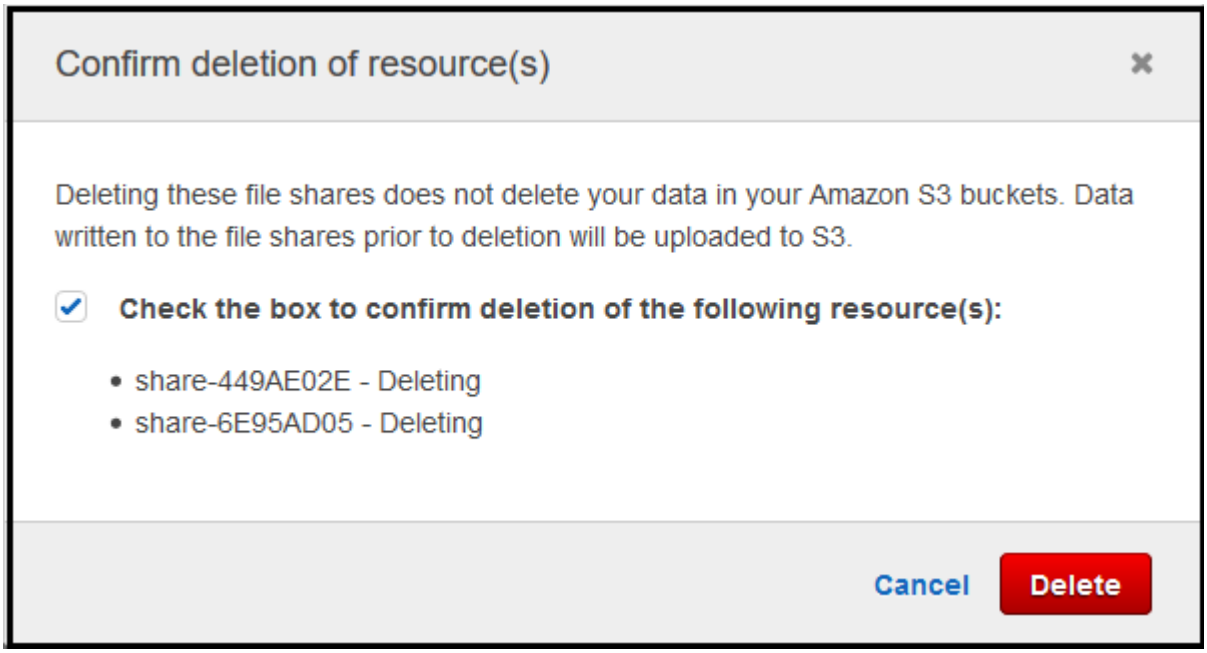
Wenn Sie eine Dateifreigabe nicht mehr benötigen, können Sie sie über die Storage Gateway Gateway-Konsole löschen. Wenn Sie eine Dateifreigabe löschen, wird das Gateway vom Amazon S3 S3-Bucket getrennt, auf den die Dateifreigabe verweist. Der S3-Bucket und seine Inhalte werden jedoch nicht gelöscht.

Wenn Ihr Gateway Daten an einen S3-Bucket hochlädt, während Sie gerade eine Dateifreigabe löschen, wird der Löschvorgang erst dann abgeschlossen, nachdem alle Daten hochgeladen sind. Die Dateifreigabe weist solange den Status DELETING auf, bis alle Daten vollständig hochgeladen sind.

Wenn Sie möchten, dass Ihre Daten vollständig hochgeladen werden, verwenden Sie den nachfolgend beschriebenen Vorgang To delete a file share (Eine direkte Dateifreigabe löschen). Wenn Sie nicht darauf warten möchten, dass Ihre Daten vollständig hochgeladen werden, beachten Sie das Verfahren To forcibly delete a file share (Löschen einer Dateifreigabe erzwingen) unten in diesem Thema.

So löschen Sie eine Dateifreigabe

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie File shares (Dateifreigaben) und wählen Sie die zu löschende Dateifreigabe.
3. Klicken Sie bei Actions (Aktionen) auf Delete file share (Dateifreigabe löschen). Es wird Ihnen das folgende Bestätigungsdialogfeld angezeigt:



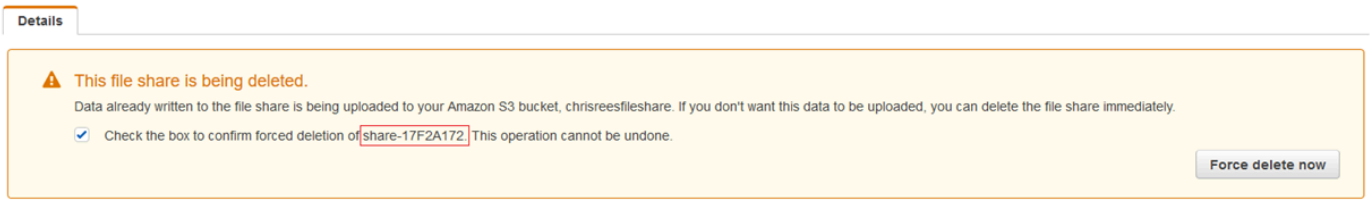
4. Wählen Sie im Bestätigungsdialogfeld das Kontrollkästchen für die Dateifreigabe(n) aus, die Sie löschen möchten, und klicken Sie dann auf Delete (Löschen).

In bestimmten Fällen möchten Sie möglicherweise nicht warten, bis alle in Dateien auf der NFS (Network File System)-Dateifreigabe geschriebenen Daten hochgeladen wurden, bevor Sie die Dateifreigabe löschen. Zum Beispiel wenn Sie absichtlich Daten verwerfen möchten, die zwar geschrieben wurden, aber noch nicht hochgeladen wurden. Oder wenn beispielsweise der Amazon S3-Bucket oder Objekte, die die Dateifreigabe stützen, bereits gelöscht wurden, sodass das Hochladen der angegebenen Daten nicht mehr möglich ist.

In diesen Fällen können Sie die Dateifreigabe gewaltsam löschen, indem SieAWS Management Consoleoder das`DeleteFileShare`API-Operation. Diese Operation bricht den Uploadvorgang ab. Wenn dies der Fall ist, geht die Dateifreigabe in den Status FORCE_DELETING über. Zum erzwungenen Löschen einer Dateifreigabe von der Konsole siehe das folgende Verfahren.

So erzwingen Sie die eine Dateifreigabe

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie File shares (Dateifreigaben) und wählen Sie die Dateifreigabe, bei der Sie das Löschen erzwingen möchten, und warten Sie einige Sekunden. Eine Löschmeldung wird auf der Registerkarte Details angezeigt.



> **Note**
>
> Sie können die Löschoperation nicht rückgängig machen.

3. Überprüfen Sie in der Meldung, die auf der Registerkarte Details angezeigt wird, die ID der Dateifreigabe, die Sie zwangsweise löschen möchten. Wählen Sie das Bestätigungsfeld und anschließend Force delete now (Löschen jetzt erzwingen) aus.

Sie können auch die API-Operation DeleteFileShare verwenden, um die Dateifreigabe zwangsweise zu löschen.

Bearbeiten von Einstellungen für Ihre NFS-Dateifreigabe

Sie können die Speicherklasse für Ihren Amazon S3 S3-Bucket, den Namen der Dateifreigabe, die Objektmetadaten, die Squash-Level, den Export als und die Einstellungen für die automatische Cache-Aktualisierung bearbeiten.

> **Note**
>
> Sie können eine vorhandene Dateifreigabe nicht bearbeiten, um auf einen neuen Bucket oder Access Point zu verweisen oder die VPC-Endpunkteinstellungen zu ändern. Sie können diese Einstellungen nur konfigurieren, wenn Sie eine neue Dateifreigabe erstellen.

So bearbeiten Sie die Dateifreigabeeinstellungen

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie die Option File shares (Dateifreigaben) und wählen Sie dann die Dateifreigabe, die Sie aktualisieren möchten.
3. FürAktionen, wählenBearbeiten von -Einstellungenaus.
4. Führen Sie eine oder mehrere der folgenden Aktionen aus:

   - (Optional) FürName der Dateifreigabeein, geben Sie einen neuen Namen für die Dateifreigabe ein.
   - Wählen Sie unter Audit logs (Prüfungsprotokolle) eine der folgenden Optionen aus:
     - Klicken Sie aufDisable logging (Protokollierung deaktivieren)um die Protokollierung zu deaktivieren.
     - Klicken Sie aufEine neue Protokollgruppe erstellenum ein neues Prüfungsprotokoll zu erstellen.
     - Klicken Sie aufVerwenden einer vorhandenen ProtokollgruppeWählen Sie und dann ein vorhandenes Prüfungsprotokoll aus der Liste aus.

     Weitere Informationen zu Auditprotokollen finden Sie unter Verstehen von Datei-Gateway-Audit.
   - (Optional) FürAutomatisierte Cache-Aktualisierung von S3, aktivieren Sie das Kontrollkästchen und legen Sie die Zeit in Tagen, Stunden und Minuten fest, um den Cache der Dateifreigabe mit Time To Live (TTL) zu aktualisieren. TTL ist die Zeitspanne seit der letzten Aktualisierung. Nach Ablauf des TTL-Intervalls führt der Zugriff auf das Verzeichnis dazu, dass das Datei-Gateway den Inhalt dieses Verzeichnisses zuerst aus dem Amazon S3 S3-Bucket aktualisiert.
   - (Optional) FürBenachrichtigung zum Hochladen von, aktivieren Sie das Kontrollkästchen, das benachrichtigt werden soll, wenn eine Datei vom S3 File Gateway vollständig auf S3 hochgeladen wurde. Legen Sie den Wert fürZeit abgewickeltin Sekunden, um die Anzahl der Sekunden zu steuern, die nach dem letzten Zeitpunkt gewartet werden müssen, den ein Client in eine Datei geschrieben hat, bevor ein`ObjectUploaded`-Benachrichtigung. Da Clients viele kleine Schreibvorgänge in Dateien vornehmen können, legen Sie diesen Parameter am besten so lange wie möglich fest, um zu vermeiden, dass mehrere Benachrichtigungen für dieselbe Datei in einem kleinen Zeitraum generiert werden. Weitere Informationen finden Sie unter Benachrichtigung zum Hochladen von Dateien.

> **Note**
>
> Diese Einstellung hat keinen Einfluss auf den Zeitpunkt des Hochladens des Objekts auf S3, nur auf den Zeitpunkt der Benachrichtigung.

- FürSpeicherklasse für neue ObjekteWählen Sie eine Speicherklasse aus, die für neue Objekte verwendet werden soll, die in Ihrem Amazon S3 S3-Bucket erstellt werden:
  - Wählen Sie S3 Standard (S3-Standard) aus, um Ihre häufig aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind. Weitere Informationen zur S3-Speicherklasse Standard finden Sie unterSpeicherklassen für Objekte mit häufigem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
  - Wählen Sie S3 Intelligent-Tiering, um die Speicherkosten zu optimieren, indem Sie Daten automatisch zur kostengünstigsten Speicherzugriffsstufe verschieben. Weitere Informationen zur S3-Intelligent-Tiering-Speicherklasse finden Sie unterSpeicherklasse, die häufig und weniger häufig verwendete Objekte optimiertimAmazon Simple Storage Service — Benutzerhandbuchaus.
  - Wählen Sie S3 Standard-IA (S3-Standard-IA) aus, um Ihre selten aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind. Weitere Informationen zur S3-Speicherklasse S3 Standard-IA-Speicherklasse finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
  - Wählen Sie S3 One Zone-IA (S3 One Zone-IA) aus, um Ihre selten aufgerufenen Objektdaten in einer einzigen Availability Zone zu speichern. Weitere Informationen zur S3 One Zone-IA-Speicherklasse finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
- Wählen Sie in Object metadata (Objektmetadaten) die Metadaten aus, die Sie verwenden möchten:
  - Wählen Sie Guess MIME type (MIME-Typ bestimmen) aus, um die Bestimmung des MIME-Typs für hochgeladene Objekte basierend auf Dateierweiterungen zu aktivieren.
  - Wählen Sie Give bucket owner full control (Bucket-Eigentümer volle Kontrolle gewähren) aus, um dem Eigentümer des S3-Buckets, der der Network File System (NFS)- oder Server Message Block (SMB)-Dateifreigabe der Datei zugeordnet ist, volle Kontrolle zu geben. Weitere Informationen dazu, wie Sie mit Ihrer Dateifreigabe auf Objekte in einem Bucket

eines anderen Kontos zugreifen, finden Sie unter Verwenden einer Dateifreigabe für kontoübergreifenden Zugriff.

- Wählen Sie Enable requester pays (Zahlung durch den Anforderer aktivieren) aus, wenn Sie diese Dateifreigabe in einem Bucket verwenden, bei dem der Anfordernde oder Abrufende anstelle des Bucket-Eigentümers für den Zugriff bezahlt. Weitere Informationen finden Sie unter Anforderer bezahlt Buckets.

- Wählen Sie für Squash level (Squash-Level) die gewünschte Squash-Level-Einstellung für die NFS-Dateifreigabe aus und klicken Sie dann auf Save (Speichern).

> **Note**
>
> Sie können eine Squash-Level-Einstellung nur für NFS-Dateifreigaben auswählen. SMB-Dateifreigaben verwenden keine Squash-Einstellungen.

Folgende Werte sind möglich:

- Root squash (default) – Der Zugriff für den Remote-Superuser (Root) wird UID (65534) und GID (65534) zugeordnet.
- No root squash (Kein Root-Squash): Der Remote-Superuser (Root) erhält Zugriff als Root.
- All squash – Alle Benutzerzugriffe werden UID (65534) und GID (65534) zugeordnet.

Der Standardwert für das Squash-Level ist Root squash (Root-Squash).

- FürExportieren von alsWählen Sie eine Option für Ihre Dateifreigabe aus. Der Standardwert ist Read-write (Lesen/Schreiben).

> **Note**
>
> Für Dateifreigaben, die auf einem Microsoft Windows-Client bereitgestellt sind, wenn SieRead-onlyzumExportieren von alsangezeigt werden, wird Ihnen möglicherweise eine Fehlermeldung zu einem unerwarteten Fehler angezeigt, der das Erstellen des Ordners verhindert. Bei diesem Fehler handelt es sich um ein bekanntes Problem mit NFS Version 3. Sie können die Meldung ignorieren.

5. Wählen Sie Save (Speichern) aus.

Bearbeiten der Metadaten-Standardwerte für Ihre NFS-Dateifreigabe

Wenn Sie keine Metadatenwerte für Ihre Dateien oder Verzeichnisse in Ihrem Bucket festlegen, legt das S3 File Gateway Standardmetadatenwerte fest. Diese Werte umfassen Unix-Berechtigungen für Dateien und Ordner. Sie können die Metadaten-Standardwerte auf der Storage Gateway Gateway-Konsole bearbeiten.

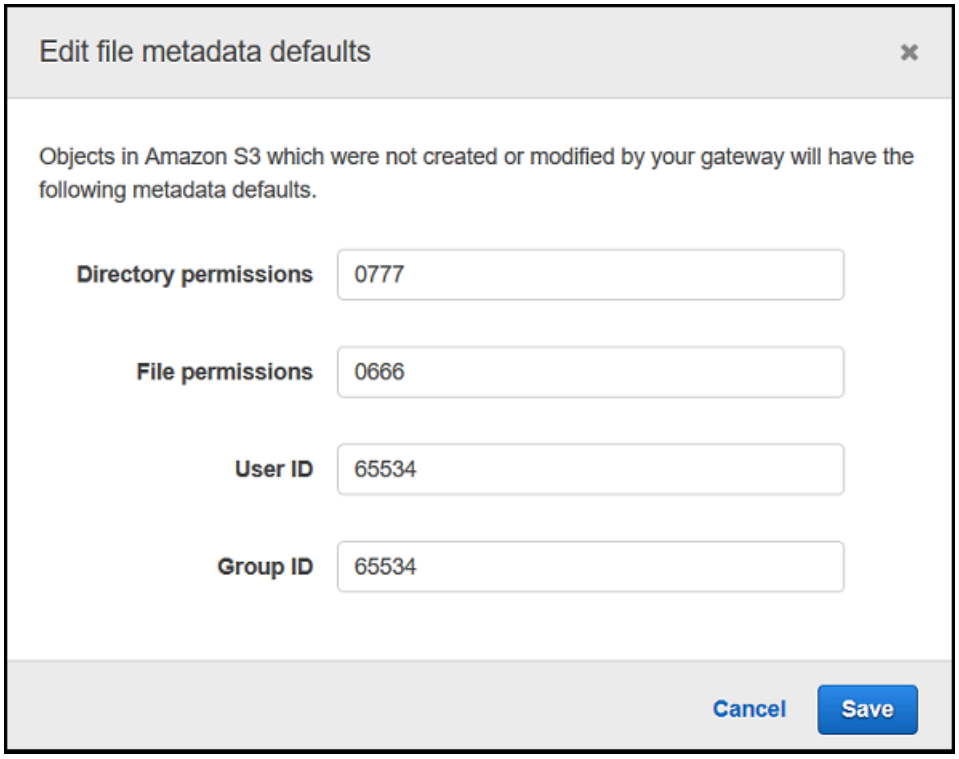
Wenn das S3 File Gateway Dateien und Ordner in Amazon S3 speichert, werden die Unix-Dateiberechtigungen in Objektmetadaten gespeichert. Wenn das S3 File Gateway Objekte erkennt, die nicht vom S3 File Gateway gespeichert wurden, werden diesen Objekten Unix-Standarddateiberechtigungen zugewiesen. Die folgende Tabelle enthält die Unix-Standardberechtigungen.

Metadaten	Description
Verzeichnisberechtigungen	Der Unix-Verzeichnismodus in der Form „nnnn“. Beispiel: „0666“ stellt den Zugriffsm odus für alle Verzeichnisse in der Dateifreigabe dar. Der Standardwert lautet 0777.
Dateiberechtigungen	Der Unix-Dateimodus in der Form „nnnn“. Beispiel: „0666“ stellt den Dateimodu s innerhalb der Dateifreigabe dar. Der Standardwert lautet 0666.
Benutzer-ID	Die Standard-Eigentümer-ID für Dateien in der Dateifreigabe. Der Standardwert lautet 65534.
Gruppen-ID	Die Standard-Gruppen-ID für die Dateifreigabe. Der Standardwert lautet 65534.

So bearbeiten Sie Metadaten-Standardwerte

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.

2. Wählen Sie die Option File shares (Dateifreigaben) und wählen Sie dann die Dateifreigabe, die Sie aktualisieren möchten.
3. Wählen Sie für Actions (Aktionen) die Option Edit file metadata defaults (Standardwerte für Dateimetadaten bearbeiten).
4. Geben Sie im Dialogfeld Edit file metadata defaults (Standardwerte für Dateimetadaten bearbeiten) die Metadateninformationen an und wählen Sie Save (Speichern).



Bearbeiten der Zugriffseinstellungen für Ihre NFS-Dateifreigabe

Wir empfehlen das Ändern der zulässigen NFS-Client-Einstellungen für die NFS-Dateifreigabe. Andernfalls kann jeder beliebige Client in Ihrem Netzwerk Ihre Dateifreigabe mounten.

So bearbeiten Sie NFS-Zugriffseinstellungen

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie die Option File shares (Dateifreigaben) aus und wählen Sie dann die NFS-Dateifreigabe, die Sie bearbeiten möchten.
3. Wählen Sie für Actions (Aktionen) die Option Edit share access settings (Freigabezugriffseinstellungen bearbeiten).

4. In derBearbeiten von zulässigen ClientsWählen Sie das DialogfeldEintrag hinzufügenGeben Sie die IP-Adresse oder CIDR-Notation für die Clients an, die Sie zulassen möchten, und wählen Sie dannSaveaus.

Bearbeiten von SMB-Einstellungen für ein Gateway

Mit den SMB-Einstellungen auf Gateway-Ebene können Sie die Sicherheitsstrategie, die Active Directory-Authentifizierung, den Gastzugriff, lokale Gruppenberechtigungen und die Sichtbarkeit der Dateifreigabe für die SMB-Dateifreigaben auf einem Gateway konfigurieren.

So bearbeiten Sie SMB-Einstellungen auf Gateway-Ebene

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Klicken Sie auf-GatewaysWählen Sie und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Von derAktionenWählen Sie das Dropdown-MenüBearbeiten von SMB-EinstellungenWählen Sie und anschließend die Einstellungen aus, die Sie bearbeiten möchten.

Weitere Informationen finden Sie in den folgenden Themen.

Themen

- Festlegen einer Sicherheitsstufe für Ihr Gateway
- Verwenden von Active Directory zum Authentifizieren von Benutzern
- Gewähren des Gastzugriffs auf Ihre Dateifreigabe
- Konfigurieren Sie lokale Gruppen für Ihr Gateway
- Festlegen der Sichtbarkeit von Datei

Festlegen einer Sicherheitsstufe für Ihr Gateway

Durch die Verwendung eines S3-File Gateways können Sie eine Sicherheitsstufe für Ihr Gateway angeben. Durch die Angabe dieser Sicherheitsstufe können Sie festlegen, ob für Ihr Gateway Server Message Block (SMB)-Signierung oder SMB-Verschlüsselung erforderlich sein soll oder ob Sie SMB-Version 1 aktivieren möchten.

So konfigurieren Sie die Sicherheitsstufe

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Klicken Sie auf-GatewaysWählen Sie und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Von derAktionenWählen Sie das Dropdown-MenüBearbeiten von SMB-Einstellungenund anschließend ausSMB-Sicherheitseinstellungenaus.
4. Wählen Sie für Security level (Sicherheitsstufe) eine der folgenden Optionen aus:

> **Note**
>
> Diese Einstellung wird in der API-Referenz als `SMBSecurityStrategy` bezeichnet. Eine höhere Sicherheitsstufe kann sich negativ auf die Leistung auswirken.

- Durchsetzen der Verschlüsselung- Wenn Sie diese Option auswählen, erlaubt S3 File Gateway nur Verbindungen von SMBv3-Clients, bei denen die Verschlüsselung aktiviert ist. Diese Option wird für Umgebungen, die sensible Daten verarbeiten, dringend empfohlen. Diese Option funktioniert mit SMB Clients auf Microsoft Windows 8, Windows Server 2012 oder höher.
- Unterzeichnung erzwingen- Wenn Sie diese Option auswählen, erlaubt S3 File Gateway nur Verbindungen von SMBv2- oder SMBv3-Clients, bei denen die Signierung aktiviert ist. Diese Option funktioniert mit SMB Clients auf Microsoft Windows Vista, Windows Server 2008 oder höher.
- Aushandlung des Kunden- Wenn Sie diese Option auswählen, werden Anfragen basierend darauf, was vom Client ausgehandelt wurde, gestellt. Diese Option wird empfohlen, wenn Sie die Kompatibilität zwischen verschiedenen Clients in Ihrer Umgebung maximieren möchten.

> **Note**
>
> Bei Gateways, die vor dem 20. Juni 2019 aktiviert wurden, ist die Standardsicherheitsstufe Client negotiated (Von Client ausgehandelt).
> Für Gateways, die am 20. Juni 2019 und später aktiviert wurden, ist die standardmäßige Sicherheitsstufe Enforce encryption (Verschlüsselung erzwingen.

5. Wählen Sie Save (Speichern) aus.

Verwenden von Active Directory zum Authentifizieren von Benutzern

Um das Active Directory Ihres Unternehmens für den benutzerauthentifizierten Zugriff auf die SMB-Dateifreigabe zu verwenden, bearbeiten Sie die SMB-Einstellungen für das Gateway mit Ihren Microsoft AD-Domain-Anmeldeinformationen. Dadurch kann sich das Gateway mit der Active Directory-Domain verbinden und Mitglieder der Domain haben Zugriff auf die SMB-Dateifreigabe.

> **Note**
>
> benutzenAWS Directory Serviceerstellen können, können Sie einen gehosteten Active Directory-Domain-Service imAWS Cloudaus.

Jeder, der das richtige Passwort angibt, erhält Gastzugriff auf die SMB-Dateifreigabe.

Sie können Zugriffskontrolllisten (Access Control Lists, ACLs) auch auf Ihrer SMB-Dateifreigabe aktivieren. Weitere Informationen darüber, wie ACLs aktiviert werden, finden Sie unter Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe.

So aktivieren Sie die Active Directory-Authentifizierung

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Klicken Sie auf-GatewaysWählen Sie und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Von derAktionenWählen Sie im Dropdown-MenüBearbeiten von SMB-Einstellungenund anschließend ausActive Directory-Einstellungenaus.
4. Geben Sie für Domain name (Domain-Name) die Domäne an, mit der sich das Gateway verbinden soll. Sie können einer Domäne über deren IP-Adresse oder Organisationseinheit beitreten. Eine Organisationseinheit ist ein Active Directory-Unterabschnitt zur Aufnahme von Benutzern, Gruppen, Computern und anderen Organisationseinheiten.

> **Note**
>
> Wenn Ihr Gateway einem Active Directory-Verzeichnis nicht beitreten kann, versuchen Sie, mithilfe der API-Operation JoinDomain über die IP-Adresse des Verzeichnisses beizutreten.

> **Note**
>
> Für Active Directory status (Active Directory-Status) wird Detached (Getrennt) angezeigt, wenn ein Gateway noch nie einer Domäne beigetreten ist.

5. Geben Sie den Domain-Benutzer und das Domain-Passwort an und klicken Sie dann auf Save (Speichern).

   Eine Meldung am oberen Rand des Abschnitts Gateways der Konsole gibt an, dass sich das Gateway erfolgreich mit der AD-Domain verbunden hat.

So schränken Sie den Dateifreigabezugriff auf bestimmte AD-Benutzer und -Gruppen ein

1. Wählen Sie in der Storage Gateway Gateway-Konsole die Dateifreigabe aus, auf die Sie den Zugriff einschränken möchten.
2. Von derAktionenWählen Sie im Dropdown-MenüEinstellungen für den Zugriff auf Dateifreigabe bearbeitenaus.
3. In derZugriff auf Benutzer- und Gruppen-DateifreigabeWählen Sie Ihre Einstellungen aus.

   FürZulässige Benutzer und Gruppen, wählenZulässigen Benutzer hinzufügenoderHinzufügen einer zulässigen Gruppeund geben Sie einen AD-Benutzer oder eine Gruppe ein, die Zugriff auf die Dateifreigabe gewähren soll. Wiederholen Sie diesen Vorgang, um so viele Benutzer und Gruppen wie nötig zuzulassen.

   FürBenutzer und Gruppen verweigert, wählenBenutzer hinzufügenoderHinzufügen einer abgelehnten Gruppeund geben Sie einen AD-Benutzer oder eine Gruppe ein, die Zugriff auf die Dateifreigabe verweigern soll. Wiederholen Sie diesen Vorgang, um so viele Benutzer und Gruppen wie nötig abzulehnen.

> **Note**
>
> DieZugriff auf Benutzer- und Gruppen-Dateifreigabewird nur angezeigt, wennActive Directoryist ausgewählt.
> Geben Sie nur den AD-Benutzernamen oder -Gruppennamen ein. Der Domänenname für das spezifische AD, mit dem das Gateway verbunden wird, geht aus der Mitgliedschaft des Gateways hervor.
> Wenn Sie keine zulässigen oder verweigerten Benutzer oder Gruppen angeben, kann jeder authentifizierte AD-Benutzer die Dateifreigabe exportieren.

4. Nachdem Sie die Einträge hinzugefügt haben, wählen Sie Save (Speichern).

Gewähren des Gastzugriffs auf Ihre Dateifreigabe

Wenn Sie nur Gastzugriff erteilen möchten, muss das S3 File Gateway nicht Teil einer Microsoft AD-Domäne sein. Sie können auch ein S3-File Gateway verwenden, das ein Mitglied einer AD-Domäne ist, um Dateifreigaben mit Gastzugriff zu erstellen. Bevor Sie eine Dateifreigabe mithilfe von Gastzugriff erstellen, müssen Sie das Standardpasswort ändern.

So ändern Sie das Passwort für den Gastzugriff

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Klicken Sie auf-GatewaysWählen Sie und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Von derAktionenWählen Sie im Dropdown-MenüBearbeiten von SMB-Einstellungenund anschließend ausEinstellungen für den Gastzugriffaus.
4. FürGäste-Passwort, geben Sie ein Passwort ein und wählen Sie dannSaveaus.

Konfigurieren Sie lokale Gruppen für Ihr Gateway

Mit den Einstellungen für lokale Gruppen können Sie Active Directory-Benutzern oder -Gruppen spezielle Berechtigungen für die SMB-Dateifreigaben auf Ihrem Gateway erteilen.

Sie können die Einstellungen für lokale Gruppen verwenden, um Gateway-Admin-Berechtigungen zuzuweisen. Gateway-Administratoren können das Microsoft Management Console-Snap-In für freigegebene Ordner verwenden, um geöffnete und gesperrte Dateien zu erzwingen.

> **Note**
>
> Sie müssen mindestens einen Gateway-Admin-Benutzer oder eine Gruppe hinzufügen, bevor Sie Ihr Gateway einer Active Directory-Domäne beitreten können.

So weisen Sie Gateway-Admins zu

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Klicken Sie auf-GatewaysWählen Sie und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Von derAktionenWählen Sie das Dropdown-MenüBearbeiten von SMB-Einstellungenund anschließend ausEinstellungen als lokaler Konzernaus.
4. In derEinstellungen als lokaler KonzernWählen Sie Ihre Einstellungen aus. Dieser Abschnitt wird nur für Dateifreigaben angezeigt, die Active Directory verwenden.

   FürGateway-Administratoren, fügen Sie Active Directory-Benutzer und Gruppen hinzu, denen Sie lokalen Gateway-Admin-Berechtigungen erteilen möchten. Fügen Sie einen Benutzer oder eine Gruppe pro Zeile hinzu, einschließlich des Domänennamens. Zum Beispiel, **`corp\Domain Admins`**. Um zusätzliche Zeilen zu erstellen, wählen SieNeuen Gateway Admin hinzufügenaus.

   > **Note**
   >
   > Das Bearbeiten von Gateway-Administratoren trennt alle SMB-Dateifreigaben und verbindet sie erneut.

5. Klicken Sie aufSpeichern Sie die Änderungenund anschließend ausFortsetzenum die angezeigte Warnmeldung zu bestätigen.

Festlegen der Sichtbarkeit von Datei

Die Sichtbarkeit der Dateifreigabe steuert, ob die Freigaben auf einem Gateway sichtbar sind, wenn Sie Aktien an Benutzer notieren.

So legen Sie Sichtbarkeit der Dateifreigabe

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Klicken Sie auf-GatewaysWählen Sie und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Von derAktionenWählen Sie im Dropdown-MenüBearbeiten von SMB-Einstellungenund anschließend ausEinstellungen für die Sichtbarkeit von Dateiaus.
4. FürSichtbarkeitsstatusaktivieren Sie das Kontrollkästchen, damit die Freigaben auf diesem Gateway angezeigt werden, wenn Aktien an Benutzer angeboten werden. Lassen Sie das Kontrollkästchen deaktiviert, damit die Freigaben auf diesem Gateway nicht angezeigt werden, wenn Sie Aktien an Benutzer anbieten.

Bearbeiten von Einstellungen für Ihre SMB-Dateifreigabe

Nachdem Sie eine SMB-Dateifreigabe erstellt haben, können Sie die Speicherklasse für Ihren Amazon S3 S3-Bucket, Objektmetadaten, Groß- und Kleinschreibung, zugriffsbasierte Aufzählung, Überwachungsprotokolle, automatisierte Cache-Aktualisierung und den Export als Einstellungen für Ihre Dateifreigabe bearbeiten.

> **Note**
>
> Sie können eine vorhandene Dateifreigabe nicht bearbeiten, um auf einen neuen Bucket oder Access Point zu verweisen oder die VPC-Endpunkteinstellungen zu ändern. Sie können diese Einstellungen nur konfigurieren, wenn Sie eine neue Dateifreigabe erstellen.

Bearbeiten von SMB-Dateifreigabeeinstellungen

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.

2. Wählen Sie die Option File shares (Dateifreigaben) und wählen Sie dann die Dateifreigabe, die Sie aktualisieren möchten.
3. FürAktionen, wählenBearbeiten von -Einstellungenaus.
4. Führen Sie eine oder mehrere der folgenden Aktionen aus:

   - (Optional) FürName der Dateifreigabeein, geben Sie einen neuen Namen für die Dateifreigabe ein.
   - Wählen Sie unter Audit logs (Prüfungsprotokolle) eine der folgenden Optionen aus:
     - Klicken Sie aufDisable logging (Protokollierung deaktivieren)um die Protokollierung zu deaktivieren.
     - Klicken Sie aufEine neue Protokollgruppe erstellenum ein neues Prüfungsprotokoll zu erstellen.
     - Klicken Sie aufVerwenden einer vorhandenen ProtokollgruppeWählen Sie und dann ein vorhandenes Prüfungsprotokoll aus der Liste aus.

     Weitere Informationen zu Auditprotokollen finden Sie unter Verstehen von Datei-Gateway-Audit.
   - (Optional) FürAutomatisierte Cache-Aktualisierung von S3 nach, aktivieren Sie das Kontrollkästchen und legen Sie die Zeit in Tagen, Stunden und Minuten fest, um den Cache der Dateifreigabe mit Time To Live (TTL) zu aktualisieren. TTL ist die Zeitspanne seit der letzten Aktualisierung. Nach Ablauf des TTL-Intervalls führt der Zugriff auf das Verzeichnis dazu, dass das Datei-Gateway den Inhalt dieses Verzeichnisses zuerst aus dem Amazon S3 S3-Bucket aktualisiert.
   - (Optional) FürBenachrichtigung zum Hochladen von, aktivieren Sie das Kontrollkästchen, das benachrichtigt werden soll, wenn eine Datei vom S3 File Gateway vollständig auf S3 hochgeladen wurde. Legen Sie den Wert fürZeit abgewickeltin Sekunden, um die Anzahl der Sekunden zu steuern, die nach dem letzten Zeitpunkt gewartet werden müssen, den ein Client in eine Datei geschrieben hat, bevor ein`ObjectUploaded`-Benachrichtigung. Da Clients viele kleine Schreibvorgänge in Dateien vornehmen können, legen Sie diesen Parameter am besten so lange wie möglich fest, um zu vermeiden, dass mehrere Benachrichtigungen für dieselbe Datei in einem kleinen Zeitraum generiert werden. Weitere Informationen finden Sie unter Benachrichtigung zum Hochladen von Dateien.

> **Note**
>
> Diese Einstellung hat keinen Einfluss auf den Zeitpunkt des Hochladens des Objekts auf S3, nur auf den Zeitpunkt der Benachrichtigung.

- FürSpeicherklasse für neue ObjekteWählen Sie eine Speicherklasse aus, die für neue Objekte verwendet werden soll, die in Ihrem Amazon S3 S3-Bucket erstellt werden:
  - Wählen Sie S3 Standard (S3-Standard) aus, um Ihre häufig aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind. Weitere Informationen zur S3-Speicherklasse Standard finden Sie unterSpeicherklassen für Objekte mit häufigem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
  - Wählen Sie S3 Intelligent-Tiering, um die Speicherkosten zu optimieren, indem Sie Daten automatisch zur kostengünstigsten Speicherzugriffsstufe verschieben. Weitere Informationen zur S3-Intelligent-Tiering-Speicherklasse finden Sie unterSpeicherklasse, die häufig und weniger häufig verwendete Objekte optimiertimAmazon Simple Storage Service — Benutzerhandbuchaus.
  - Wählen Sie S3 Standard-IA (S3-Standard-IA) aus, um Ihre selten aufgerufenen Objektdaten redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind. Weitere Informationen zur S3-Speicherklasse S3 Standard-IA-Speicherklasse finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
  - Wählen Sie S3 One Zone-IA (S3 One Zone-IA) aus, um Ihre selten aufgerufenen Objektdaten in einer einzigen Availability Zone zu speichern. Weitere Informationen zur S3 One Zone-IA-Speicherklasse finden Sie unterSpeicherklassen für Objekte mit seltenem ZugriffimAmazon Simple Storage Service — Benutzerhandbuchaus.
- Wählen Sie in Object metadata (Objektmetadaten) die Metadaten aus, die Sie verwenden möchten:
  - Wählen Sie Guess MIME type (MIME-Typ bestimmen) aus, um die Bestimmung des MIME-Typs für hochgeladene Objekte basierend auf Dateierweiterungen zu aktivieren.
  - Wählen Sie Give bucket owner full control (Bucket-Eigentümer volle Kontrolle gewähren) aus, um dem Eigentümer des S3-Buckets, der der Network File System (NFS)- oder Server Message Block (SMB)-Dateifreigabe der Datei zugeordnet ist, volle Kontrolle zu geben. Weitere Informationen zum Verwenden der Dateifreigabe für den Zugriff auf Objekte in

einem Bucket eines anderen Kontos finden Sie unterVerwenden einer Dateifreigabe für kontoübergreifenden Zugriffaus.

- Wählen Sie Enable requester pays (Zahlung durch den Anforderer aktivieren) aus, wenn Sie diese Dateifreigabe in einem Bucket verwenden, bei dem der Anfordernde oder Abrufende anstelle des Bucket-Eigentümers für den Zugriff bezahlt. Weitere Informationen finden Sie unter Anforderer bezahlt Buckets.

- FürExportieren von alsWählen Sie eine Option für Ihre Dateifreigabe aus. Der Standardwert ist Read-write (Lesen/Schreiben).

> **Note**
>
> Für Dateifreigaben, die auf einem Microsoft Windows-Client bereitgestellt sind, wenn SieRead-onlyzumExportieren von alsangezeigt werden, wird Ihnen möglicherweise eine Fehlermeldung zu einem unerwarteten Fehler angezeigt, der das Erstellen des Ordners verhindert. Bei diesem Fehler handelt es sich um ein bekanntes Problem mit NFS Version 3. Sie können die Meldung ignorieren.

- Für File/directory access controlled by (Datei-/Verzeichniszugriff kontrolliert von) wählen Sie eine der folgenden Optionen aus:
  - Wählen Sie Windows Access Control List (Windows-Zugriffskontrollliste) aus, um differenzierte Berechtigungen für Dateien und Ordner in Ihrer SMB-Dateifreigabe festzulegen. Weitere Informationen finden Sie unter Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe.
  - Wählen Sie POSIX permissions (POSIX-Berechtigungen) aus, um POSIX-Berechtigungen zum Steuern des Zugriffs auf Dateien und Verzeichnisse zu verwenden, die über ein NFS- oder eine SMB-Dateifreigabe gespeichert werden.

  Wenn Ihre Authentifizierungsmethode lautetActive Directory, fürAdmin-Benutzer/GruppenGeben Sie eine durch Komma getrennte Liste der AD-Benutzer und -Gruppen ein. Tun Sie dies, wenn Sie möchten, dass der Admin-Benutzer zum Aktualisieren von ACLs für alle Dateien und Ordnern in der Dateifreigabe berechtigt ist. Diese Benutzer und Gruppen haben dann Administratorrechte für die Dateifreigabe. Einer Gruppe muss das Präfix@Charakter zum Beispiel`@group1`aus.

- FürGroß-/Kleinschreibungaktivieren Sie das Kontrollkästchen, damit das Gateway die Groß- und Kleinschreibung steuern kann, oder deaktivieren Sie das Kontrollkästchen, damit der Client die Groß- und Kleinschreibung steuern kann.

> **Note**
>
> - Wenn Sie dieses Kontrollkästchen aktivieren, gilt diese Einstellung sofort für neue SMB-Clientverbindungen. Bestehende SMB-Clientverbindungen müssen sich von der Dateifreigabe trennen und erneut verbinden, damit die Einstellung wirksam wird.
> - Wenn Sie dieses Kontrollkästchen deaktivieren, kann diese Einstellung dazu führen, dass Sie den Zugriff auf Dateien mit Namen verlieren, die sich nur in ihrem Fall unterscheiden.

- FürZugriffs-basierte Aufzählungaktivieren Sie das Kontrollkästchen, um die Dateien und Ordner auf der Freigabe nur für Benutzer sichtbar zu machen, die Lesezugriff haben. Lassen Sie das Kontrollkästchen deaktiviert, um die Dateien und Ordner auf der Freigabe während der Verzeichnisaufzählung für alle Benutzer sichtbar zu machen.

  > **Note**
  >
  > Die zugriffsbasierte Aufzählung ist ein System, das die Aufzählung von Dateien und Ordnern auf einer SMB-Dateifreigabe basierend auf den Zugriffskontrolllisten (ACLs) der Freigabe filtert.

- FürOpportunistisches Schloss (Oplock)Wählen Sie eine der folgenden Optionen aus:
  - Klicken Sie aufEnableddamit die Dateifreigabe die opportunistische Sperre verwenden kann, um die Dateipufferungsstrategie zu optimieren, was in den meisten Fällen die Leistung verbessert, insbesondere im Hinblick auf Windows-Kontextmenüs.
  - Klicken Sie aufDisabledum die Verwendung opportunistischer Sperren zu verhindern. Wenn mehrere Windows-Clients in Ihrer Umgebung häufig dieselben Dateien gleichzeitig bearbeiten, kann das Deaktivieren der opportunistischen Sperre manchmal die Leistung verbessern.

> **Note**
>
> Die Aktivierung des opportunistischen Sperren von Shares mit Berücksichtigung von Groß- und Kleinschreibung wird nicht für Workloads empfohlen, die in einem anderen Fall Zugriff auf Dateien mit demselben Namen beinhalten.

5. Wählen Sie Save Changes (Änderungen speichern) aus.

Aktualisieren von Objekten in Ihrem Amazon S3 S3-Bucket

Wenn der NFS- oder SMB-Client Dateisystemvorgänge ausführt, pflegt das Gateway ein Verzeichnis der Objekte im S3-Bucket, das mit der Dateifreigabe verknüpft ist. Ihr Gateway verwendet dieses Verzeichnis im Cache, um die Latenz und Häufigkeit der S3-Anforderungen zu reduzieren. Dieser Vorgang importiert keine Dateien in den Cache-Speicher des S3 File Gateways. Es aktualisiert nur das zwischengespeicherte Inventar, um Änderungen im Inventar der Objekte im S3-Bucket widerzuspiegeln.

Zum Aktualisieren des S3-Buckets für Ihre Dateifreigabe können Sie die Storage Gateway Gateway-Konsole verwenden, dieRefreshCacheBetrieb in der Storage Gateway Gateway-API oder einemAWS LambdaFunktion.

So aktualisieren Sie Objekte in einem S3-Bucket über die Konsole

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie File shares (Dateifreigaben) und wählen Sie dann die Dateifreigabe, die mit dem zu aktualisierenden S3-Bucket verknüpft ist.
3. Wählen Sie für Actions (Aktionen)die Option Refresh cache (Cache aktualisieren).

   Die Dauer des Aktualisierungsprozesses hängt von der Anzahl der Objekte ab, die im Gateway zwischengespeichert sind, sowie von der Anzahl der Objekte, die dem S3-Bucket hinzugefügt oder aus ihm entfernt wurden.

So aktualisieren Sie Objekte in einem S3-Bucket mit einemAWS Lambdawirken

1. Identifizieren Sie den S3-Bucket, der vom S3 File Gateway verwendet wird.
2. Überprüfen Sie, dass derEreignis-Abschnitt ist leer. Es füllt sich später automatisch aus.
3. Erstellen Sie eine IAM-Rolle und erlauben Sie Trust Relationship for Lambda`lambda.amazonaws.com`aus.
4. Verwenden Sie die folgende Richtlinie.

```
{
    "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. Erstellen Sie eine Lambda-Funktion von der Lambda-Konsole aus.
6. Verwenden Sie die folgende Funktion für Ihre Lambda-Aufgabe.

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

7. FürAusführungsrolleWählen Sie die IAM-Rolle aus, die Sie erstellt haben.
8. Optional: Fügen Sie einen Trigger für Amazon S3 hinzu und wählen Sie das EreignisObjectCreatedoderObjectRemovedaus.

> **Note**
>
> `RefreshCache`muss einen Prozess abschließen, bevor Sie einen anderen starten. Wenn Sie viele Objekte in einem Bucket erstellen oder löschen, kann sich die Leistung

verschlechtern. Daher empfehlen wir, S3-Trigger zu verwenden. Verwenden Sie stattdessen die im Folgenden beschriebene Amazon CloudWatch CloudWatch-Regel.

9. Erstellen Sie eine CloudWatch-Regel in der CloudWatch-Konsole und fügen Sie einen Zeitplan hinzu. Im Allgemeinen empfehlen wir eineFestzinssatzVon 30 Minuten. Sie können jedoch 1-2 Stunden für einen großen S3-Eimer verwenden.
10. Fügen Sie einen neuen Trigger für CloudWatch-Ereignisse hinzu und wählen Sie die Regel aus, die Sie gerade erstellt haben.
11. Speichern Sie Ihre Lambda-Konfiguration. Wählen Sie Test aus.
12. Klicken Sie aufS3 SETZENund passen Sie den Test an Ihre Anforderungen an.
13. Der Test sollte erfolgreich sein. Wenn nicht, ändern Sie den JSON an Ihre Anforderungen und testen Sie es erneut.
14. Öffnen Sie die Amazon S3 S3-Konsole und stellen Sie sicher, dass das von Ihnen erstellte Ereignis und die Lambda-Funktion ARN vorhanden sind.
15. Hochladen eines Objekts mit der Amazon S3 S3-Konsole oder demAWS CLIaus.

Die CloudWatch-Konsole generiert eine CloudWatch-Ausgabe ähnlich der Folgenden.

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

Durch den Lambda-Aufruf erhalten Sie eine Ausgabe wie die folgende.

```
{
```

```
    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'
        }
    }
}
```

Ihre NFS-Freigabe, die auf Ihrem Client bereitgestellt ist, spiegelt dieses Update wider.

> **Note**
>
> Für Caches, die die Erstellung oder das Löschen großer Objekte in großen Buckets mit Millionen von Objekten aktualisieren, können Aktualisierungen Stunden dauern.

16. Löschen Sie Ihr Objekt manuell mit der Amazon S3 S3-Konsole oderAWS CLIaus.
17. Zeigen Sie die NFS-Freigabe an, die auf Ihrem Client bereitgestellt wurde Stellen Sie sicher, dass Ihr Objekt verschwunden ist (weil Ihr Cache aktualisiert wurde).
18. Prüfen Sie Ihre CloudWatch-Protokolle, um das Protokoll Ihrer Löschung mit dem Ereignis anzuzeigen`ObjectRemoved:Delete`aus.

```
{
    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**
>
> Für Cron-Jobs oder geplante Aufgaben ist Ihr CloudWatch-Protokollereignisu`'detail-type': u'Scheduled Event'`aus.

Beim Aktualisieren des Cache wird nur der Aktualisierungsvorgang initiiert. Ist die Cache-Aktualisierung abgeschlossen, bedeutet das nicht zwangsläufig, dass die Dateiaktualisierung abgeschlossen ist. Um zu ermitteln, ob der Datei-Aktualisierungsvorgang abgeschlossen ist, bevor Sie nach neuen Dateien in der Gateway-Dateifreigabe suchen, verwenden Sie die `refresh-complete`-Benachrichtigung. Zu diesem Zweck können Sie sich durch ein Amazon CloudWatch CloudWatch-Ereignis benachrichtigen lassen, wenn IhreRefreshCacheVorgang ist abgeschlossen. Weitere Informationen finden Sie unter Benachrichtigungen zu Dateioperationen erhalten.

Verwenden der S3-Objektsperre mit einem Amazon S3 S3-Datei-Gateway

Amazon S3 File Gateway unterstützt den Zugriff auf S3-Buckets, für die Amazon S3 S3-Objektsperre aktiviert ist. Mit Amazon S3 Object Lock können Sie Objekte anhand des Modells „Write Once Read Many“ (WORM) speichern. Wenn Sie Amazon S3 S3-Objektsperre verwenden, können Sie verhindern, dass ein Objekt in Ihrem S3-Bucket gelöscht oder überschrieben wird. Amazon S3 Object Lock arbeitet zusammen mit der Objektversionierung, um Ihre Daten zu schützen.

Wenn Sie Amazon S3 S3-Objektsperre aktivieren, können Sie das Objekt weiterhin ändern. Beispielsweise kann es in eine Dateifreigabe auf einem S3-File Gateway geschrieben, gelöscht oder umbenannt werden. Wenn Sie ein Objekt auf diese Weise ändern, platziert S3 File Gateway eine neue Version des Objekts, ohne die vorherige Version (d. h. das gesperrte Objekt) zu beeinflussen.

Wenn Sie beispielsweise die S3-File Gateway-NFS oder -SMB-Schnittstelle zum Löschen einer Datei verwenden und das entsprechende S3-Objekt ist gesperrt, platziert das Gateway eine S3-Löschmarkierung als die nächste Version des Objekts und lässt die ursprüngliche Objektversion bestehen. Wenn ein S3-File Gateway den Inhalt oder Metadaten eines gesperrten Objekts ändert, wird eine neue Version des Objekts mit den neuesten Änderungen hochgeladen, aber die ursprüngliche gesperrte Version des Objekts bleibt unverändert.

Weitere Informationen zur Amazon-S3-Objektsperre finden Sie unterSperren von Objekten mit S3-ObjektsperreimAmazon Simple Storage Service — Benutzerhandbuchaus.

Den Status der Dateifreigabe verstehen

Jede Dateifreigabe verfügt über einen verknüpften Status, aus dem sich auf einen Blick der Zustand der Dateifreigabe ersehen lässt. In den meisten Fällen gibt der Status an, dass die Dateifreigabe ordnungsgemäß funktioniert und Sie keine Aktion durchzuführen brauchen. In einigen Fällen gibt der Status ein Problem an, das eventuell eine Aktion Ihrerseits erforderlich macht.

Sie können den Dateifreigabestatus auf der Storage Gateway Gateway-Konsole anzeigen. Der Dateifreigabenstatus wird in der Spalte Status für jede Dateifreigabe im Gateway angezeigt. Eine Dateifreigabe, die ordnungsgemäß funktioniert, hat den Status AVAILABLE.

In der folgenden Tabelle finden Sie eine Beschreibung aller Dateifreigabestatus sowie Hinweise, ob und wann abhängig vom Status Maßnahmen ergriffen werden müssen. Eine Dateifreigabe sollte während der gesamten bzw. eines Großteils der Nutzungszeit den Status AVAILABLE aufweisen.

Status	Bedeutung
AVAILABLE	Die Dateifreigabe ist ordnungsgemäß konfiguriert und verfügbar. Der Status AVAILABLE ist der normale Ausführungsstatus für eine Dateifrei gabe.
CREATING	Die Dateifreigabe wird erstellt und ist noch nicht einsatzbereit. Der Status CREATING ist vorübergehend. Es ist keine Aktion erforderlich. Wenn eine Dateifreigabe in diesem Status hängen bleibt, liegt dies wahrscheinlich daran, dass die Verbindung der Gateway-VM zu getrennt wurdeAWSaus.
UPDATING	Die Dateifreigabenkonfiguration wird aktualisiert. Wenn eine Dateifrei gabe in diesem Status hängen bleibt, liegt dies wahrscheinlich daran, dass die Verbindung der Gateway-VM zu getrennt wurdeAWSaus.
DELETING	Die Dateifreigabe wird gelöscht. Die Dateifreigabe wird erst dann gelöscht, wenn alle Daten hochgeladen sindAWSaus. Der Status DELETING ist vorübergehend, und es ist keine Aktion erforderlich.
FORCE_DELETING	Die Dateifreigabe wird gewaltsam gelöscht. Die Dateifreigabe wird umgehend gelöscht und hochgeladenAWSwird abgebrochen. Der Status FORCE DELETING ist vorübergehend, und es ist keine Aktion erforderl ich.
UNAVAILABLE	Die Dateifreigabe befindet sich in einem fehlerhaften Status. Bestimmte Probleme können dazu führen, dass die Dateifreigabe einen fehlerhaften Status annimmt. Beispiel: Dies kann aufgrund von Fehlern der Rollenric htlinie geschehen oder weil die Dateifreigabe auf einen Amazon S3 S3-Bucket verweist, der nicht existiert. Wenn das Problem, das den fehlerhaf

Status	Bedeutung
	ten Status verursacht hat, behoben ist, kehrt die Dateifreigabe in den Status AVAILABLE zurück.

Bewährte Methoden für die Datei

In diesem Abschnitt finden Sie Informationen zu bewährten Methoden für das Erstellen von Dateifreigaben.

Themen

- Verhindern, dass mehrere Dateifreigaben in Ihren Amazon S3 S3-Bucket schreiben
- Bestimmten NFS-Clients erlauben, Ihre Dateifreigabe zu mounten

Verhindern, dass mehrere Dateifreigaben in Ihren Amazon S3 S3-Bucket schreiben

Wenn Sie eine Dateifreigabe erstellen, sollten Sie den Amazon S3 S3-Bucket so konfigurieren, dass nur eine Dateifreigabe darin schreiben kann. Wenn Sie den S3-Bucket so konfigurieren, dass mehrere Dateifreigaben darin schreiben können, kann dies zu unvorhersehbaren Ergebnissen führen. Um dies zu verhindern, können Sie eine S3-Bucket-Richtlinie erstellen, die allen Rollen außer der Rolle für die Dateifreigabe das Ablegen oder Löschen von Objekten im Bucket verweigert. Fügen Sie diese Richtlinie an den S3-Bucket an.

Die folgende Beispielrichtlinie verweigert allen Rollen mit Ausnahme der Rolle, die das Bucket erstellt hat, das Schreiben im S3-Bucket. Die Aktionen `s3:DeleteObject` und `s3:PutObject` werden für alle Rollen außer `"TestUser"` verweigert. Die Richtlinie gilt für alle Objekte im `"arn:aws:s3:::TestBucket/*"` Bucket.

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

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

Bestimmten NFS-Clients erlauben, Ihre Dateifreigabe zu mounten

Wir empfehlen das Ändern der zulässigen NFS-Client-Einstellungen für Ihre Dateifreigabe. Andernfalls kann jeder beliebige Client in Ihrem Netzwerk Ihre Dateifreigabe mounten. Weitere Informationen zum Bearbeiten der NFS-Client-Einstellungen finden Sie unter Bearbeiten der Zugriffseinstellungen für Ihre NFS-Dateifreigabe.

Überwachen Sie Ihr Datei-Gateway

Sie können Ihren Datei-Gateway und die zugehörigen Ressourcen inAWS Storage Gatewaymithilfe von Amazon CloudWatch CloudWatch-Metriken und Überwachungsprotokollen für Dateifreigaben. Sie können CloudWatch Events auch verwenden, um benachrichtigt zu werden, wenn Ihre Dateioperationen abgeschlossen sind. Informationen zu Typmetriken für Datei-Gateways finden Sie unter Überwachen Sie Ihr Datei-Gateway.

Themen

Abrufen von Datei-Gateway-Integritätsprotokollen mit CloudWatch

Sie können Amazon CloudWatch Logs verwenden, um Informationen über den Zustand Ihres File Gateways und verwandte Ressourcen abzurufen. Sie können die Protokolle verwenden, um Ihr Gateway auf auftretende Fehler zu überwachen. Darüber hinaus können Sie Amazon CloudWatch CloudWatch-Abonnementfilter verwenden, um die Verarbeitung der Protokollinformationen in Echtzeit zu automatisieren. Weitere Informationen finden Sie unterProtokolldaten-Verarbeitung in Echtzeit mit AbonnementsimBenutzerhandbuch zu Amazon CloudWatch.

Sie können zum Beispiel eine CloudWatch-Protokollgruppe dazu konfigurieren, Ihr Gateway zu überwachen und benachrichtigt werden, wenn Ihr File Gateway keine Dateien zu einem Amazon S3 S3-Bucket hochladen kann. Sie können die Gruppe entweder beim Aktivieren des Gateways konfigurieren oder nachdem das Gateway aktiviert wurde und in Betrieb ist. Weitere Informationen zum Konfigurieren einer CloudWatch-Protokollgruppe beim Aktivieren eines Gateways finden Sie unterKonfigurieren Sie Ihr Amazon S3 File Gatewayaus. Allgemeine Informationen zu CloudWatch-Protokollgruppen finden Sie unterArbeiten mit Log-Gruppen und Log-StreamsimBenutzerhandbuch zu Amazon CloudWatch.

Nachfolgend finden Sie ein Beispiel für einen Fehler, der von einem Datei-Gateway gemeldet wird.

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

Dieser Fehler bedeutet, dass das Datei-Gateway das Objekt nicht hochladen kann`myFolder/myFile.text`zu Amazon S3, da es aus der Speicherklasse Amazon S3 Standard in die Speicherklasse S3 Glacier Flexible Retrieval oder die Speicherklasse S3 Glacier Deep Archive übergegangen ist.

Im obigen Gateway-Zustandsprotokoll geben diese Elemente die angegebenen Informationen an:

- `source: share-E1A2B34C` gibt die Dateifreigabe an, bei der dieser Fehler aufgetreten ist.
- `"type": "InaccessibleStorageClass"` gibt die Art des aufgetretenen Fehlers an. In diesem Fall ist dieser Fehler aufgetreten, als das Gateway versucht hat, das angegebene Objekt in Amazon S3 hochzuladen oder aus Amazon S3 zu lesen. In diesem Fall ist das Objekt jedoch zum Amazon S3 Gletscher übergegangen. Der Wert von `"type"` kann jeder Fehler sein, der beim File Gateway aufgetreten. Eine Liste möglicher Fehler finden Sie unter Fehlerbehebung bei File Gateway Problemen.
- `"operation": "S3Upload"`gibt an, dass dieser Fehler aufgetreten ist, als das Gateway versucht hat, dieses Objekt zu S3 hochzuladen.
- `"key": "myFolder/myFile.text"` gibt das Objekt an, das den Fehler verursacht hat.
- `gateway": "sgw-B1D123D4` gibt das File Gateway an, bei dem dieser Fehler aufgetreten ist.
- `"timestamp": "1565740862516"`gibt den Zeitpunkt an, zu dem der Fehler aufgetreten ist.

Weitere Informationen zum Beheben von Fehlern dieser Art finden Sie unter Fehlerbehebung bei File Gateway Problemen.

Eine CloudWatch-Protokollgruppe konfigurieren, nachdem Ihr Gateway aktiviert wurde

Das folgende Verfahren zeigt, wie Sie eine CloudWatch -Protokollgruppe konfigurieren, nachdem Ihr Gateway aktiviert wurde.

So konfigurieren Sie eine CloudWatch-Protokollgruppe für Ihr Datei-Gateway

1. Melden Sie sich beimAWS Management Consoleund öffnen Sie die Storage Gateway Gateway-Konsole unterhttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie im Navigationsbereich und dann aus.-Gatewaysund dann das Gateway aus, für das Sie die CloudWatch-Protokollgruppe konfigurieren möchten.
3. FürAktionen, wählenBearbeiten von Gatewayinformationenaus. Oder auf der-DetailsTab unterGesundheits-ProtokolleundNicht aktiviert, wählenProtokollgruppe konfigurierenSo öffnen Sie denBearbeitenCustomerGatewayNameDialogfeld.
4. FürProtokollgruppe Gateway-Wählen Sie eine der folgenden Optionen:

   - Disable logging (Protokollierung deaktivieren)wenn Sie Ihr Gateway nicht mit CloudWatch-Protokollgruppen überwachen möchten.
   - Eine neue Protokollgruppe erstellenUm eine neue CloudWatch-Protokollgruppe zu erstellen.
   - Verwenden einer vorhandenen Protokollgruppeum eine bereits vorhandene CloudWatch-Protokollgruppe zu verwenden.

     Wählen Sie eine Protokollgruppe aus derBestehende Loggruppenlisteaus.
5. Wählen Sie Save Changes (Änderungen speichern) aus.
6. Um die Zustandsprotokolle für Ihr Gateway anzuzeigen, gehen Sie wie folgt vor:

   1. Wählen Sie im Navigationsbereich und dann aus.-Gatewaysund dann das Gateway aus, für das Sie die CloudWatch-Protokollgruppe konfiguriert haben.
   2. Wählen Sie das Symbol-DetailsTab und unterGesundheits-Protokolle, wählenCloudWatch-Protokolleaus. DieProtokollgruppendetailswird in der CloudWatch-Konsole geöffnet.

So konfigurieren Sie eine CloudWatch -Protokollgruppe für Ihr Datei-Gateway

1. Melden Sie sich beimAWS Management Consoleund öffnen Sie die Storage Gateway Gateway-Konsole unterhttps://console.aws.amazon.com/storagegateway/homeaus.

2. Klicken Sie auf-Gatewaysund dann das Gateway aus, für das Sie die CloudWatch-Protokollgruppe konfigurieren möchten.
3. FürAktionen, wählenBearbeiten von Gatewayinformationenaus. Oder im-DetailsTab, nebenProtokollierungunterNicht aktiviert, wählenProtokollgruppe konfigurierenSo öffnen Sie denBearbeiten von GatewayinformationenDialogfeld.
4. FürProtokollgruppe Gateways, wählenVerwenden einer vorhandenen ProtokollgruppeWählen Sie dann die Protokollgruppe aus, die Sie verwenden möchten.

   Wenn keine Protokollgruppe vorhanden ist, wählen Sie Eine Protokollgruppe erstellen aus, um eine Protokollgruppe zu erstellen. Sie werden zur CloudWatch Logs -Protokoll-Konsole weitergeleitet, in der Sie die -Protokollgruppe erstellen können. Wenn Sie eine neue Protokollgruppe erstellen, klicken Sie auf die Schaltfläche „Refresh“ (Aktualisieren), um die neue Protokollgruppe in der Dropdown-Liste anzuzeigen.
5. Klicken Sie abschließend auf Save.
6. Um die Protokolle für Ihr Gateway anzuzeigen, wählen Sie das Gateway und dann den-DetailsRegisterkarte.

Informationen zur Fehlerbehebung finden Sie unter Fehlerbehebung bei File Gateway Problemen.

Verwenden von Amazon-CloudWatch-Metriken

Sie können Überwachungsdaten für Ihr Datei-Gateway mithilfe derAWS Management Consoleoder die CloudWatch-API. Die Konsole zeigt eine Reihe von Graphen an, die auf den unformatierten Daten aus der CloudWatch-API basieren. Die CloudWatch-API kann auch über eine derAWS-SDKsoderAmazon CloudWatch CloudWatch-API-Tools. Je nach Anforderungen können Sie entweder die in der Konsole angezeigten oder die mit der API aufgerufenen Graphen verwenden.

Unabhängig davon, mit welcher Methode Sie mit Metriken arbeiten, müssen Sie die folgenden Informationen angeben:

- Die zu verwendende Metrikdimension. Eine Dimension ist ein Name-Wert-Paar, mit dem Sie eine Metrik eindeutig identifizieren. Die Dimensionen für Storage Gateway sind`GatewayId`und`GatewayName`aus. In der CloudWatch-Konsole können Sie die`Gateway Metrics`anzeigen, um gateway-spezifische Dimensionen auszuwählen. Weitere Informationen zu Dimensionen finden Sie unterDimensionenimAmazon CloudWatch-Benutzerhandbuchaus.
- Der Metrikname, beispielsweise `ReadBytes`.

In der folgenden Tabelle finden Sie eine Zusammenfassung der verfügbaren Typen von Storage Gateway Gateway-Metrikdaten.

Amazon CloudWatch CloudWatch-Namespace	Dimension	Description
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Diese Dimensionen filtern nach Metrikdaten, die Aspekte des Gateways beschreiben. Sie können ein zu verwendendes Datei-Gateway identifizieren, indem Sie die Dimensionen `GatewayId` und `GatewayName` angeben. Die Durchsatz- und Latenzdaten eines Gateways basieren auf allen Dateifreigaben im Gateway. Die Daten werden automatisch in 5-Minuten-Intervallen kostenlos zur Verfügung gestellt.

Das Arbeiten mit Gateway- und Dateimetriken gleicht dem Arbeiten mit anderen Service-Metriken. Eine Erläuterung einiger der häufigsten Aufgaben mit Metriken finden Sie in der folgenden CloudWatch-Dokumentation:

- Anzeigen der verfügbaren Metriken
- Abrufen von Statistiken für eine Metrik
- Erstellen von CloudWatch-Alarmen

Benachrichtigungen zu Dateioperationen erhalten

Storage Gateway kann CloudWatch-Ereignisse initiieren, wenn Ihre Dateioperationen abgeschlossen sind:

- Sie erhalten eine Benachrichtigung, sobald das Gateway mit dem asynchronen Hochladen Ihrer Dateien aus der Dateifreigabe in Amazon S3 fertig ist. Verwenden der`NotificationPolicy`-Parameter zum Anfordern einer Benachrichtigung über das Hochladen. Dies sendet eine

Benachrichtigung für jeden abgeschlossenen Datei-Upload an Amazon S3. Weitere Informationen finden Sie unter Benachrichtigung zum Hochladen von Dateien.

- Sie erhalten eine Benachrichtigung, sobald das Gateway mit dem asynchronen Hochladen Ihrer Arbeitsdatei fertig ist, die von der Dateifreigabe in Amazon S3 gespeichert wird. Verwenden derNotifyWhenUploadedAPI-Vorgang zum Anfordern einer Upload-Benachrichtigung zur Arbeitsdatei. Dies sendet eine Benachrichtigung, wenn alle Dateien in der Arbeitsdateigruppe zu Amazon S3 hochgeladen wurden. Weitere Informationen finden Sie unter Upload-Benachrichtigung für Arbeitsdatei-Set.
- Sie können eine Benachrichtigung erhalten, wenn ein Gateway die Aktualisierung des Caches für Ihren S3-Bucket abgeschlossen hat. Wenn Sie dieRefreshCache-Betrieb über die Storage Gateway Gateway-Konsole oder -API, abonnieren Sie die Benachrichtigung, wenn die Operation abgeschlossen ist. Weitere Informationen finden Sie unter Aktualisierungs-Cache-Benachrichtigung erhalten.

Wenn die angeforderte Dateioperation abgeschlossen ist, sendet Storage Gateway Ihnen eine Benachrichtigung über CloudWatch Events. Sie können CloudWatch Events so konfigurieren, dass die Benachrichtigung durch Ereignisziele wie Amazon SNS, Amazon SQS oder ein gesendet wird.AWS LambdaFunktion. Sie können zum Beispiel ein Amazon SNS SNS-Ziel so konfigurieren, dass die Benachrichtigung an Amazon SNS-Nutzer beispielsweise eine E-Mail oder SMS gesendet wird. Informationen zu CloudWatch Events finden Sie unterWas ist CloudWatch Events?

So richten Sie die Benachrichtigung über CloudWatch Events ein

1. Erstellen Sie ein Ziel, wie etwa ein Amazon SNS-Thema oder eine Lambda-Funktion, das aufgerufen wird, wenn das angeforderte Ereignis in Storage Gateway ausgelöst wird.
2. Erstellen Sie eine Regel in der CloudWatch Events -Konsole, um Ziele basierend auf einem Ereignis in Storage Gateway aufzurufen.
3. In der Regel erstellen Sie ein Ereignismuster für den Ereignistyp. Die Benachrichtigung wird ausgelöst, wenn das Ereignis diesem Regelmuster entspricht.
4. Wählen Sie das Ziel aus und konfigurieren Sie die Einstellungen.

Das folgende Beispiel zeigt eine Regel, die den angegebenen Ereignistyp im angegebenen Gateway und im angegebenen Gateway initiiert.AWSRegion : Sie können beispielsweise als Ereignistyp `Storage Gateway File Upload Event` angeben.

```
{
```

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

Weitere Informationen zum Auslösen von CloudWatch Events zum Auslösen von Regeln finden Sie unterErstellen einer CloudWatch-Ereignisregel, die bei einem Ereignis ausgelöst wirdimBenutzerhandbuch für Amazon CloudWatch Eventsaus.

Benachrichtigung zum Hochladen von Dateien

Es gibt zwei Anwendungsfälle, in denen Sie die Datei-Upload-Benachrichtigung verwenden können:

- Um die Cloud-Verarbeitung von Dateien zu automatisieren, die hochgeladen werden, können Sie den`NotificationPolicy`-Parameter und erhalte eine Benachrichtigungs-ID zurück. Die Benachrichtigung, die nach dem Hochladen der Dateien ausgelöst wird, hat die gleiche Benachrichtigung-ID wie diejenige, die von der API zurückgegeben wurde. Wenn Sie diese Benachrichtigung-ID zuordnen, um die Liste der Dateien nachzuverfolgen, die Sie hochladen, können Sie die Verarbeitung der Datei auslösen, die in hochgeladen wird.AWSwenn das Ereignis mit derselben ID generiert wird.
- Für Anwendungsfälle bei der Inhaltsverteilung können Sie über zwei Datei-Gateways verfügen, die demselben Amazon S3-Bucket zugeordnet sind. Der Dateifreigabe-Client für Gateway1 kann neue Dateien in Amazon S3 hochladen, und die Dateien werden von Dateifreigabe-Clients auf Gateway2 gelesen. Die Dateien werden in Amazon S3 hochgeladen, sind jedoch nicht in Gateway2 sichtbar, da es eine lokal zwischengespeicherte Version von Dateien in Amazon S3 verwendet. Um die Dateien in Gateway2 sichtbar zu machen, können Sie die`NotificationPolicy`-Parameter, um eine Benachrichtigung über das Hochladen von Dateien von Gateway1 anzufordern, die Sie informiert, wenn die Upload-Datei abgeschlossen ist. Sie können dann CloudWatch Events verwenden, um automatisch eineRefreshCacheAnforderung der Dateifreigabe in Gateway2. WennRefreshCacheAnfrage ist abgeschlossen, die neue Datei ist in Gateway2 sichtbar.

Example Beispiel: Benachrichtigung über das Hochladen von Dateien

Das folgende Beispiel zeigt eine Benachrichtigung über das Hochladen von Dateien, die an Sie über CloudWatch übermittelt wird, wenn das Ereignis mit der von Ihnen erstellten Regel übereinstimmt. Diese Benachrichtigung weist das JSON-Format auf. Sie können diese Benachrichtigung so konfigurieren, dass sie als Textnachricht an das Ziel übermittelt wird. Der `detail-type` ist `Storage Gateway Object Upload Event`.

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

Feldnamen	Description
Version	Die aktuelle Version der IAM-Richtlinie
id	Die ID, welche die IAM-Richtlinie identifiziert
detail-type	Eine Beschreibung des Ereignisses, das die gesendete Benachrichtigung ausgelöst hat

Feldnamen	Description
Quelle	DieAWS-Dienst, der die Quelle der Anforderung und Benachrichtigung ist
Konto	Die ID derAWS-Konto, in dem die Anfrage und Benachrichtigung generiert wurden
variieren	Zeitpunkt der Anforderung zum Hochladen von Dateien zu Amazon S3.
region (Region)	DieAWSRegion, in der die Anfrage und Benachrichtigung gesendet wurden
Ressourcen	Der Storage Gateway-Ressourcen, für die die Richtlinie gilt
Objektgröße	Die Größe des Objekts in Bytes.
Änderungszeit	Die Zeit, zu der der Client die Datei geändert hat.
Objektschlüssel	Der Pfad der Datei.
event-type	Die CloudWatch Events, die die Benachrichtigung ausgelöst haben
prefix	Der Präfixname des S3-Buckets.
bucket-name	Der Name des S3-Buckets.

Upload-Benachrichtigung für Arbeitsdatei-Set

Es gibt zwei Anwendungsfälle, in denen Sie die Upload-Benachrichtigung für Arbeitsdatei-Sets verwenden können:

- Um die Cloud-Verarbeitung von Dateien zu automatisieren, die hochgeladen werden, können Sie den`NotifyWhenUploaded`API und erhalte eine Benachrichtigungs-ID zurück. Die Benachrichtigung, die nach dem Hochladen der Arbeitsgruppe von Dateien ausgelöst wird, hat

die gleiche Benachrichtigungs-ID wie diejenige, die von der API zurückgegeben wurde. Wenn Sie diese Benachrichtigung-ID zuordnen, um die Liste der Dateien nachzuverfolgen, die Sie hochladen, können Sie die Verarbeitung des Arbeitssatzes von Dateien auslösen, die in hochgeladen werden.AWSwenn das Ereignis mit derselben ID generiert wird.

- Für Anwendungsfälle bei der Inhaltsverteilung können Sie über zwei Datei-Gateways verfügen, die demselben Amazon S3-Bucket zugeordnet sind. Der Dateifreigabe-Client für Gateway1 kann neue Dateien in Amazon S3 hochladen, und die Dateien werden von Dateifreigabe-Clients auf Gateway2 gelesen. Die Dateien werden in Amazon S3 hochgeladen, sind jedoch nicht in Gateway2 sichtbar, da es eine lokal zwischengespeicherte Version von Dateien in S3 verwendet. Um die Dateien in Gateway2 sichtbar zu machen, verwenden Sie dieNotifyWhenUploadedDer API-Vorgang, um eine Benachrichtigung über das Hochladen von Dateien von Gateway1 anzufordern, die Sie informiert, wenn das Hochladen des Arbeitssatzes abgeschlossen ist. Sie können dann die CloudWatch Events verwenden, um automatisch eineRefreshCacheAnforderung der Dateifreigabe in Gateway2. WennRefreshCacheDie Anforderung ist abgeschlossen, die neuen Dateien sind in Gateway2 sichtbar. Dieser Vorgang importiert keine Dateien in den Cache-Speicher des Datei-Gateways. Es aktualisiert nur das zwischengespeicherte Inventar, um Änderungen im Inventar der Objekte im S3-Bucket widerzuspiegeln.

Example Beispiel: Upload-Benachrichtigung für Arbeitsdatei-Sets

Das folgende Beispiel zeigt eine Benachrichtigung über das Hochladen von Arbeitsdatei-Sets, die an Sie über CloudWatch übermittelt wird, wenn das Ereignis mit der von Ihnen erstellten Regel übereinstimmt. Diese Benachrichtigung weist das JSON-Format auf. Sie können diese Benachrichtigung so konfigurieren, dass sie als Textnachricht an das Ziel übermittelt wird. Der `detail-type` ist `Storage Gateway File Upload Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Upload Notification Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
```

```
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

Feldnamen	Description
Version	Die aktuelle Version der IAM-Richtlinie
id	Die ID, welche die IAM-Richtlinie identifiziert
detail-type	Eine Beschreibung des Ereignisses, das die gesendete Benachrichtigung ausgelöst hat
Quelle	DieAWSDer Dienst, der die Quelle der Anforderung und Benachrichtigung ist
Konto	Die ID derAWS-Konto, in dem die Anfrage und Benachrichtigung generiert wurden
variieren	Zeitpunkt der Anforderung zum Hochladen von Dateien zu Amazon S3.
region (Region)	DieAWSRegion, in der die Anfrage und Benachrichtigung gesendet wurden
Ressourcen	Die Storage Gateway Gateway-Ressourcen, für die die Richtlinie gilt.
event-type	Die CloudWatch Events, die die Benachric htigung ausgelöst haben
notification-id	Die zufällig generierte ID der gesendeten Benachrichtigung. Diese ID liegt im UUID-Format vor. Hierbei handelt es sich um die Benachrichtigungs-ID, die beim Aufrufen von `NotifyWhenUploaded` zurückgegeben wird.

Feldnamen	Description
request-received	Wann das Gateway die `NotifyWhenUploaded` -Anforderung erhalten hat
Um diese potenziell sensiblen Informationen zu schützen, empfehlen wir dringend, die Protokolle für alle Aufträge zu löschen, die den erreicht haben.	Wenn alle Dateien im Arbeitssatz auf Amazon S3 hochgeladen wurden.

Aktualisierungs-Cache-Benachrichtigung erhalten

Für Benachrichtigungen zu Cache-Aktualischungen können Sie zwei Datei-Gateways vorliegen haben, die demselben Amazon S3 S3-Bucket zugeordnet sind, und der NFS-Client für Gateway1 lädt neue Dateien in den S3-Bucket hoch. Die Dateien werden in Amazon S3 hochgeladen, werden jedoch erst in Gateway2 angezeigt, wenn Sie den Cache aktualisieren. Dies liegt daran, dass Gateway2 eine lokal zwischengespeicherte Version der Dateien in Amazon S3 verwendet. Nach der Cache-Aktualisierung können Sie die Dateien in Gateway2 verwenden. Bei großen Dateien kann es länger dauern, bis sie in Gateway2 angezeigt werden. Es kann daher sinnvoll sein, sich benachrichtigen zu lassen, wenn die Cache-Aktualisierung abgeschlossen ist. Sie können eine Benachrichtigung über die Cache-Aktualisierung von Gateway2 anfordern, um benachrichtigt zu werden, wenn alle Dateien in Gateway2 sichtbar sind.

Example Beispiel: Benachrichtigung zur Cache-Aktualisierung

Das folgende Beispiel zeigt eine Benachrichtigung zur Cache-Aktualisierung, die an Sie über CloudWatch übermittelt wird, wenn das Ereignis mit der von Ihnen erstellten Regel übereinstimmt. Diese Benachrichtigung weist das JSON-Format auf. Sie können diese Benachrichtigung so konfigurieren, dass sie als Textnachricht an das Ziel übermittelt wird. Der `detail-type` ist `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": [
            "/"
        ]
    }
}
```

Feldnamen	Description
Version	Die aktuelle Version der IAM-Richtlinie
id	Die ID, welche die IAM-Richtlinie identifiziert
detail-type	Eine Beschreibung des Typs des Ereignisses, das die gesendete Benachrichtigung ausgelöst hat
Quelle	DieAWS-Dienst, der die Quelle der Anforderung und Benachrichtigung ist
Konto	Die ID derAWS-Konto, in dem die Anfrage und Benachrichtigung generiert wurden
variieren	Zeitpunkt der Anforderung zum Aktualisieren der Dateien im Arbeitssatz
region (Region)	DieAWSRegion, in der die Anfrage und Benachrichtigung gesendet wurden
Ressourcen	Die Storage Gateway Gateway-Ressourcen, für die die Richtlinie gilt.

Feldnamen	Description
event-type	Die CloudWatch Events, die die Benachric htigung ausgelöst haben
notification-id	Die zufällig generierte ID der gesendeten Benachrichtigung. Diese ID liegt im UUID-Format vor. Hierbei handelt es sich um die Benachrichtigungs-ID, die zurückgegeben wird, wenn Sie `RefreshCache` aufrufen.
started	wenn das Gateway den`RefreshCache` - Anforderung und die Aktualisierung gestartet.
Um diese potenziell sensiblen Informationen zu schützen, empfehlen wir dringend, die Protokoll e für alle Aufträge zu löschen, die den erreicht haben.	Wann die Aktualisierung des Arbeitssatzes abgeschlossen wurde
folderList	Eine durch Komma getrennte Liste der Pfade von Ordnern, die im Cache aktualisiert wurden. Der Standardwert ist ["/"].

Grundlagen zu Gateway-Metriken

In der folgenden Tabelle werden Metriken beschrieben, die S3-Datei-Gateways abdecken. Jedes Gateway verfügt über eine Reihe von zugeordneten Metriken. Einige Gateway-spezifische Metriken haben denselben Namen wie bestimmte Dateifreigabe-spezifische Metriken. Diese Metriken stellen die gleichen Messungsarten dar, beziehen sich jedoch eher auf das Gateway als auf die Dateifreigabe.

Geben Sie immer an, ob Sie mit einer Gateway- oder einer Dateifreigabe arbeiten möchten, wenn Sie eine bestimmte Metrik verwenden. Insbesondere müssen Sie bei der Arbeit mit Gateway-Metriken den`Gateway NameFür` das Gateway, dessen Metrikdaten Sie anzeigen möchten. Weitere Informationen finden Sie unter Verwenden von Amazon-CloudWatch-Metriken.

In der folgenden Tabelle werden die Metriken beschrieben, die Sie zum Abrufen von Informationen über IhrenS3-File Gateway-Geräte.

Metrik	Description
`AvailabilityNotifications`	Diese Metrik gibt die Anzahl der Zustandsm eldungen im Zusammenhang mit der Verfügbar keit an, die vom Gateway im Berichtszeitraum generiert wurden. Einheiten: Anzahl
`CacheFileSize`	Diese Metrik verfolgt die Größe von Dateien im Gateway-Cache. Verwenden Sie diese Metrik mit dem`Average`Statistik zur Messung der durchschnittlichen Größe einer Datei im Gateway-Cache. Verwenden Sie diese Metrik mit dem`Max`Statistik zur Messung der maximalen Größe einer Datei im Gateway-C ache. Einheiten: Byte
`CacheFree`	Diese Metrik meldet die Anzahl der verfügbaren Bytes im Gateway-Cache. Einheiten: Byte
`CacheHitPercent`	Prozentsatz der Anwendungsleseoperationen vom Gateway aus, die vom Cache aus bedient werden. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Wenn keine Anwendungsleseoperationen vom Gateway vorhanden sind, wird dieser Metrikwer t mit 100% angegeben. Einheiten: Prozent

Metrik	Description
`CachePercentDirty`	Der Gesamtprozentsatz des Gateway-Caches, der nicht in erhalten geblieben istAWSaus. Die Stichprobe wird am Ende des Berichtsz eitraums entnommen. Einheiten: Prozent
`CachePercentUsed`	Der Gesamtprozentsatz des verwendeten Gateway-Cache-Speichers. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheiten: Prozent
`CacheUsed`	Diese Metrik meldet die Anzahl der verwendet en Bytes im Gateway-Cache. Einheiten: Byte
`CloudBytesDownloaded`	Die Gesamtanzahl der Bytes, die das Gateway hochgeladen hatAWSwährend des Berichtsz eitraums. Verwenden Sie diese Metrik mit der `Sum`-Statisti k, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die Ein- und Ausgabeop erationen pro Sekunde (IOPS) zu messen. Einheiten: Byte

Metrik	Description
`CloudBytesUploaded`	Die Gesamtanzahl der Bytes, die das Gateway heruntergeladen hatAWSwährend des Berichtszeitraums. Verwenden Sie diese Metrik mit der `Sum`-Statistik, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die IOPS-Werte zu messen. Einheiten: Byte
`FilesFailingUpload`	Diese Metrik verfolgt die Anzahl der Dateien, die nicht hochgeladen werden könnenAWSaus. Diese Dateien generieren Gesundheitsbenachrichtigungen, die weitere Informationen zu dem Problem enthalten. Verwenden Sie diese Metrik mit dem`Sum`Statistik, um die Anzahl der Dateien anzuzeigen, die derzeit nicht hochgeladen werden könnenAWSaus. Einheiten: Anzahl
`FileSharesUnavailable`	Diese Metrik gibt die Anzahl der Dateifreigaben auf diesen Gateways an, die sich imNicht verfügbarZustand. Wenn diese Metrik meldet, dass Dateifreigaben nicht verfügbar sind, liegt wahrscheinlich ein Problem mit dem Gateway vor, das zu einer Störung Ihres Workflows führen kann. Es wird empfohlen, einen Alarm zu erstellen, wenn diese Metrik einen Wert ungleich null meldet. Einheiten: Anzahl

Metrik	Description
`FilesRenamed`	Diese Metrik verfolgt die Anzahl der Dateien, die im Berichtszeitraum umbenannt wurden. Einheiten: Anzahl
`HealthNotifications`	Diese Metrik gibt die Anzahl der Gesundhei tsbenachrichtigungen an, die von diesem Gateway im Berichtszeitraum generiert wurden. Einheiten: Anzahl
`IoWaitPercent`	Diese Metrik gibt den Prozentanteil der Zeit an, für die die CPU auf eine Antwort vom lokalen Datenträger wartet. Einheiten: Prozent
`MemTotalBytes`	Diese Metrik meldet die Gesamtspeichermenge auf dem Gateway. Einheiten: Byte
`MemUsedBytes`	Diese Metrik gibt die Menge des verwendeten Speichers auf dem Gateway an. Einheiten: Byte
`NfsSessions`	Diese Metrik meldet die Anzahl der NFS-Sitzu ngen, die auf dem Gateway aktiv sind. Einheiten: Anzahl

Metrik	Description
RootDiskFreeBytes	Diese Metrik meldet die Anzahl der verfügbaren Bytes auf dem Stammdatenträger des Gateways. Wenn diese Metrik meldet, dass weniger als 20 GB kostenlos sind, sollten Sie die Größe des Stammdatenträgers erhöhen. Einheiten: Byte
S3GetObjectRequestTime	Diese Metrik gibt die Zeit an, zu der das Gateway S3-Abrufobjektanfragen abschließen kann. Einheiten: Millisekunden
S3PutObjectRequestTime	Diese Metrik gibt die Zeit an, zu der das Gateway S3-Put-Objektanfragen abschließen kann. Einheiten: Millisekunden
S3UploadPartRequestTime	Diese Metrik gibt an, wann das Gateway S3-Upload-Teile-Anfragen abschließen kann. Einheiten: Millisekunden
SmbV1Sessions	Diese Metrik meldet die Anzahl der SMB V1-Sitzungen, die auf dem Gateway aktiv sind. Einheiten: Anzahl
SmbV2Sessions	Diese Metrik meldet die Anzahl der SMB V2-Sitzungen, die auf dem Gateway aktiv sind. Einheiten: Anzahl

Metrik	Description
`SmbV3Sessions`	Diese Metrik meldet die Anzahl der SMB v3-Sitzungen, die auf dem Gateway aktiv sind. Einheiten: Anzahl
`TotalCacheSize`	Diese Metrik gibt die Gesamtgröße des Cache an. Einheiten: Byte
`UserCpuPercent`	Diese Metrik gibt den Prozentsatz der Zeit an, die für die Gateway-Verarbeitung aufgewendet wird. Einheiten: Prozent

Datenfreigabe-Metriken verstehen

Im Folgenden finden Sie Informationen über die Storage Gateway Gateway-Metriken, die Dateifreigaben betreffen. Jede Dateifreigabe verfügt über eine Reihe von zugeordneten Metriken. Einige Dateifreigabe-spezifische Metriken haben denselben Namen wie bestimmte Gateway-spezifische Metriken. Diese Metriken stellen die gleichen Messungsarten dar, beziehen sich jedoch auf die Dateifreigabe.

Geben Sie immer an, ob Sie mit einer Gateway- oder einer Dateifreigabe-Metrik arbeiten möchten, bevor Sie eine Metrik verwenden. Insbesondere müssen Sie bei der Arbeit mit Dateifreigabe-Metriken die `File share ID` angeben, die die Dateifreigabe kennzeichnet, für die Sie Metriken anzeigen möchten. Weitere Informationen finden Sie unter Verwenden von Amazon-CloudWatch-Metriken.

In der folgenden Tabelle werden die Storage Gateway Gateway-Metriken beschrieben, die Sie zum Abrufen von Informationen über Ihre Dateifreigaben verwenden können.

Metrik	Description
`CacheHitPercent`	Prozentsatz der Anwendungsleseoperationen aus den Dateifreigaben, die vom Cache

Metrik	Description
	verarbeitet werden. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Wenn keine Anwendungsleseoperationen von der Dateifreigabe vorhanden sind, wird dieser Metrikwert mit 100% angegeben. Einheiten: Prozent
`CachePercentDirty`	Der Anteil der Dateifreigabe am Gesamtpro zentsatz des Gateway-Caches, der nicht für beibehalten wurdeAWSaus. Die Stichprob e wird am Ende des Berichtszeitraums entnommen. Verwenden der`CachePercentDirty` -Metrik des Gateways, um den Gesamtprozentsatz des Gateway-Caches anzuzeigen, der nicht für beibehalten wurdeAWSaus. Einheiten: Prozent
`CachePercentUsed`	Der Beitrag der Dateifreigabe zur Gesamtpro zentsatz Auslastung des Cache-Speichers des Gateways. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Verwenden Sie die `CachePercentUsed` - Metrik des Gateways, um den Gesamtpro zentsatz der Auslastung des Cache-Speichers des Gateways anzusehen. Einheiten: Prozent

Metrik	Description
`CloudBytesUploaded`	Die Gesamtanzahl der Bytes, die das Gateway hochgeladen hatAWSwährend des Berichtszeitraums. Verwenden Sie diese Metrik mit der `Sum`-Statistik, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die IOPS-Werte zu messen. Einheiten: Byte
`CloudBytesDownloaded`	Die Gesamtanzahl der Bytes, die das Gateway heruntergeladen hatAWSwährend des Berichtszeitraums. Verwenden Sie diese Metrik mit der `Sum`-Statistik, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die Ein- und Ausgabeoperationen pro Sekunde (IOPS) zu messen. Einheiten: Byte
`ReadBytes`	Die Gesamtzahl der Byte, die in Ihren lokalen Anwendungen im Berichtszeitraum für eine Dateifreigabe gelesen wurde. Verwenden Sie diese Metrik mit der `Sum`-Statistik, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die IOPS-Werte zu messen. Einheiten: Byte

Metrik	Description
`WriteBytes`	Die Gesamtzahl in Byte, die in Ihren lokalen Anwendungen im Berichtszeitraum geschrieben wurde. Verwenden Sie diese Metrik mit der `Sum`-Statistik, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die IOPS-Werte zu messen. Einheiten: Byte

Verstehen von Datei-Gateway-Audit

Auditprotokolle bei Amazon S3 File Gateway (S3 File Gateway) stellen Ihnen Details zum Benutzerzugriff auf Dateien und Ordner innerhalb einer Dateifreigabe zur Verfügung. Sie können sie verwenden, um Benutzeraktivitäten zu überwachen und Maßnahmen zu ergreifen, wenn unangemessene Aktivitätsmuster identifiziert werden.

Operationen

In der folgenden Tabelle werden die Zugriffsvorgänge für Datei-Gateway-Auditprotokolldateien beschrieben.

Vorgangsname	Definition
Daten lesen	Den Inhalt einer Datei lesen.
Daten schreiben	Ändern Sie den Inhalt einer Datei.
Erstellen	Eine neue Datei oder einen neuen Ordner erstellen.
Umbenennen	Eine vorhandene Datei oder einen vorhanden en Ordner umbenennen.
Löschen	Eine Datei oder einen Ordner löschen.

Vorgangsname	Definition
Schreibattribute	Datei- oder Ordnermetadaten (ACLs, Besitzer, Gruppe, Berechtigungen) aktualisieren.

Attribute

In der folgenden Tabelle werden Zugriffsattribute für S3 File Gateway Auditprotokolldateien beschrieben.

Attribut	Definition
`accessMode`	Die Berechtigungseinstellung für das Objekt.
`accountDomain` (nur SMB)	Die Active Directory-Domäne (AD), zu der das Konto des Clients gehört.
`accountName` (nur SMB)	Der Active Directory-Benutzername des Clients.
`bucket`	Der Name des S3-Buckets.
`clientGid` (nur NFS)	Der Bezeichner der Gruppe des Benutzers, der auf das Objekt zugreift.
`clientUid` (nur NFS)	Der Bezeichner des Benutzers, der auf das Objekt zugreift.
`ctime`	Der Zeitpunkt, zu dem der Inhalt oder die Metadaten des Objekts geändert wurden; wird vom Client festgelegt.
`groupId`	Der Bezeichner für den Gruppenbesitzer des Objekts.
`fileSizeInBytes`	Die Größe der Datei in Bytes, die vom Client zum Zeitpunkt der Dateierstellung festgelegt wird.

Attribut	Definition
`gateway`	Die Storage Gateway-ID.
`mtime`	Der Zeitpunkt, zu dem der Inhalt des Objekts geändert wurde; wird vom Client festgelegt.
`newObjectName`	Der vollständige Pfad zum neuen Objekt, nachdem es umbenannt wurde.
`objectName`	Der vollständige Pfad zum Objekt.
`objectType`	Definiert, ob es sich bei dem Objekt um eine Datei oder einen Ordner handelt.
`operation`	Der Name des Objektzugriffsvorgangs.
`ownerId`	Der Bezeichner für den Besitzer des Objekts.
`securityDescriptor` (nur SMB)	Zeigt die für ein Objekt festgelegte besitzerv erwaltete Zugriffskontrollliste (DACL) im SDDL-Format an.
`shareName`	Der Name der Freigabe, auf die zugegriffen wird.
`source`	Die ID der Dateifreigabe, die überwacht wird.
`sourceAddress`	Die IP-Adresse des Dateifreigabe-Clie ntcomputers.
`status`	Der Status der aktuellen Operation. Nur Erfolg wird protokolliert (Fehler werden protokoll iert, mit Ausnahme von Fehlern, die sich aus verweigerten Berechtigungen ergeben).
`timestamp`	Der Zeitpunkt, zu dem der Vorgang basierend auf dem Betriebssystemzeitstempel des Gateways ausgeführt wurde.

Attribut	Definition
`version`	Die Version des Auditprotokollformats.

Pro Operation protokollierte Attribute

Die folgende Tabelle enthält die Attribute des S3 File Gateway-Auditprotokolls, die bei jedem Dateizugriffsvorgang protokolliert werden.

	Daten lesen	Daten schreiben	Ordner erstellen	Datei erstellen	Benennen Sie Datei/Ordner um	Datei/Ordner löschen	Attribute schreiben (ACL ändern -Nur SMBs)	Attribute schreiben (chown)	Attribute schreiben (chmod)	Attribute schreiben (chgrp)
`access`			X	X					X	
`accoun` `main` (nur SMB)	X	X	X	X	X	X	X	X	X	X
`accoun` `me` (nur SMB)	X	X	X	X	X	X	X	X	X	X
`bucket`	X	X	X	X	X	X	X	X	X	X
`client` (nur NFS)	X	X	X	X	X	X		X	X	X

	Daten lesen	Daten schreiben	Ordner erstellen	Datei erstellen	Benennen Sie Datei/Ordner um	Datei/Ordner löschen	Attribute schreiben (ACL ändern -Nur SMBs)	Attribute schreiben (chown)	Attribute schreiben (chmod)	Attribute schreiben (chgrp)
client (nur NFS)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			X	X						
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
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		

	Daten lesen	Daten schreiben	Ordner erstellen	Datei erstellen	Benennen Sie Datei/Ordner um	Datei/Ordner löschen	Attribute schreiben (ACL ändern -Nur SMBs)	Attribute schreiben (chown)	Attribute schreiben (chmod)	Attribute schreiben (chgrp)
`securi escrip` (nur 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
`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

Warten eines Gateways

Zu den Aufgaben im Rahmen der Gateway-Wartung zählen die Konfiguration von Cache-Speicher und Upload-Puffer-Speicher sowie allgemeine Wartungsaufgaben im Hinblick auf die Gateway-Leistung. Diese Aufgaben sind für alle Gateway-Typen gleich.

Themen

Herunterfahren Ihrer Gateway-VM

Es kann z. B. erforderlich sein, die Gateway-VM zu Wartungszwecken herunterzufahren oder neu zu starten, etwa wenn ein Patch auf Ihren Hypervisor angewendet wird. Bevor Sie das Gateway stoppen, müssen Sie zunächst die VM anhalten. Für das File Gateway fahren Sie einfach Ihre VM herunter. In diesem Abschnitt geht es hauptsächlich um das Starten und Anhalten Ihres Gateways über die Storage Gateway -Managementkonsole. Beachten Sie jedoch, dass Sie das Gateway auch über die lokale Konsole oder Storage Gateway Gateway-API anhalten können. Denken Sie daran, Ihr Gateway neu zu starten, wenn Sie Ihre VM einschalten.

Es kann z. B. erforderlich sein, die Gateway-VM zu Wartungszwecken herunterzufahren oder neu zu starten, etwa wenn ein Patch auf Ihren Hypervisor angewendet wird. Für das File Gateway fahren Sie einfach Ihre VM herunter. Sie beenden das Gateway nicht. In diesem Abschnitt geht es hauptsächlich um das Starten und Anhalten Ihres Gateways über die Storage Gateway -Managementkonsole. Beachten Sie jedoch, dass Sie das Gateway auch über die lokale Konsole oder Storage Gateway Gateway-API anhalten können. Denken Sie daran, Ihr Gateway neu zu starten, wenn Sie Ihre VM einschalten.

- Gateway-VM-lokale Konsole — siheAusführen von Wartungsaufgaben in der lokalen Konsoleaus.
- Storage Gateway API—sieheShutdownGateway

Verwalten lokaler Festplatten für Ihr Storage Gateway

Die virtuelle Maschine (VM) des Gateways verwendet die lokalen Festplatten, die Sie vor Ort zuweisen, als Puffer und Speicher. Gateways, die auf Amazon EC2 EC2-Instances erstellt wurden, verwenden Amazon EBS -Volumes als lokale Festplatten.

Themen

Entscheiden der Menge des lokalen Festplattenspeichers

Sie müssen die Anzahl und Größe von Festplatten bestimmen, die Sie Ihrem Gateway zuweisen möchten. Das Gateway benötigt folgenden zusätzlichen Speicher:

File-Gateways benötigen mindestens eine Festplatte als Cache. In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt. Nach dem Einrichten des Gateways können Sie entsprechend der steigenden Auslastung weiteren lokalen Speicher zuweisen.

Lokaler Speicher	Description	Gateway-Typ
Cache-Speicher	Der Cache-Speicher fungiert wie der dauerhafte Vor-Ort-Speicher für Daten mit ausstehendem Upload anAmazon S3 oder Dateisyst em.	• File Gateways

> **Note**
>
> Zugrunde liegende physische Speicherressourcen werden als Datenspeicher in VMware dargestellt. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-Dateien. Wenn Sie eine lokale Festplatte bereitstellen (z. B. zur

Verwendung als Cache-Speicher), haben Sie die Möglichkeit, die virtuelle Festplatte im gleichen Datenspeicher wie die VM oder in einem anderen Datenspeicher zu speichern. Wenn Sie über mehr als einen Datenspeicher verfügen, sollten Sie unbedingt einen Datenspeicher als Cache-Speicher wählen. Ein Datenspeicher, der nur durch eine zugrunde liegende physische Festplatte oder durch eine leistungsfähige RAID-Konfiguration wie RAID 1 gesichert wird, kann in einigen Situationen zu schlechter Leistung führen, wenn er beide Cache-Speicher verwendet Dies gilt auch, wenn die Sicherung ist eine weniger leistungsfähige RAID-Konfiguration wie RAID 1 ist.

Nach der ersten Konfiguration und Bereitstellung Ihres Gateways können Sie den lokalen Speicher anpassen, indem Sie Festplatten für den Cache-Speicher hinzufügen.

Bestimmen der Größe des zuweisenden Cache-Speichers

Ihr Gateway nutzt seinen Cache-Speicher, um Zugriff mit niedriger Latenz auf Daten bereitzustellen, auf die kürzlich zugegriffen wurde. Der Cache-Speicher fungiert wie der dauerhafte Vor-Ort-Speicher für Daten mit ausstehendem Upload anAmazon S3 oder Dateisystem. Weitere Informationen dazu, wie Sie Ihre Cache-Speichergröße abschätzen können, finden Sie unter Verwalten lokaler Festplatten für Ihr Storage Gateway.

Sie können anfänglich diese Schätzung für die Bereitstellung von Festplatten für den Cache-Speicher verwenden. Anschließend können Sie die Betriebsmetriken von Amazon CloudWatch verwenden, um die Cache-Speichernutzung zu überwachen und bei Bedarf mithilfe der Konsole mehr Speicher bereitzustellen. Weitere Informationen zur Verwendung der Metriken und dem Einrichten von Alarmen finden Sie unter Leistung.

Hinzufügen von Cache-Speicher

Wenn sich Ihre Anwendung ändern, können Sie die Cache-Speicherkapazität des Gateways erhöhen. Sie können mehr Cache-Kapazität zu Ihrem Gateway hinzufügen, ohne die laufenden Gateway-Funktionen zu unterbrechen. Wenn Sie mehr Speicherkapazität hinzufügen, tun Sie dies bei laufender Gateway-VM.

Important

Wenn Sie einen Cache zu einem vorhandenen Gateway hinzufügen, müssen neue Festplatten auf Ihrem Host (Hypervisor- oder Amazon EC2 EC2-Instance) erstellt werden.

> Ändern Sie nicht die Größe von vorhandenen Festplatten, wenn die Festplatten zuvor bereits als Cache zugewiesen wurden. Entfernen Sie keine Cache-Festplatten, die als Cache-Speicher zugewiesen wurden.

Im folgenden Verfahren wird gezeigt, wie Sie Speicher für Ihr Gateway konfigurieren oder zwischenspeichern.

So fügen Sie Speicher hinzu und konfigurieren einen Cache-Speicher

1. Stellen Sie einen neuen Datenträger in Ihrem Host bereit (Hypervisor- oder Amazon EC2 EC2-Instance). Weitere Informationen darüber, wie Sie einen Datenträger in einem Hypervisor bereitstellen, finden Sie in Ihrem Hypervisor-Benutzerhandbuch. Sie konfigurieren diesen Datenträger als Cache-Speicher.
2. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
3. Wählen Sie im Navigationsbereich Gateways aus.
4. Wählen Sie im Menü Actions (Aktionen) die Option Edit local disks (Lokale Datenträger bearbeiten) aus.
5. Identifizieren Sie im Dialogfeld „Edit local disks“ die Festplatten, die Sie bereitgestellt haben, und entscheiden Sie, welche als Cache-Speicher verwendet werden sollen.

   Wenn Ihre Festplatten nicht angezeigt werden, klicken Sie auf Refresh (Aktualisieren).
6. Wählen Sie Save (Speichern), um die Konfigurationseinstellungen zu speichern.

Verwenden von kurzlebigem Speicher mit EC2-Gateways

In diesem Abschnitt werden die Schritte zum Verhindern von Datenverlust bei Auswahl eines flüchtigen Datenträgers als Speicherort für Ihren Gateway-Cache beschrieben.

Flüchtige Datenträger stellen für Ihre Amazon EC2 EC2-Instance temporären Speicher auf Blockebene bereit. Flüchtige Datenträger eignen sich ideal als temporärer Speicher für Daten, die sich häufig ändern, wie beispielsweise Daten in einem Gateway-Cache-Speicher. Wie Sie Ihren Gateway in Amazon EC2 Amazon Machine Image starten und der Instance-Typ, den Sie ausgewählt haben, flüchtigen Speicher unterstützt, wird der Datenträger automatisch aufgelistet und Sie können einen der Datenträger zum Speichern von Daten in Ihrem Gateway-Cache auswählen. Weitere

Informationen finden Sie unterAmazon EC2-Instance-SpeicherimAmazon EC2-Benutzerhandbuch für Linux-Instancesaus.

Anwendungs-Schreibvorgänge auf die Datenträger werden im Cache synchron gespeichert und asynchron in dauerhaften Speicher in Amazon S3 hochgeladen. Wenn die im flüchtigen Speicher gespeicherten Daten verlorengehen, weil eine Amazon EC2 EC2-Instance angehalten wird, bevor der Daten-Upload abgeschlossen wurde, können die Daten verlorengehen, die sich noch im Cache befinden und noch nicht auf Amazon S3 hochgeladen wurden. Sie können diese Datenverluste verhindern, indem Sie diese Schritte befolgen, bevor Sie die EC2-Instance starten oder anhalten, die Ihren Gateway hostet.

> **Note**
>
> Wenn Sie flüchtigen Speicher verwenden und Ihr Gateway anhalten und starten, ist das Gateway dauerhaft offline. Dies geschieht, weil der physische Speicherdatenträger ersetzt wird. Dieses Problem kann nicht umgangen werden. Daher müssen Sie das Gateway löschen und ein neues auf einer neuen EC2-Instance aktivieren.

Diese Schritte im folgenden Verfahren gelten speziell für File Gateways.

So verhindern Sie Datenverlust in File Gateways, die flüchtige Datenträger verwenden

1. Halten Sie alle Prozesse an, die in die Dateifreigabe schreiben.
2. Abonnieren Sie die Benachrichtigungen von CloudWatch Events. Weitere Informationen finden Sie unter Benachrichtigungen zu Dateioperationen erhalten.
3. Rufen Sie dieNotifyWhenUploaded APIum benachrichtigt zu werden, wenn Daten, die geschrieben wurden, bis der flüchtige Speicher unterbrochen wurde, dauerhaft in Amazon S3 gespeichert wurden.
4. Warten Sie, bis der API-Vorgang abgeschlossen wurde und Sie eine Benachrichtigungs-ID erhalten.

   Sie erhalten ein CloudWatch-Ereignis mit derselben Benachrichtigungs-ID.
5. Stellen Sie sicher, dass die `CachePercentDirty`-Metrik für Ihre Dateifreigabe 0 ist. Dies bestätigt, dass alle Ihre Daten in Amazon S3 geschrieben wurden. Informationen zu Metriken für Dateifreigaben finden Sie unter Datenfreigabe-Metriken verstehen.
6. Sie können jetzt das File Gateway ohne das Risiko eines Datenverlusts neu starten oder anhalten.

Verwalten der Bandbreite für Ihr Amazon S3 S3-Datei-Gateway

Sie können den Upload-Durchsatz von Ihrem Gateway aufAWSSo steuern Sie die Netzwerkbandbreite, die das Gateway verwendet. Standardmäßig verfügt ein aktiviertes Gateway über keine Ratenlimits.

Sie können einen Zeitplan für die Bandbreitenrate konfigurieren, indem Sie dieAWS Management Console, einAWSDas Software Development Kit (SDK) oder dasAWS Storage GatewayAPI (sieheupdateBandWidthrateLimitScheduleimAWSStorage Gateway Gateway-API.). Mit einem Zeitplan für das Bandbreitenratenlimit können Sie Limits so konfigurieren, dass sie sich während des Tages oder der Woche automatisch ändern. Weitere Informationen finden Sie unter Anzeigen und bearbeiten Sie den Zeitplan für die Bandbreitenrate für Ihr Gateway mithilfe der Storage Gateway Gateway-Konsole.

> **Note**
>
> Das Konfigurieren von Bandbreitenratenlimits und -plänen wird derzeit für den Amazon FSx File Gateway-Typ nicht unterstützt.

Themen

Anzeigen und bearbeiten Sie den Zeitplan für die Bandbreitenrate für Ihr Gateway mithilfe der Storage Gateway Gateway-Konsole

In diesem Abschnitt wird beschrieben, wie Sie den Zeitplan für das Bandbreitenlimit für das Gateway anzeigen und bearbeiten.

So zeigen Sie einen Zeitplan für das Bandbreitenlimit an und bearbeiten ihn

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.

2. Wählen Sie im linken Navigationsbereich-GatewaysWählen Sie dann das Gateway aus, das Sie verwalten möchten.
3. FürAktionen, wählenZeitplan für Bandbreitenratenlimits bearbeitenaus.

   Der aktuelle Zeitplan des Gateways für Bandbreiten-Raten-Limit wird auf derZeitplan für Bandbreitenratenlimits bearbeitenangezeigten. Standardmäßig hat ein neues Gateway keine definierten Bandbreitenratengrenzwerte.
4. (Optional) Wählen SieNeues Bandbreitenratenlimit hinzufügenum dem Zeitplan ein neues konfigurierbares Intervall hinzuzufügen. Geben Sie für jedes hinzugefügte Intervall die folgenden Informationen ein:

   - Upload-rate— Geben Sie das Upload-Ratenlimit in Megabit pro Sekunde (Mbit/s) ein. Der Mindestwert beträgt 100 Mbit/s.
   - Wochentage— Wählen Sie den Tag oder die Tage in jeder Woche aus, an denen das Intervall angewendet werden soll. Sie können das Intervall an Wochentagen (Montag bis Freitag), am Wochenende (Samstag und Sonntag), an jedem Wochentag oder an einem bestimmten Tag pro Woche anwenden. Um das Bandbreitenlimit gleichmäßig und konstant an allen Tagen und zu jeder Zeit anzuwenden, wählen SieKein Zeitplanaus.
   - Beginnzeit— Geben Sie die Startzeit für das Bandbreitenintervall ein, indem Sie das HH:MM-Format und den Zeitzonen-Offset von UTC für Ihr Gateway verwenden.

     > **Note**
     >
     > Ihr Bandbreitenrate-Limit-Intervall beginnt zu Beginn der Minute, die Sie hier angeben.
   - Endzeit— Geben Sie die Endzeit für das Bandbreitenintervall ein, indem Sie das HH:MM-Format und den Zeitzonen-Offset von GMT für Ihr Gateway verwenden.

     > **Important**
     >
     > Das Bandbreiten-Grenz-Intervall endet am Ende der hier angegebenen Minute. Um ein Intervall zu planen, das am Ende einer Stunde endet, geben Sie**59**aus.
     > Um aufeinanderfolgende kontinuierliche Intervalle zu planen, die zu Beginn der Stunde ohne Unterbrechung zwischen den Intervallen übergehen, geben Sie ein**59**für die Endminute des ersten Intervalls. Geben Sie ein.**00**für die Startminute des nachfolgenden Intervalls.

5. (Optional) Wiederholen Sie den vorherigen Schritt bei Bedarf, bis der Zeitplan für die Bandbreitenlimits abgeschlossen ist. Wenn Sie ein Intervall aus Ihrem Zeitplan löschen müssen, wählen SieRemoveaus.

> **Important**
>
> Bandbreitenrate-Grenzintervalle können sich nicht überlappen. Die Startzeit eines Intervalls muss nach der Endzeit eines vorhergehenden Intervalls und vor der Startzeit eines folgenden Intervalls erfolgen.

6. Wenn Sie fertig sind, wählen SieSpeichern Sie die Änderungenaus.

Aktualisieren von Gateway-Bandbreitenlimits mitAWS SDK für Java

Durch die programmgesteuerte Aktualisierung von Bandbreitenlimits können Sie diese Limits automatisch über einen bestimmten Zeitraum hinweg anpassen, z. B. durch die Verwendung von geplanten Aufgaben. Im folgenden Beispiel wird gezeigt, wie Sie die Bandbreitenlimits eines Gateways mit aktualisierenAWS SDK für Javaaus. Wenn Sie den Beispielcode verwenden möchten, sollten Sie mit der Ausführung einer Java-Konsolenanwendung vertraut sein. Weitere Informationen finden Sie unter Erste Schritte im AWS SDK für Java-Entwicklerhandbuch.

Example : Aktualisieren von Gateway-Bandbreitenlimits mitAWS SDK für Java

Mit dem folgenden Java-Codebeispiel werden die Bandbreitenlimits eines Gateways aktualisiert. Um diesen Beispielcode verwenden zu können, müssen Sie den Service-Endpunkt, den Amazon-Ressourcennamen (ARN) des Gateways sowie das Upload-Limit angeben. Für eine ListeAWSDienstendpunkte, die Sie mit Storage Gateway verwenden können, sieheAWS Storage GatewayEndpunkte und KontingenteimAWS– Allgemeine Referenzaus.

```
    import java.io.IOException;

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

    import java.util.Arrays;
```

```
    import java.util.Collections;
    import java.util.List;

    public class UpdateBandwidthExample {

        public static AWSStorageGatewayClient sgClient;

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

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

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

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

            // Create a storage gateway client
            sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

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

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

        }

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

```
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

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

Aktualisieren von Gateway-Bandbreitenlimits mitAWS SDK für .NET

Durch die programmgesteuerte Aktualisierung von Bandbreitenlimits können Sie diese Limits automatisch über einen bestimmten Zeitraum hinweg anpassen, z. B. durch die Verwendung von geplanten Aufgaben. Im folgenden Beispiel wird gezeigt, wie Sie die Bandbreitenlimits eines Gateways mit aktualisierenAWSSoftware Development Kit (SDK) für .NET. Wenn Sie den Beispielcode verwenden möchten, sollten Sie mit der Ausführung einer .NET-Konsolenanwendung vertraut sein. Weitere Informationen finden Sie unter Erste Schritte im AWS SDK für .NET-Entwicklerhandbuch.

Example : Aktualisieren von Gateway-Bandbreitenlimits mitAWS SDK für .NET

Mit dem folgenden C#-Codebeispiel werden die Bandbreitenlimits eines Gateways aktualisiert. Um diesen Beispielcode verwenden zu können, müssen Sie den Service-Endpunkt, den Amazon-Ressourcennamen (ARN) des Gateways sowie das Upload-Limit angeben. Für eine

ListeAWSDienstendpunkte, die Sie mit Storage Gateway verwenden können, sieheAWS Storage GatewayEndpunkte und KontingenteimAWS– Allgemeine Referenzaus.

```
    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());
                }
            }
        }
    }
```

Aktualisieren von Gateway-Bandbreitenlimits mitAWS Tools for Windows PowerShell

Durch die programmgesteuerte Aktualisierung von Bandbreitenlimits können Sie diese Limits automatisch über einen bestimmten Zeitraum hinweg anpassen, z. B. durch die Verwendung von geplanten Aufgaben. Im folgenden Beispiel wird gezeigt, wie Sie die Bandbreitenlimits eines Gateways mit aktualisierenAWS Tools for Windows PowerShellaus. Wenn Sie den Beispielcode verwenden möchten, sollten Sie mit der Ausführung eines PowerShell-Skripts vertraut sein. Weitere Informationen finden Sie unterErste SchritteimAWS Tools for Windows PowerShell-Benutzerhandbuchaus.

Example : Aktualisieren von Gateway-Bandbreitenlimits mitAWS Tools for Windows PowerShell

Mit dem folgenden PowerShell-Skriptbeispiel werden die Bandbreitenlimits eines Gateways aktualisiert. Um dieses Beispielskript verwenden zu können, müssen Sie den Amazon-Ressourcennamen (ARN) des Gateways sowie das Uploadlimit angeben.

```
    <#
    .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)
```

Verwalten von Gateway-Updates über die AWS Storage Gateway-Konsole

Storage Gateway veröffentlicht in regelmäßigen Abständen wichtige Software-Updates für Ihr Gateway. Sie können Updates auch in der Storage Gateway -Managementkonsole manuell anwenden oder warten, bis die Updates während des konfigurierten Wartungszeitplans automatisch angewendet werden. überprüft Storage Gateway jede Minute, ob Updates vorliegen, führt jedoch Wartung und Neustart nur durch, wenn Updates vorhanden sind.

Gateway-Software-Releases enthalten regelmäßig Betriebssystem-Updates und Sicherheitspatches, die vonAWSaus. Diese Updates werden normalerweise alle sechs Monate veröffentlicht und werden im Rahmen des normalen Gateway-Aktualisierungsprozesses während geplanter Wartungsfenster angewendet.

> **Note**
>
> Sie sollten die Storage Gateway Gateway-Appliance als verwaltetes eingebettetes Gerät behandeln und nicht versuchen, auf ihre Installation zuzugreifen oder sie in irgendeiner Weise zu ändern. Der Versuch, Softwarepakete mit anderen Methoden als dem normalen Gateway-Update-Mechanismus zu installieren oder zu aktualisieren (z. B.

Bevor ein Update auf Ihr Gateway angewendet wird,AWSbenachrichtigt Sie mit einer Nachricht in der Storage Gateway Gateway-Konsole undAWS Health Dashboardaus. Weitere Informationen finden Sie unter AWS Health Dashboard. Die VM wird nicht neu gestartet, aber das Gateway steht für einen kurzen Zeitraum während der Aktualisierung und des Neustarts nicht zur Verfügung.

Wenn Sie das Gateway bereitstellen und aktivieren, wird standardmäßig eine wöchentliche Wartung festgelegt. Sie können den Wartungszeitplan jederzeit ändern. Wenn Updates verfügbar sind, wird auf der Registerkarte Details eine Wartungsmeldung angezeigt. Das Datum und die Uhrzeit des letzten erfolgreichen Software-Updates für Ihr Gateway werden auf der Registerkarte Details angezeigt.

So ändern Sie den Wartungsplan

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie im Navigationsmenü erst Gateways und anschließend das Gateway, für das Sie den Aktualisierungszeitplan ändern möchten.
3. Wählen Sie im Menü Actions (Aktionen) die Option Edit maintenance window (Wartungsfenster bearbeiten) aus, um das Dialogfeld „Edit maintenance start time (Wartungsstartzeit bearbeiten)“ zu öffnen.
4. Wählen Sie für Schedule (Zeitplan) die Option Weekly (Wöchentlich) oder Monthly (Monatlich) aus, um Aktualisierungen zu planen.
5. Wenn Sie Weekly (Wöchentlich) auswählen, ändern Sie die Werte für Day of the week (Tag der Woche) und Time (Zeit).

   Wenn Sie Monthly (Monatlich) auswählen, ändern Sie die Werte für Day of the month (Tag des Monats) und Time (Zeit). Wenn Sie diese Option auswählen und eine Fehlermeldung angezeigt wird, bedeutet dies, dass es sich bei Ihrem Gateway um eine ältere Version handelt, die noch nicht auf eine neuere Version aktualisiert wurde.

   > **Note**
   >
   > Der Höchstwert, der für den Tag des Monats festgelegt werden kann, ist 28. Wenn 28 ausgewählt ist, liegt die Startzeit für die Wartung am 28. Tag eines jeden Monats.

Ihre Wartungsstartzeit wird auf der Registerkarte Details für das Gateway beim nächsten Öffnen der Registerkarte Details angezeigt.

Ausführen von Wartungsaufgaben in der lokalen Konsole

Über die lokale Konsole des Hosts können Sie die folgenden Wartungsaufgaben ausführen: Aufgaben für die lokale Konsole können auf dem VM-Host- oder in der Amazon EC2 EC2-Instance ausgeführt werden. Viele der Aufgaben sind für die verschiedenen Hosts typisch, aber es gibt auch einige Unterschiede.

Themen

- Ausführen von Aufgaben in der lokalen VM-Konsole (File Gateway)
- Aufgaben auf der lokalen Amazon EC2 EC2-Konsole (Datei-Gateway) ausführen
- Zugreifen auf die lokale Konsole des Gateways
- Konfigurieren von Networkadaptern für Ihr Gateway

Ausführen von Aufgaben in der lokalen VM-Konsole (File Gateway)

Für ein lokal bereitgestelltes File Gateway können Sie die folgenden Wartungsaufgaben über die lokale Konsole des VM-Hosts ausführen. Diese Aufgaben sind VMware-, Microsoft Hyper-V- und Linux KVM-Hypervisoren (Kernel-basierte virtuelle Maschine) gemeinsam.

Themen

- Anmelden an der lokalen Konsole des File Gateways
- Konfigurieren eines HTTP-Proxys
- Konfigurieren Ihrer Gateway-Netzwerkeinstellungen
- Testen der Netzwerkkonnektivität Ihres Gateways
- Anzeigen des Ressourcenstatus Ihres Gateway-Syst
- Konfigurieren eines Network Time Protocol (NTP) -Servers für Ihr Gateway
- Ausführen von Speicher-Gateway-Befehlen auf der lokalen
- Konfigurieren von Netzwerkadaptern für Ihr Gateway

Anmelden an der lokalen Konsole des File Gateways

Sobald Sie sich an die VM anmelden können, wird der Anmeldebildschirm angezeigt. Wenn Sie zum ersten Mal an die lokale Konsole anmelden, verwenden Sie den Standard-Benutzernamen und das Standard-Passwort. Mit diesen Standard-Anmeldeinformationen haben Sie Zugriff auf Menüs, in denen sie die Gateway-Netzwerkeinstellungen konfigurieren und das Passwort aus der lokalen Konsole ändern können.AWS Storage GatewayMit können Sie ein eigenes Passwort aus der Storage Gateway Gateway-Konsole festlegen, statt es über die lokale Konsole zu ändern. Sie müssen das Standard-Passwort nicht kennen, um ein neues Passwort einzustellen. Weitere Informationen finden Sie unter Anmelden an der lokalen Konsole des File Gateways.

So melden Sie sich an die lokale Konsole des Gateways an

- Wenn Sie sich zum ersten Mal bei der lokalen Konsole anmelden, melden Sie sich unter Verwendung der Standard-Anmeldeinformationen bei der VM an. Der Standardbenutzername lautet `admin`, das Passwort ist `password`. Verwenden Sie andernfalls Ihre Anmeldeinformationen.

  > **Note**
  >
  > Wir empfehlen das Ändern des Standard-Passworts. Dies geschieht durch Ausführen des Befehls `passwd` über das Menü der lokalen Konsole (Element 6 im Hauptmenü). Weitere Informationen zum Ausführen des Befehls finden Sie unter Ausführen von Speicher-Gateway-Befehlen auf der lokalen. Sie können das Passwort auch über die Storage Gateway Gateway-Konsole festlegen. Weitere Informationen finden Sie unter Anmelden an der lokalen Konsole des File Gateways.

Festlegen des Kennworts für die lokale Konsole über die Storage Gateway

Wenn Sie sich erstmalig bei der lokalen Konsole anmelden, melden Sie sich mit den Standard-Anmeldeinformationen bei der VM an. Verwenden Sie für alle Gateway-Typen Standardanmeldeinformationen. Der Benutzername ist `admin` , das Passwort ist `password`.

Wir empfehlen, immer direkt ein neues Passwort festzulegen, wenn Sie ein neues Gateway erstellt haben. Sie können dieses Passwort aus der AWS Storage Gateway-Konsole heraus festlegen, statt die lokale Konsole zu verwenden. Sie müssen das Standard-Passwort nicht kennen, um ein neues Passwort einzustellen.

So richten Sie das Passwort der lokalen Konsole in der Storage Gateway Gateway-Konsole ein

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie im Navigationsbereich Gateways und anschließend den Gateway aus, für den Sie ein neues Passwort festlegen möchten.
3. Wählen Sie im Menü Actions (Aktionen) die Option Set Local Console Password (Passwort für lokale Konsole einrichten) aus.
4. Geben Sie in das Dialogfeld Set Local Console Password (Passwort für lokale Konsole einrichten) ein neues Passwort ein, bestätigen Sie das Passwort und wählen Sie anschließend Save (Speichern).

   Das neue Passwort ersetzt das Standard-Passwort. Storage Gateway speichert das Passwort nicht, sondern überträgt es sicher an die VM.

   > **Note**
   >
   > Das Passwort kann aus einer beliebigen Zeichenfolge bestehen und 1 bis 512 Zeichen lang sein.

Konfigurieren eines HTTP-Proxys

File Gateways unterstützen die Konfiguration eines HTTP-Proxy-Servers.

> **Note**
>
> File Gateways unterstützen als einige Proxy-Konfiguration HTTP.

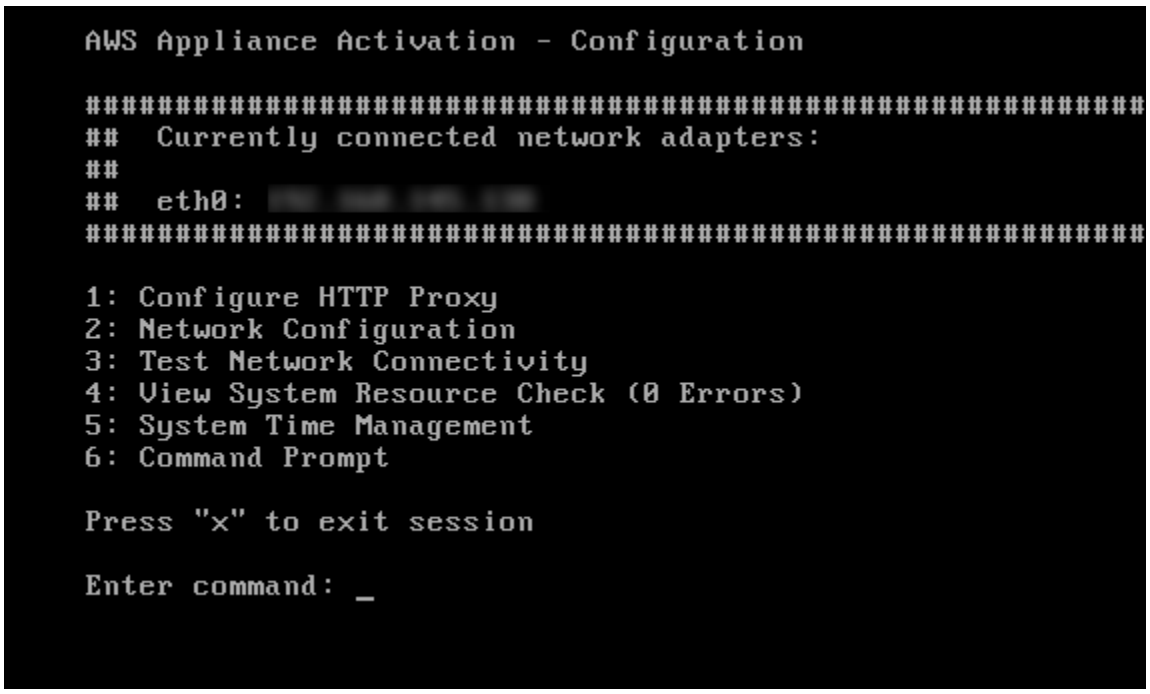
Wenn das Gateway einen Proxy-Server für die Kommunikation mit dem Internet verwenden muss, müssen Sie die HTTP-Proxy-Einstellungen für das Gateway konfigurieren. Dazu geben Sie eine IP-Adresse und die Portnummer für den Host an, auf dem der Proxy ausgeführt wird. Danach leitet Storage Gateway alleAWSEndpunkt-Datenverkehr über Ihren Proxy-Server. Die Kommunikation zwischen dem Gateway und den Endpunkten ist verschlüsselt, selbst wenn der HTTP-Proxy verwendet wird. Weitere Informationen zu den Netzwerk-Anforderungen für Ihr Gateway finden Sie unter Netzwerk- und Firewall-Anforderungen.

So konfigurieren Sie einen HTTP-Proxy für ein File Gateway

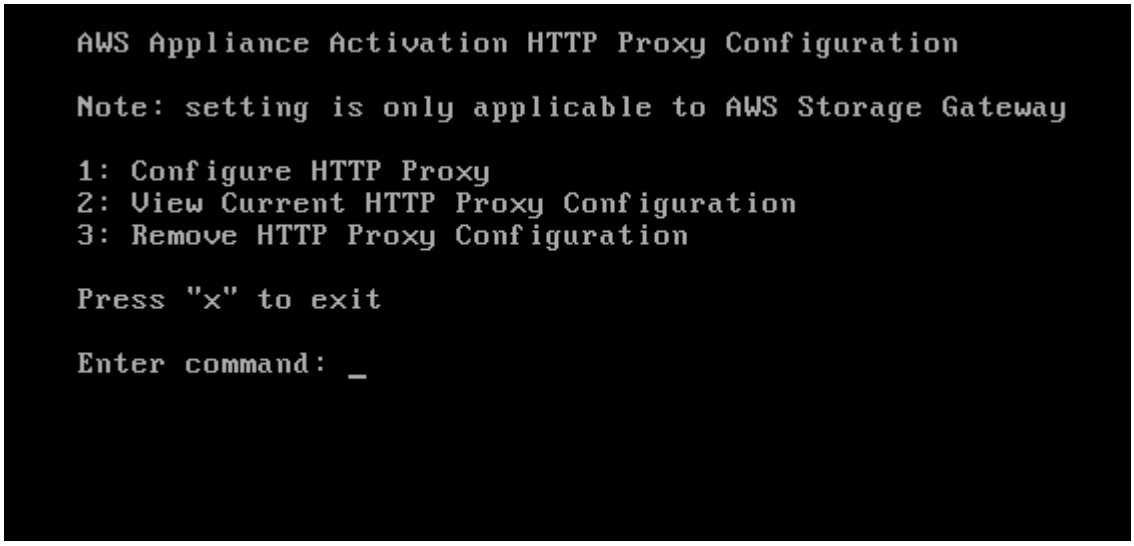
1. Melden Sie sich bei der lokalen Konsole des Gateways an:

   - Weitere Informationen zum Anmelden bei der lokalen VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden an der lokalen Konsole für die Linux-Kernel-basierte virtuelle Maschine (KVM) finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.

2. Auf derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie**1**um mit der Konfiguration des HTTP-Proxys zu beginnen.



3. Geben Sie im Menü HTTP Proxy Configuration (HTTP-Proxy-Konfiguration) **1** ein und geben Sie den Hostnamen für den HTTP-Proxy-Server ein.



Sie können über dieses Menü wie folgt andere HTTP-Einstellungen konfigurieren.

Bis	Vorgehensweise
Konfigurieren eines HTTP-Proxys	Geben Sie ei **1**.

Bis	Vorgehensweise
	Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
Anzeigen der aktuellen HTTP-Proxy-Konfiguration	Geben Sie ei **2**. Wenn kein HTTP-Proxy konfiguriert ist, wird die Meldung `HTTP Proxy not configured` angezeigt. Ist ein HTTP-Proxy konfiguriert, werden der Hostname und Port des Proxys angezeigt.
Entfernen einer HTTP-Proxy-Konfiguration	Geben Sie ei **3**. Die Meldung `HTTP Proxy Configuration Removed` wird angezeigt.

4. Starten Sie Ihre VM, um die HTTP-Konfigurationseinstellungen anzuwenden.

Konfigurieren Ihrer Gateway-Netzwerkeinstellungen

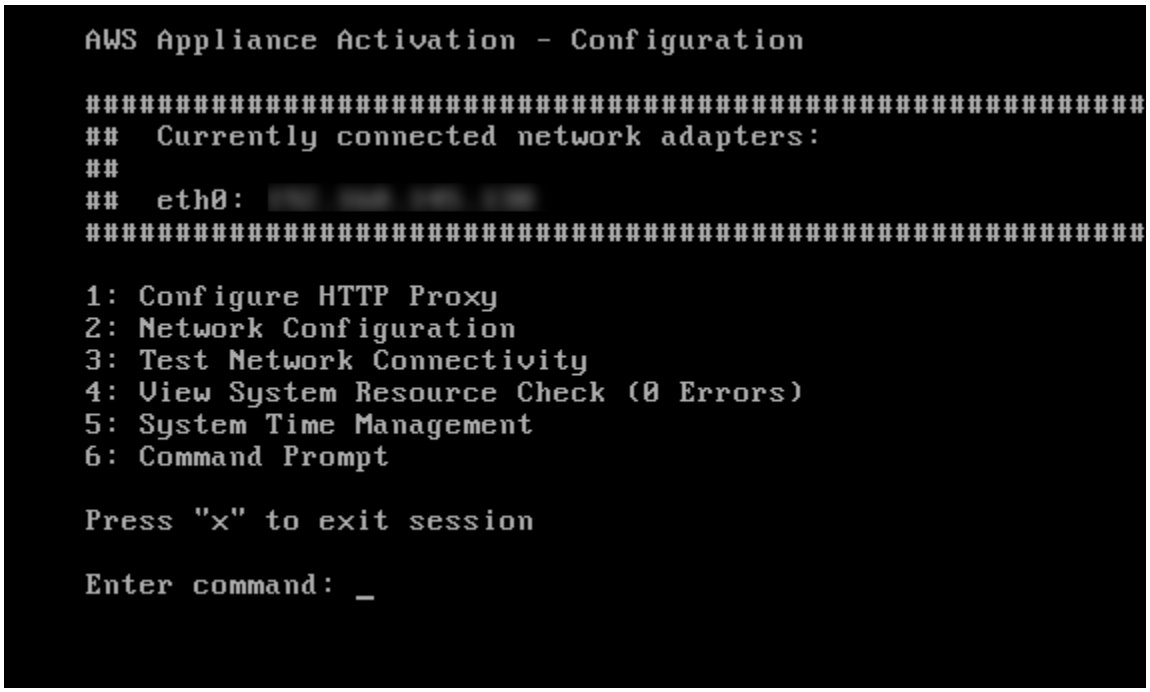
Die Standard-Netzwerkkonfiguration für das Gateway ist das Dynamic Host Configuration Protocol (DHCP). Mit dem DHCP wird Ihr Gateway automatisch einer IP-Adresse zugewiesen. In einigen Fällen müssen Sie die IP Ihres Gateways wie im Folgenden beschrieben möglicherweise manuell eine statischen IP-Adresse zuweisen.

So konfigurieren Sie Ihr Gateway zur Verwendung einer statischen IP-Adresse

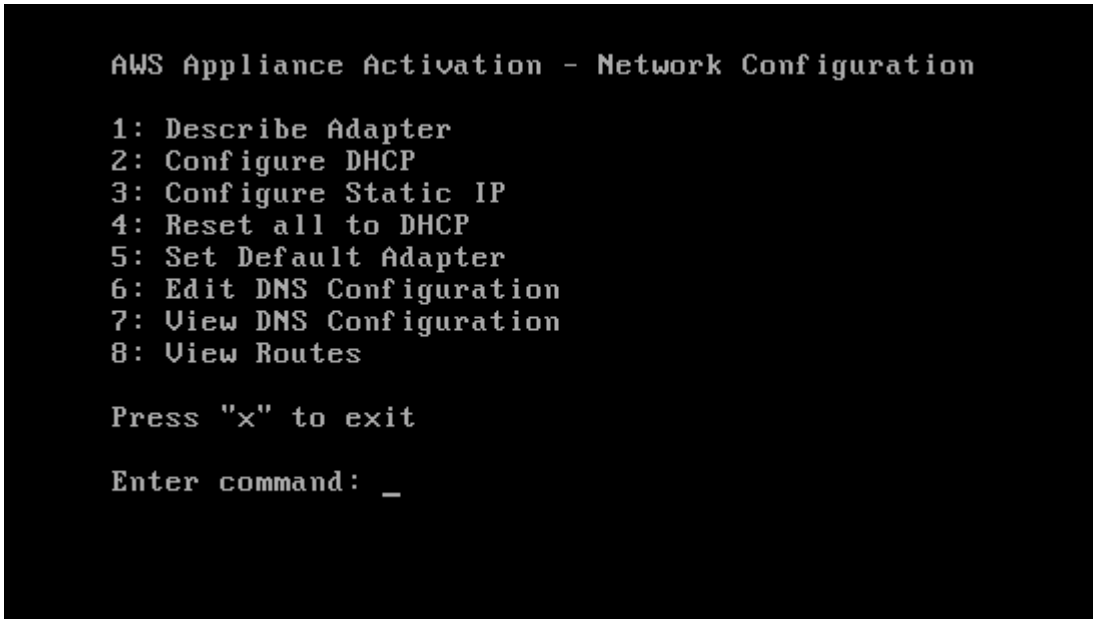
1. Melden Sie sich bei der lokalen Konsole des Gateways an:

   - Weitere Informationen zum Anmelden bei der lokalen VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.

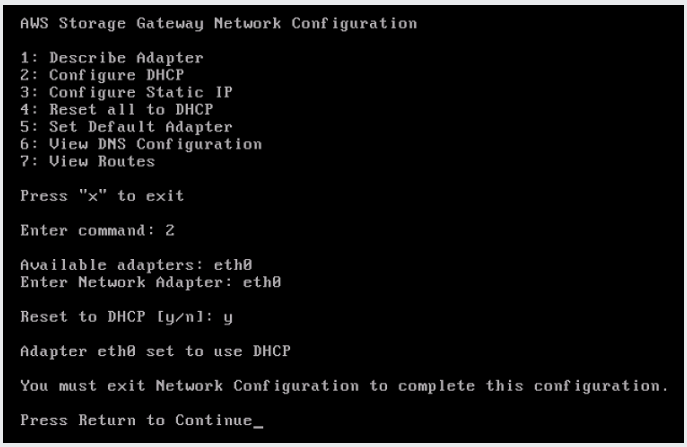
2. Auf derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie**2**um mit der Konfiguration Ihres Netzwerks zu beginnen.



3. Wählen Sie eine der folgenden Optionen im Menü Network Configuration (Netzwerkkonfiguration) aus.



Bis	Vorgehensweise
Abrufen von Informationen zum Netzwerkadapter	Geben Sie ei **1**. Eine Liste der Adapternamen wird angezeigt, und Sie werden aufgefordert, einen Adapternamen einzugeben — z. B.**eth0**aus. Wenn der von Ihnen angegebene Adapter verwendet wird, werden die folgenden Informationen zum Adapter angezeigt: • Media Access Control-Adresse (MAC) • IP-Adresse • Netzmaske • Gateway-IP-Adresse • DHCP-fähiger Status Sie verwenden denselben Adaptername für die Konfiguration einer statischen IP-Adresse (Option 3) wie für die Einrichtung des Standard-Route-Adapters Ihres Gateways (Option 5).

Bis	Vorgehensweise
Konfigurieren von DHCP	Geben Sie ei **2**. Sie werden aufgefordert, die Netzwerkschnittstelle für die Verwendung von DHCP zu konfigurieren. 

Bis	Vorgehensweise
Konfigurieren einer statischen IP-Adresse für Ihr Gateway	Geben Sie ei **3**. Sie werden aufgefordert, die folgenden Informationen zur Konfiguration einer statischen IP-Adresse einzugeben: • Netzwerkadaptername • IP-Adresse • Netzmaske • Standard-Gateway-Adresse • Primary Domain Name Service-Adresse (DNS) • Sekundäre DNS-Adresse **Important** Wenn Ihr Gateway bereits aktiviert wurde, müssen Sie es aus der Storage Gateway Gatewaykonsole beenden und neu starten, damit die Einstellungen wirksam werden. Weitere Informationen finden Sie unter Herunterfahren Ihrer Gateway-VM. Wenn Ihr Gateway mehrere Netzwerkschnittste llen verwendet, müssen Sie alle aktivierten

Bis	Vorgehensweise
	Schnittstellen für die Verwendung von DHCP- oder statischen IP-Adressen einrichten. Angenommen, Ihre Gateway-VM verwendet als DHCP konfigurierte Schnittstellen. Wenn Sie später eine Schnittstelle für eine statische IP einrichten, wird die andere Schnittstelle deaktiviert. Um die Schnittstelle in diesem Fall zu deaktivieren, müssen Sie sie für eine statische IP einrichten. Wenn beide Schnittstellen anfänglich für die Verwendung von statischen IP-Adressen eingerichtet sind und Sie das Gateway für die Verwendung von DHCP einrichten, verwenden beide Schnittstellen DHCP.
Zurücksetzen der Netzwerkkonfiguration Ihres Gateways auf DHCP	Geben Sie ei **4**. Alle Netzwerkschnittstellen sind für die Verwendung von DHCP eingerichtet. **Important** Wenn Ihr Gateway bereits aktiviert wurde, müssen Sie es aus der Storage Gatewaykonsole beenden und neu starten, damit die Einstellungen wirksam werden. Weitere Informationen finden Sie unter Herunterfahren Ihrer Gateway-VM.

Bis	Vorgehensweise
Einrichten des Standard-Routing-Adapters Ihres Gateways	Geben Sie ei **5**. Die Adapter, die für Ihr Gateway verfügbar sind, werden angezeigt und Sie werden aufgeford ert, einen der Adapter auszuwählen — z. B.**`eth0`**aus.
Bearbeiten der DNS-Konfiguration Ihres Gateways	Geben Sie ei **6**. Die verfügbaren Adapter des primären und sekundären DNS-Servers werden angezeigt. Sie werden aufgefordert, die neue IP-Adresse einzugeben.
Anzeigen der DNS-Konfiguration Ihres Gateways	Geben Sie ei **7**. Die verfügbaren Adapter des primären und sekundären DNS-Servers werden angezeigt. **Note** Bei einigen Versionen des VMware-Hypervisor können Sie die Adapterko nfiguration in diesem Menü bearbeiten.
Anzeigen von Routing-Tabellen	Geben Sie ei **8**. Die Standard-Route Ihres Gateways wird angezeigt.

Testen der Netzwerkkonnektivität Ihres Gateways

Sie können die lokale Konsole des Gateways verwenden, um Ihre Netzwerkkonnektivität zu testen. Dieser Test kann nützlich sein, wenn Sie Netzwerkprobleme mit dem Gateway beheben.

So testen Sie die Netzwerkkonnektivität Ihres Gateways

1. Melden Sie sich bei der lokalen Konsole des Gateways an:

   - Weitere Informationen zum Anmelden bei der lokalen VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Von derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie die entsprechende Zahl ein, um auszuwählenTesten der Netzwerkkonnektivitätaus.

   Wenn Ihr Gateway bereits aktiviert wurde, beginnt der Konnektivitätstest sofort. Für Gateways, die noch nicht aktiviert wurden, müssen Sie den Endpunkttyp angeben undAWS-Regionwie in den folgenden Schritten beschrieben.
3. Wenn Ihr Gateway noch nicht aktiviert ist, geben Sie die entsprechende Zahl ein, um den Endpunkttyp für Ihr Gateway auszuwählen.
4. Wenn Sie den Typ des öffentlichen Endpunkts ausgewählt haben, geben Sie die entsprechende Zahl ein, um dieAWS-RegionDas willst du testen. Für unterstützteAWS-Regionenund eine ListeAWSService-Endpoints, die Sie mit Storage Gateway verwenden können, sieheAWS Storage Gateway-Endpunkte und -KontingenteimAWS– Allgemeine Referenzaus.

Während der Test fortschreitet, wird jeder Endpunkt entweder angezeigt[BESTANDEN]oder[FEHLGESCHLAGEN]und gibt den Status der Verbindung wie folgt an:

Fehlermeldung	Description
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über eine Netzwerkv erbindung.

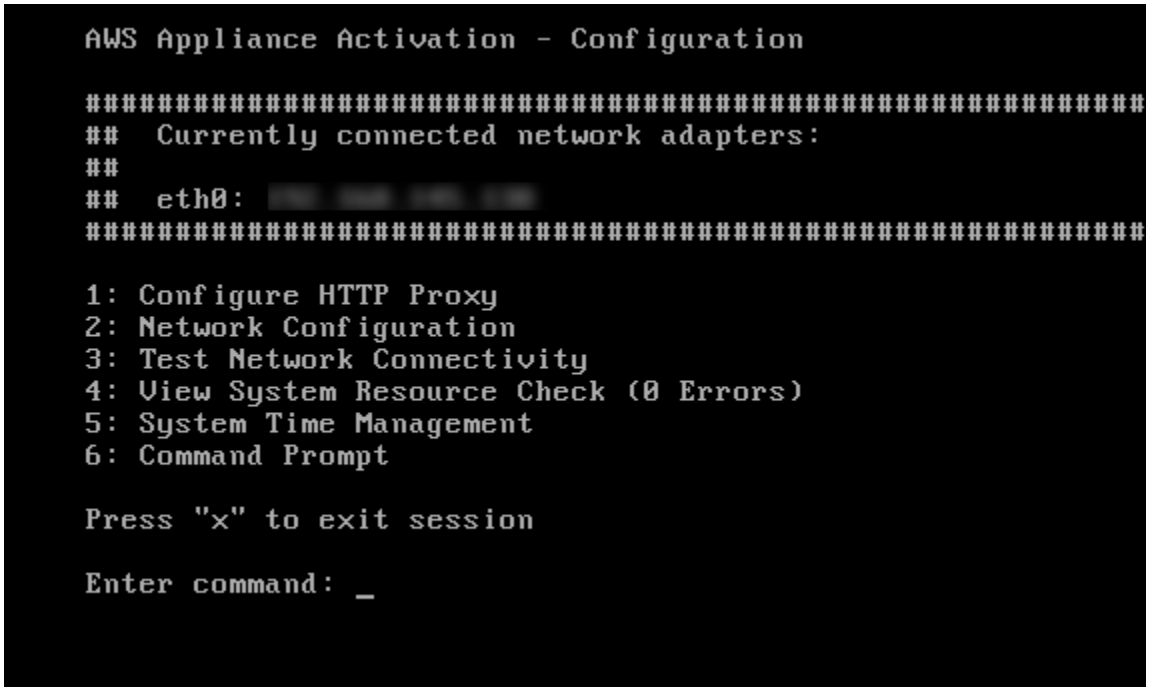
Fehlermeldung	Description
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway verfügt über keine Netzwerkk onnektivität.

Anzeigen des Ressourcenstatus Ihres Gateway-Syst

Beim Starten überprüft Ihr Gateway seine virtuellen CPU-Kerne, Stamm-Volume-Größe und RAM. Er kann dann bestimmen, ob ausreichend Systemressourcen für die ordnungsgemäße Funktionsweise Ihres Gateways verfügbar sind. Sie können die Ergebnisse dieser Prüfung auf der lokalen Gateway-Konsole anzeigen.

So zeigen Sie den Status einer Systemressourcenprüfung an

1. Melden Sie sich bei der lokalen Konsole des Gateways an:
   - Weitere Informationen zum Anmelden bei der VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. In derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie**4**So zeigen Sie die Ergebnisse einer Systemressourcenprüfung an.



Die Konsole zeigt für jede Ressource [OK], [WARNING] ([WARNUNG]) oder [FAIL] ([FEHLGESCHLAGEN]) an (siehe folgende Tabelle).

Fehlermeldung	Description
[OK]	Die Ressource hat die Systemressourcenprüfung bestanden.
[WARNING] ([WARNUNG])	Die Ressource erfüllt nicht die empfohlenen Anforderungen, aber das Gateway ist weiterhin funktionsfähig. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.
[FAIL] ([FEHLGESCHLAGEN])	Die Ressource erfüllt nicht die Mindestanforderungen. Das Gateways funktioniert möglicherweise nicht ordnungsgemäß. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.

Die Konsole zeigt die Anzahl der Fehler und Warnungen neben der Menüoption für die Ressourcenprüfung an.

Konfigurieren eines Network Time Protocol (NTP) -Servers für Ihr Gateway

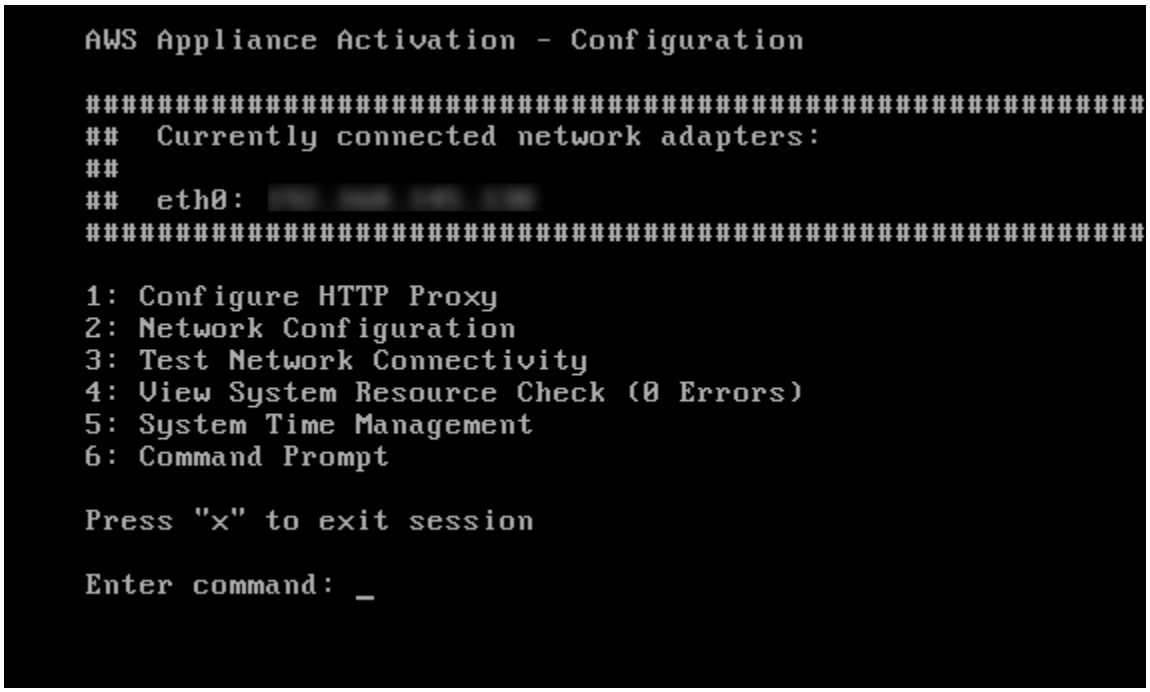
Sie können Network Time Protocol (NTP)-Serverkonfigurationen anzeigen und bearbeiten und die VM-Zeit auf dem Gateway mit Ihrem Hypervisor-Host synchronisieren.

So verwalten Sie die Systemzeit

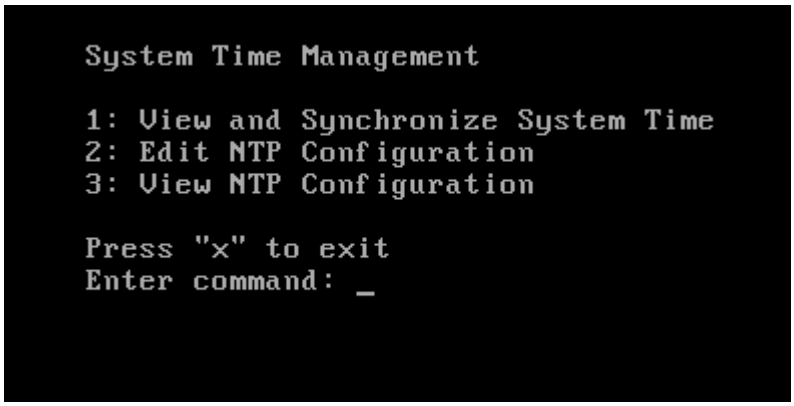
1. Melden Sie sich bei der lokalen Konsole des Gateways an:

   - Weitere Informationen zum Anmelden bei der lokalen VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.

2. In derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie**5**um die Zeit Ihres Systems zu verwalten.



3. Wählen Sie im Menü System Time Management (Systemzeit-Verwaltung) eine der folgenden Optionen aus.



Bis	Vorgehensweise
Zeigen Sie Ihre VM-Zeit an und synchroni sieren Sie sie mit der NTP-Serverzeit.	Geben Sie ei **1**. Die aktuelle Zeit der VM wird angezeigt. Ihr File Gateway bestimmt den zeitlichen Unterschi ed zwischen der Zeit des Gateways, der VM und des NTP-Servers und fordert Sie zum Synchronisieren der VM-Zeit mit der NTP-Zeit auf. Nachdem Sie Ihr Gateway bereitgestellt und aktiviert haben, kann die Gateway-VM-Zeit in manchen Fällen abweichen. Angenommen, es tritt ein längerer Netzwerkausfall auf und die Zeit Ihres Hypervisor-Netzwerks und Ihres Gateways wird nicht aktualisiert. In diesem Fall weicht die Zeit der Gateway-VM von der tatsächlichen Zeit ab. Bei einer Abweichung besteht eine Diskrepanz den angegebenen Zeiten von Vorgängen wie Snapshots und den tatsächlichen Zeiten, zu denen die Vorgänge ausgeführt wurden. Bei einem Gateway, das auf einem VMware ESXi bereitgestellt wird, reicht es aus, die Hypervisor-Host-Zeit einzustellen und die VM-Zeit mit dem Host zu synchronisieren, um eine Abweichung zu verhindern. Weitere Informati onen finden Sie unter Synchronisieren der VM-Zeit mit der Host-Zeit. Bei einem Gateway, das auf Microsoft Hyper-V bereitgestellt wird, sollten Sie die Zeit Ihrer VM in regelmäßigen Abständen überprüfe

Bis	Vorgehensweise
	n. Weitere Informationen finden Sie unter Synchronisieren der Gateway-VM-Zeit. Bei einem Gateway, das auf KVM bereitges tellt wird, können Sie die VM-Zeit mithilfe der `virsh`-Befehlszeilenschnittstelle für KVM überprüfen und synchronisieren.
Bearbeiten Ihrer NTP-Serverkonfiguration	Geben Sie ei **2**. Sie werden zur Angabe eines bevorzugten und eines sekundären NTP-Servers aufgefordert.
Anzeigen Ihrer NTP-Serverkonfiguration	Geben Sie ei **3**. Ihre NTP-Serverkonfiguration wird angezeigt.

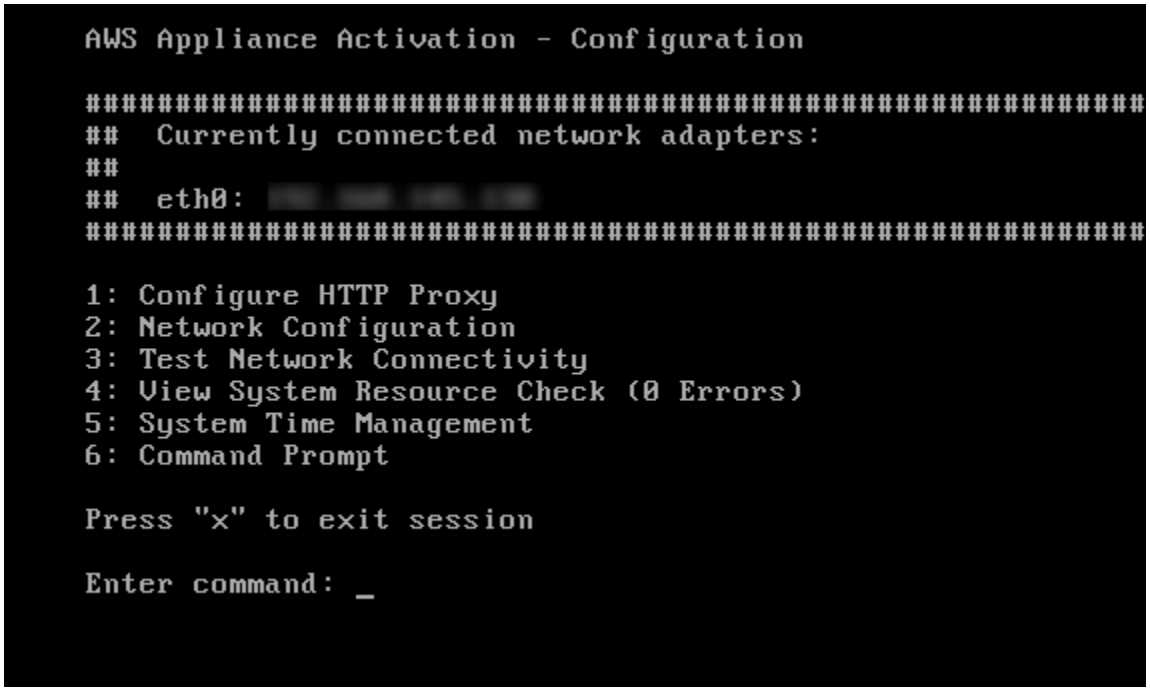
Ausführen von Speicher-Gateway-Befehlen auf der lokalen

Die lokale Konsole der VM in Storage Gateway stellt eine sichere Umgebung für die Konfiguration und Diagnose von Problemen mit dem Gateway bereit. Mithilfe der lokalen Konsolenbefehle können Sie Wartungsaufgaben wie das Speichern von Routing-Tabellen oder das Herstellen einer Verbindung mit dem Amazon Web Services Services-Support durchführen.

So führen Sie eine Konfiguration oder einen Diagnosebefehl aus

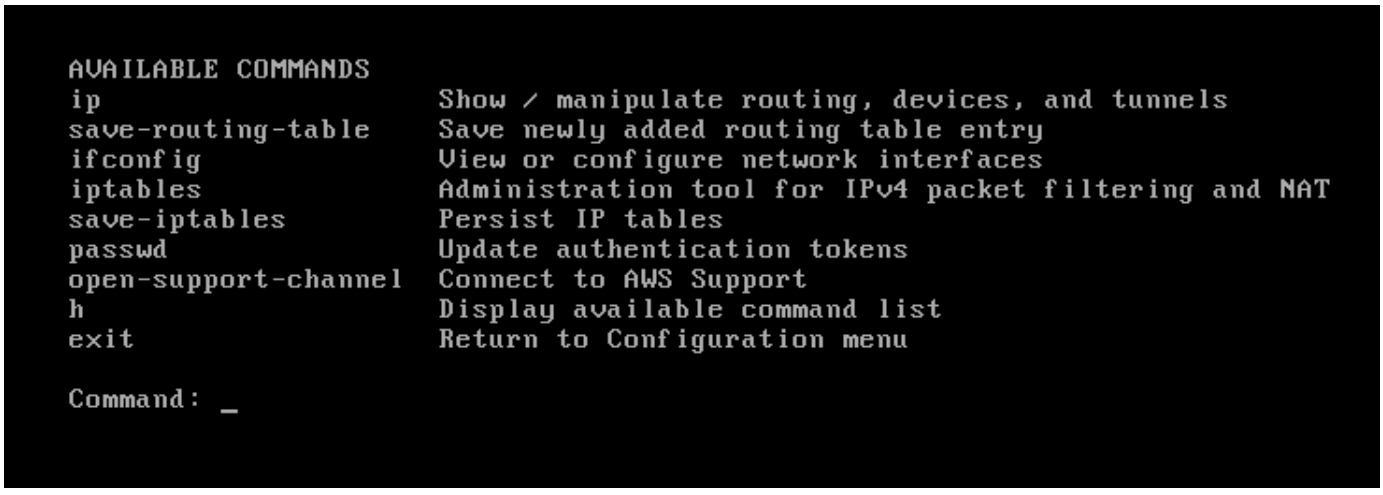
1. Melden Sie sich bei der lokalen Konsole des Gateways an:

   - Weitere Informationen zum Anmelden bei der lokalen VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Auf derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie**6**zumEingabeaufforderungaus.



3. Auf derAWSAppliance-Aktivierung - Eingabeauconsole, geben Sie**h**und drücken Sie dannErgebnisSchlüssel.

   Die Konsole zeigt das Menü AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) mit den Funktionen der Befehle an (siehe Abbildung unten).



4. Geben Sie in der Befehlszeile den Befehl ein, den Sie verwenden möchten, und befolgen Sie die Anweisungen.

Wenn Sie weitere Informationen erhalten möchten, geben Sie in der Befehlszeile den Namen des Befehls ein.

Konfigurieren von Netzwerkadaptern für Ihr Gateway

Standardmäßig ist Storage Gateway für die Verwendung eines Netzwerkadapters des Typs E1000 konfiguriert, aber Sie können Ihr Gateway auch für die Verwendung eines Netzwerkadapters des Typs VMXNET3 (10 GbE) konfigurieren. Sie können Storage Gateway auch so konfigurieren, mehr als eine IP-Adresse darauf zugreifen können. Konfigurieren Sie hierzu Ihr Gateway für die Verwendung mehrerer Netzwerkadapter.

Themen

Konfigurieren des Gateways für die Verwendung des VMXNET3-Netzwerkadapters

Storage Gateway unterstützt E1000-Netzwerkadapter in VMware ESXi- und Microsoft Hyper-V Hypervisor-Hosts. Allerdings werden VMXNET3-Netzwerkadapter (10 GbE) nur von VMware ESXi-Hypervisor unterstützt. In einem VMware ESXi-Hypervisor gehostete Gateways können jetzt so konfiguriert werden, dass sie den Adaptertyp VMXNET3 (10 GbE) verwenden. Weitere Informationen zu diesem Adapter finden Sie auf der VMware-Website.

Storage Gateway unterstützt für KVM-Hypervisor-Hosts die Verwendung von`virtio`Netzwerkgerätetreiber. Die Verwendung des E1000-Netzwerkadaptertyps für KVM-Hosts wird nicht unterstützt.

> **Important**
>
> Um VMXNET3 zu wählen, muss Ihr Gast-Betriebssystem Other Linux64 (Andere Linux64) sein.

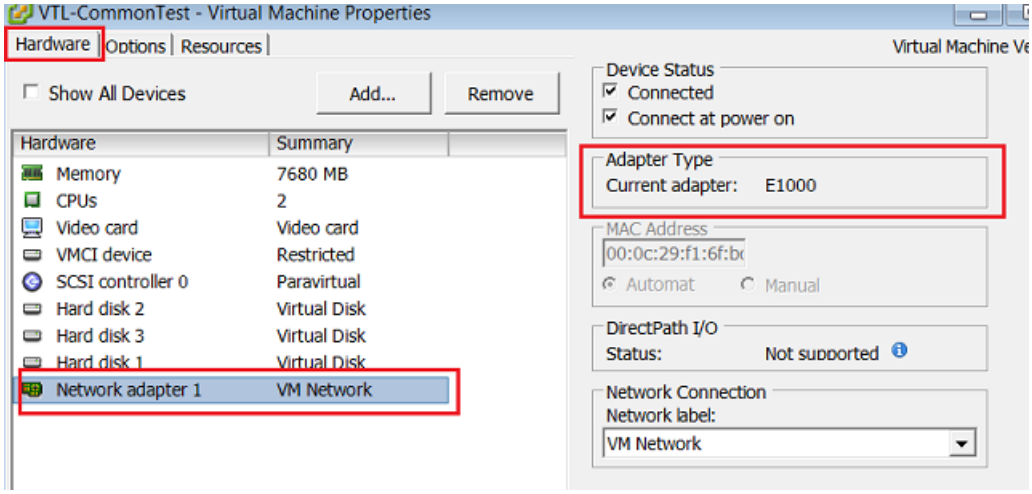
In den folgenden Abschnitten werden die Schritte beschrieben, mit denen Sie Ihr Gateway für die Verwendung eines VMXNET3-Adapter konfigurieren:

1. Entfernen Sie die Standard-E1000 Adapter.
2. Fügen Sie den VMXNET3-Adapter hinzu.
3. Starten Sie Ihr Gateway neu.
4. Konfigurieren Sie den Adapter für das Netzwerk.

Nähere Informationen über die Ausführung der einzelnen Schritte finden Sie im Folgenden.

So entfernen Sie einen Standard-E1000-Adapter und konfigurieren Ihr Gateway für die Verwendung eines VMXNET3-Adapters

1. Öffnen Sie in VMware das Kontextmenü (Klick mit der rechten Maustaste) für Ihr Gateway und wählen Sie Edit Settings (Einstellungen bearbeiten).
2. Wählen Sie im Fenster Virtual Machine Properties (Eigenschaften der virtuellen Maschine) die Registerkarte Hardware.
3. Wählen Sie für Hardware die Option Network Adapter (Netzwerkadapter). Beachten Sie, dass der aktuelle Adapter im Abschnitt Adapter Type (Adaptertyp) ein E1000 ist. Ersetzen Sie diesen Adapter durch den VMXNET3-Adapter.



4. Wählen Sie den E1000-Netzwerkadapter und wählen Sie Remove (Entfernen). In diesem Beispiel ist der E1000-Netzwerkadapter Network Adapter 1 (Netzwerkadapter 1).

> **Note**
>
> Obwohl Sie den E1000- und den VMXNET3-Netzwerkadapter in Ihrem Gateway gleichzeitig ausführen können, wird dies nicht empfohlen, da es zu Netzwerkproblemen kommen kann.

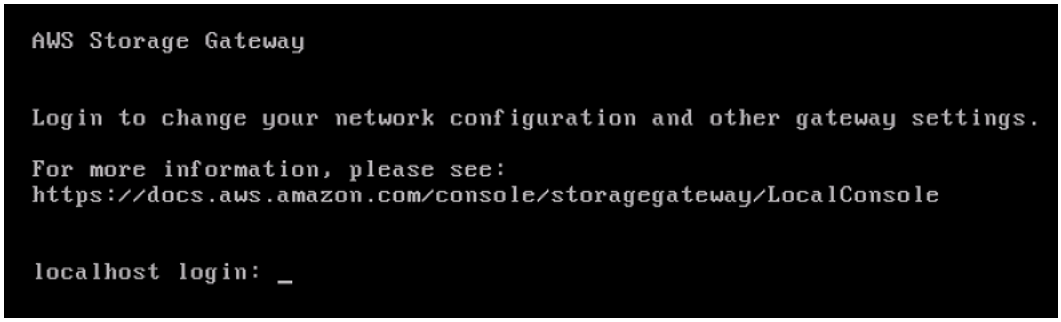
5. Wählen Sie zum Öffnen des Assistenten zum Hinzufügen von Hardware die Option Add (Hinzufügen).
6. Wählen Sie Ethernet Adapter (Ethernet-Adapter) und anschließend Next (Weiter).
7. Wählen Sie im Netzwerktyp-Assistenten **`VMXNET3`** für Adapter Type (Adaptertyp) aus und wählen Sie anschließend Next (Weiter).

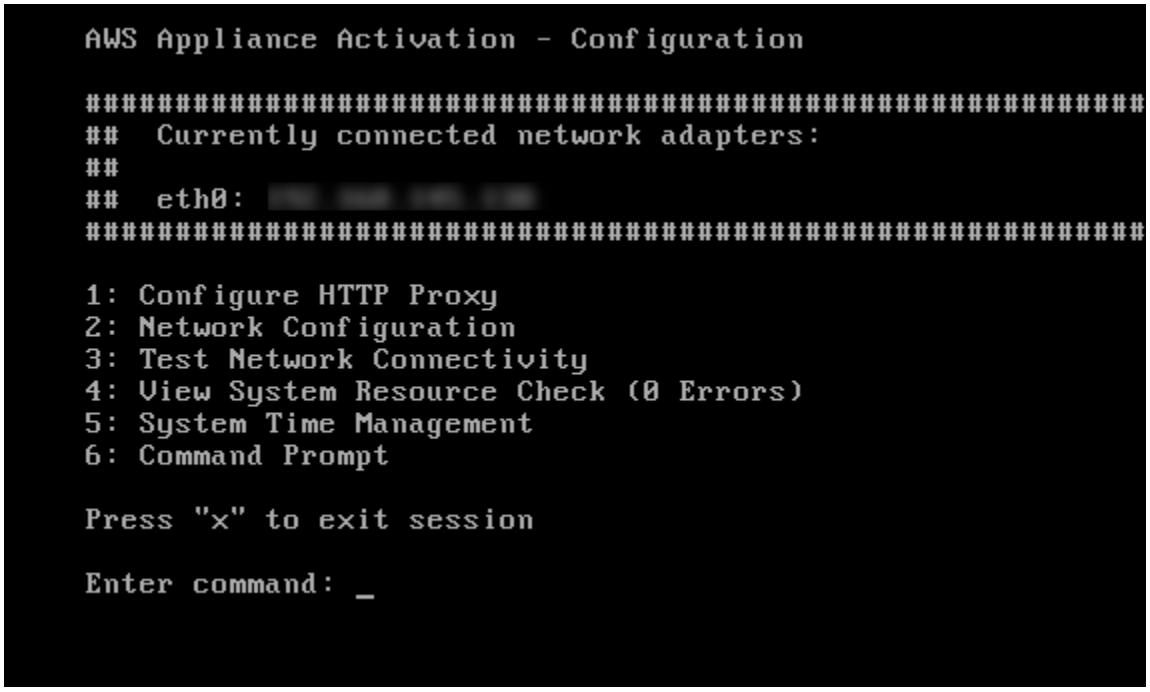
8. Prüfen Sie im Assistenten für die Eigenschaften der virtuellen Maschine im Abschnitt Adapter Type (Adaptertyp), ob Current Adapter (Aktueller Adapter) auf VMXNET3 eingestellt ist, und wählen Sie anschließend OK.
9. Deaktivieren Sie Ihr Gateway im VMware VSphere-Client.
10. Starten Sie Ihr Gateway im VMware VSphere-Client neu.

Konfigurieren Sie nach dem Neustart Ihres Gateways den Adapter neu, den Sie gerade hinzugefügt haben, um sicherzustellen, dass die Netzwerkverbindung mit dem Internet hergestellt wird.

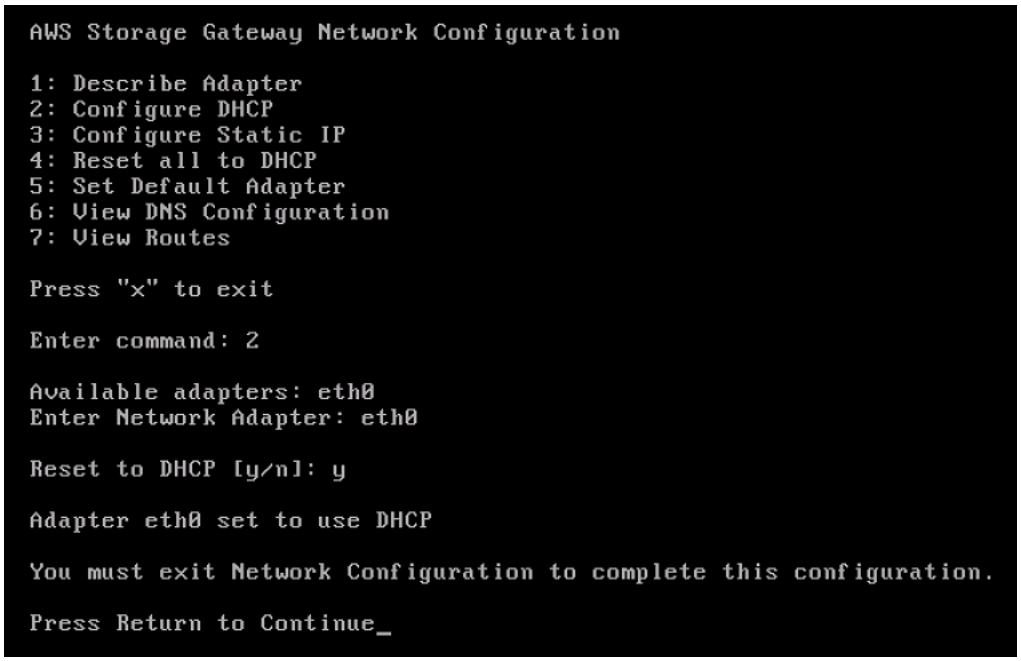
So konfigurieren Sie den Adapter für das Netzwerk

1. Wählen Sie im VSphere-Client die Registerkarte Console (Konsole), um die lokale Konsole zu starten. Verwenden Sie die Standard-Anmeldeinformationen für die Anmeldung bei der lokalen Konsole des Gateways für diese Konfigurationsaufgabe. Weitere Informationen zur Anmeldung mit den Standard-Anmeldeinformationen finden Sie unter Anmelden an der lokalen Konsole des File Gateways.





2. Geben Sie an der Eingabeaufforderung **2** ein, um Network Configuration (Netzwerkkonfiguration) auszuwählen, und drücken Sie dann **Enter**, um das Netzwerkkonfigurationsmenü zu öffnen.
3. Geben Sie an der Eingabeaufforderung **4** ein, um Reset all to DHCP (Alle auf DHCP zurücksetzen) auszuwählen. Geben Sie dann **y** (für "Yes") an der Eingabeaufforderung ein, um für alle Adapter die Verwendung des Dynamic Host Configuration Protocol (DHCP) festzulegen. Alle verfügbaren Adapter werden für die Verwendung von DHCP eingestellt.



Wenn Ihr Gateway bereits aktiviert ist, müssen Sie es über die Storage Gateway Management Console beenden und neu starten. Nach dem Neustart des Gateways müssen Sie die Netzwerkverbindung mit dem Internet testen. Weitere Informationen zum Testen der Netzwerkverbindung finden Sie unter Testen der Netzwerkkonnektivität Ihres Gateways.

Aufgaben auf der lokalen Amazon EC2 EC2-Konsole (Datei-Gateway) ausführen

Für einige Wartungsaufgaben müssen Sie sich bei der lokalen Konsole anmelden, wenn ein Gateway auf einer Amazon EC2 EC2-Instance ausgeführt wird. In diesem Abschnitt finden Sie Informationen dazu, wie Sie sich bei der lokalen Konsole anmelden und Wartungsaufgaben ausführen.

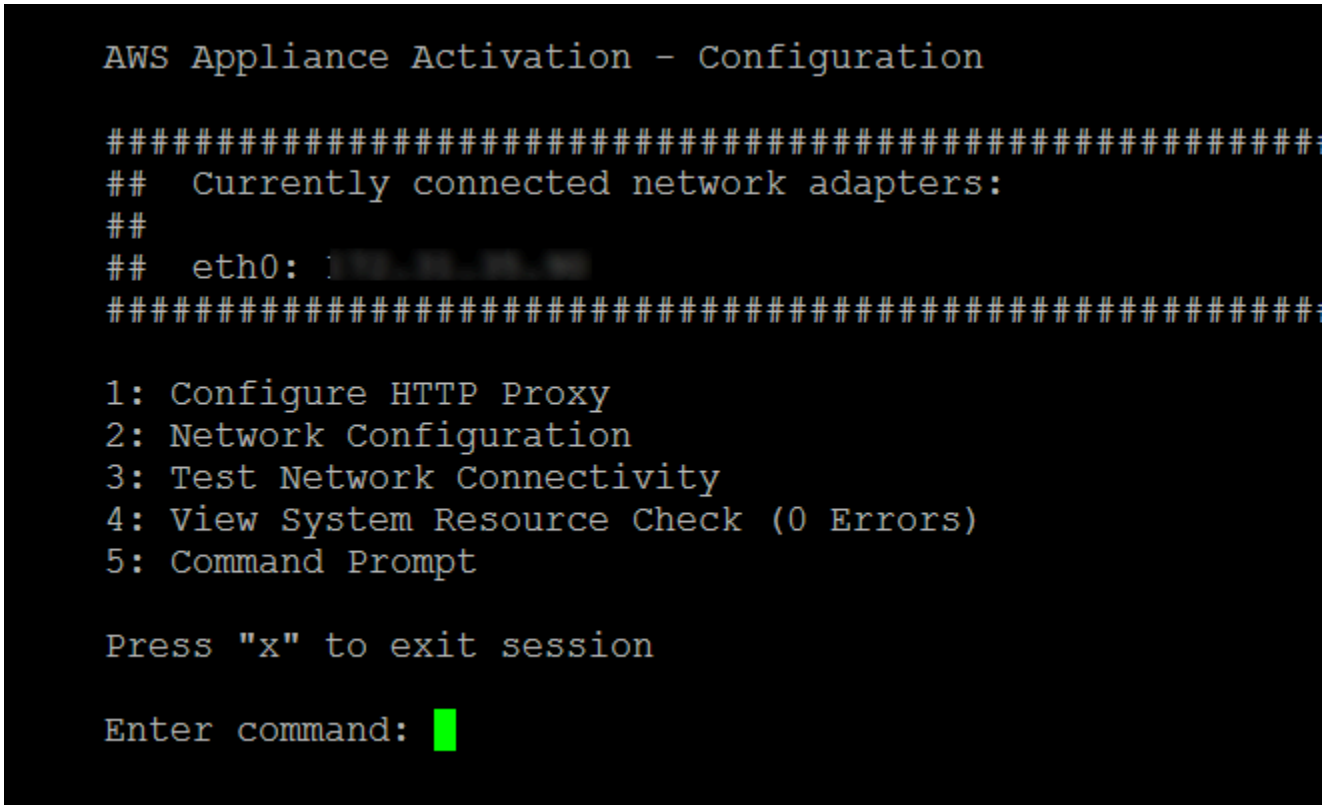
Themen

Melden Sie sich bei Ihrer lokalen Konsole des Amazon EC2 EC2-Gateways an

Sie können über einen Secure Shell (SSH) -Client eine Verbindung mit der Amazon EC2 EC2-Instance herstellen. Ausführliche Informationen hierzu finden Sie unterVerbinden Sie sich mit der InstanceimBenutzerhandbuch für Amazon EC2aus. Für diese Art des Verbindungsaufbaus benötigen Sie das SSH-Schlüsselpaar, das Sie beim Starten Ihrer Instance angegeben haben. Weitere Informationen über Amazon EC2 EC2-Schlüsselpaare finden Sie unterAmazon EC2-SchlüsselpaareimBenutzerhandbuch für Amazon EC2

So melden Sie sich bei der lokalen Konsole des Gateways an

1. Melden Sie sich bei der lokalen Konsole an. Wenn Sie auf einem Windows-Computer eine Verbindung zu Ihrer EC2-Instance herstellen, melden Sie sich als admin an.
2. Nachdem Sie sich angemeldet haben, sehen Sie dieAWSAppliance-Aktivierung - KonfigurationHauptmenü, wie im folgenden Screenshot gezeigt.



Für weitere Informationen über	Siehe folgendes Thema
Konfigurieren eines HTTP-Proxys für Ihr Gateway	Routing Ihres auf EC2 bereitgestellten Gateway über einen HTTP-Proxy
Konfigurieren von Netzwerkeinstellungen für Ihr Gateway	Testen der Netzwerkkonnektivität Ihres Gateways
Testen der Netzwerkverbindung	Testen der Netzwerkkonnektivität Ihres Gateways
Anzeigen einer Systemressourcenprüfung	Melden Sie sich bei Ihrer lokalen Konsole des Amazon EC2 EC2-Gateways an.
Ausführen von Storage Gateway Gateway-	Ausführen von Storage Gateway Gateway-Befehlen auf der

Wenn Sie das Gateway beenden möchten, geben Sie **0** ein.

Zum Beenden der Konfigurationssitzung geben Sie **x** ein, sodass das Menü beendet wird.

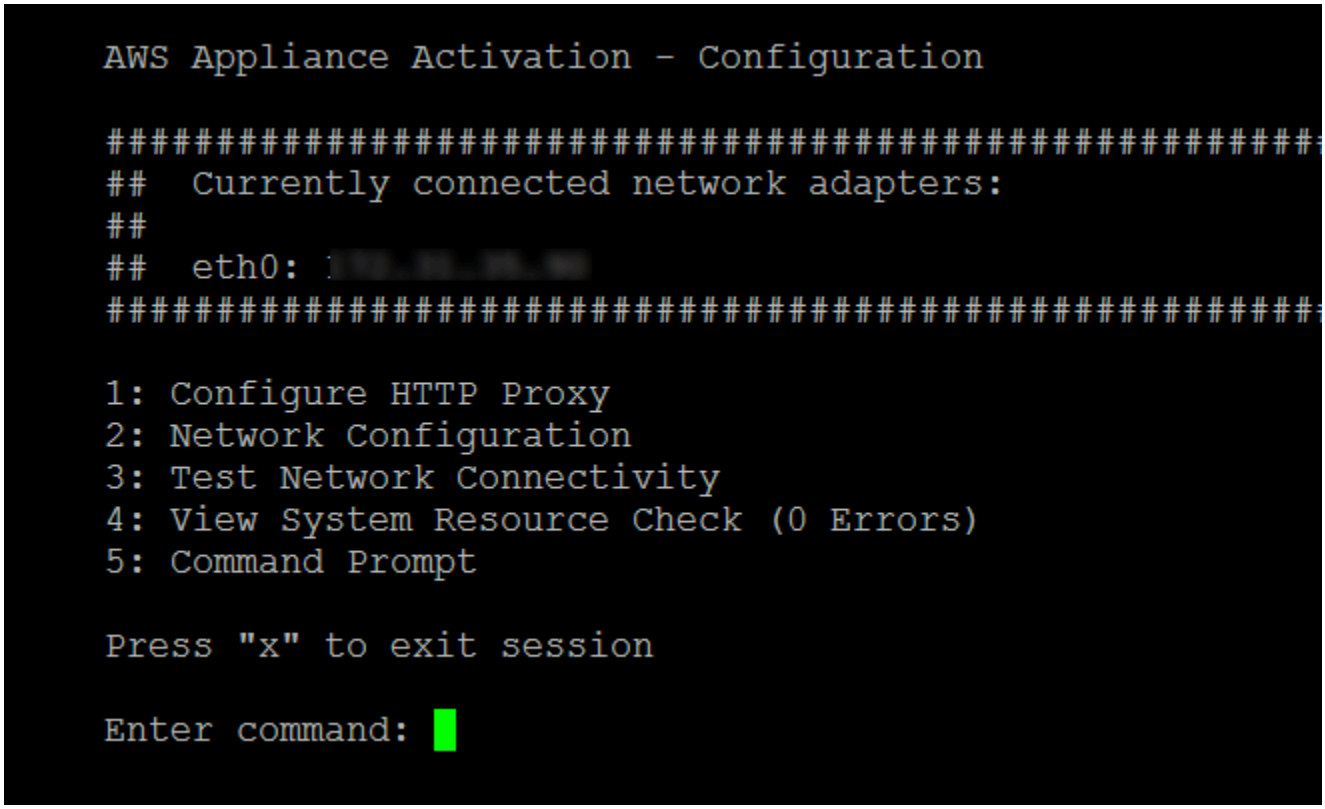
Routing Ihres auf EC2 bereitgestellten Gateway über einen HTTP-Proxy

Storage Gateway unterstützt die Konfiguration einer Socket Secure-Proxy Version 5 (SOCKS5) zwischen dem auf Amazon EC2 bereitgestellten Gateway undAWSaus.

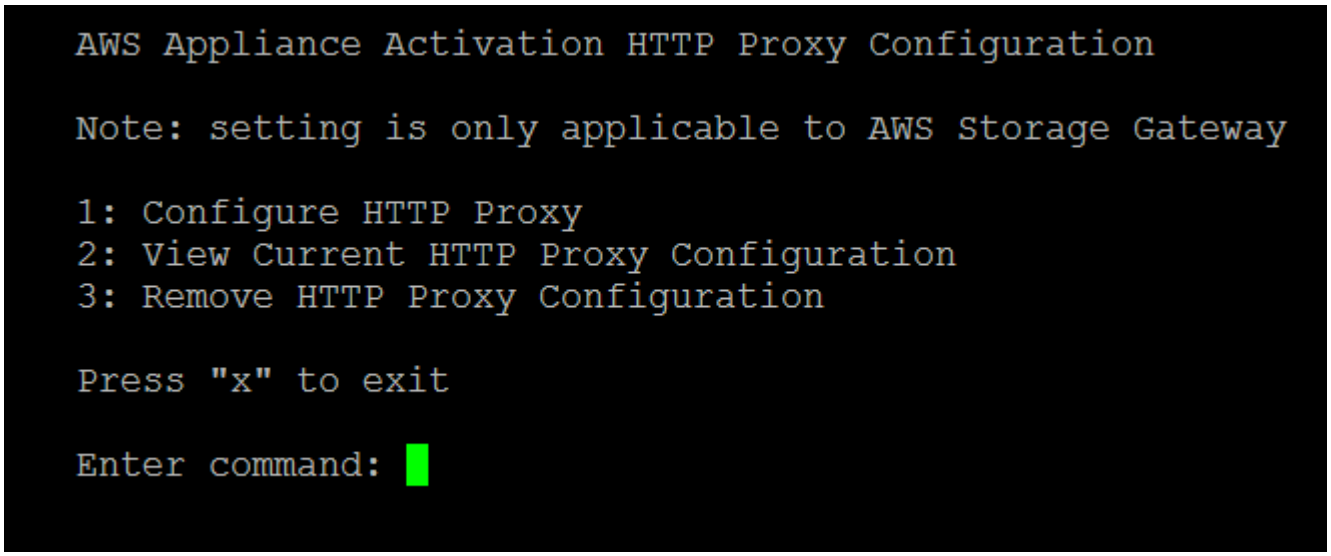
Wenn das Gateway einen Proxy-Server für die Kommunikation mit dem Internet verwenden muss, müssen Sie die HTTP-Proxy-Einstellungen für das Gateway konfigurieren. Dazu geben Sie eine IP-Adresse und die Portnummer für den Host an, auf dem der Proxy ausgeführt wird. Danach leitet Storage Gateway alleAWSEndpunkt-Datenverkehr über Ihren Proxy-Server. Die Kommunikation zwischen dem Gateway und den Endpunkten ist verschlüsselt, selbst wenn der HTTP-Proxy verwendet wird.

So leiten Sie Ihren Gateway-Internet-Datenverkehr über einen lokalen Proxy-Server weiter

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Konsole des Amazon EC2 EC2-Gateways an.
2. Auf derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie**1**um mit der Konfiguration des HTTP-Proxys zu beginnen.



3. Wählen Sie eine der folgenden Optionen imAWSAppliance-Aktivierung - KonfigurationHTTP-ProxykonfigurationMenü im



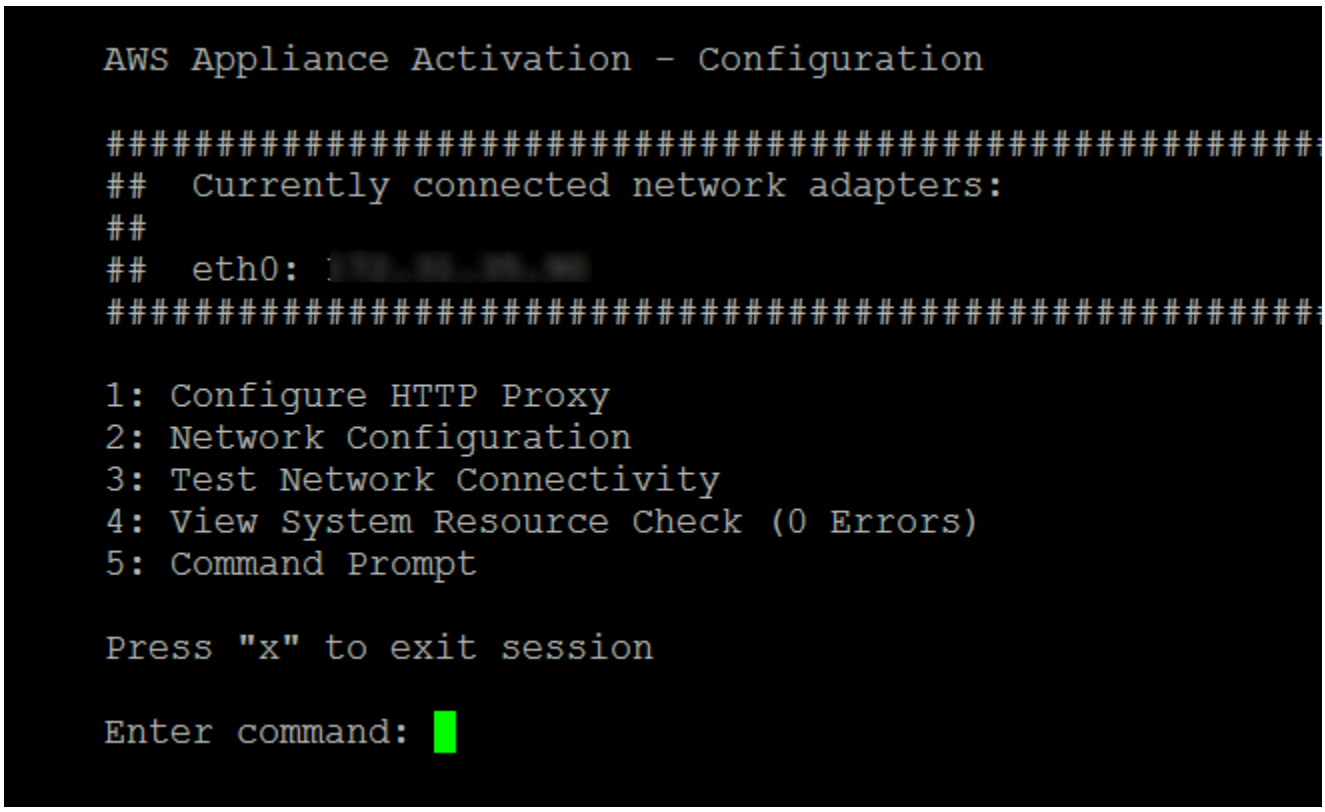
Bis	Vorgehensweise
Konfigurieren eines HTTP-Proxys	Geben Sie ei **1**. Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
Anzeigen der aktuellen HTTP-Proxy-Konfiguration	Geben Sie ei **2**. Wenn kein HTTP-Proxy konfiguriert ist, wird die Meldung `HTTP Proxy not configured` angezeigt. Ist ein HTTP-Proxy konfiguriert, werden der Hostname und Port des Proxys angezeigt.
Entfernen einer HTTP-Proxy-Konfiguration	Geben Sie ei **3**. Die Meldung `HTTP Proxy Configuration Removed` wird angezeigt.

Konfigurieren Ihrer Gateway-Netzwerkeinstellungen

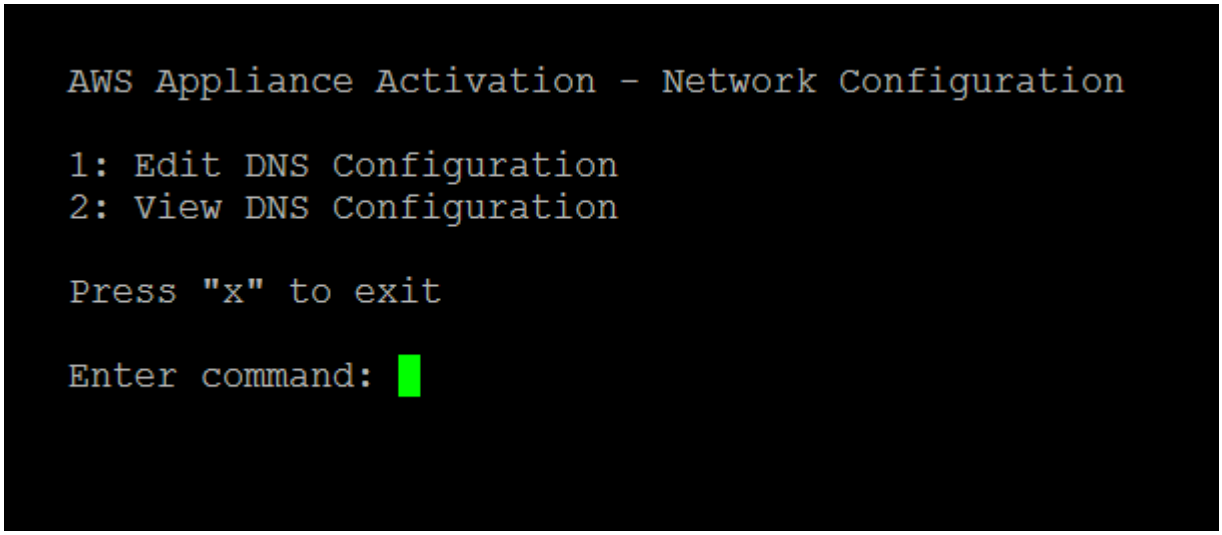
Sie können die Einstellungen für "Domain Name Server (DNS)" über die lokale Konsole anzeigen und konfigurieren.

So konfigurieren Sie Ihr Gateway zur Verwendung einer statischen IP-Adresse

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Konsole des Amazon EC2 EC2-Gateways an.
2. Auf derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie**2**um mit der Konfiguration Ihres DNS-Servers zu beginnen.



3. Wählen Sie eine der folgenden Optionen im Menü Network Configuration (Netzwerkkonfiguration) aus.



Bis	Vorgehensweise
Bearbeiten der DNS-Konfiguration Ihres Gateways	Geben Sie ei **1**. Die verfügbaren Adapter des primären und sekundären DNS-Servers werden angezeigt. Sie werden aufgefordert, die neue IP-Adresse einzugeben.
Anzeigen der DNS-Konfiguration Ihres Gateways	Geben Sie ei **2**. Die verfügbaren Adapter des primären und sekundären DNS-Servers werden angezeigt.

Testen der Netzwerkkonnektivität Ihres Gateways

Sie können die lokale Konsole des Gateways verwenden, um Ihre Netzwerkkonnektivität zu testen. Dieser Test kann nützlich sein, wenn Sie Netzwerkprobleme mit dem Gateway beheben.

So testen Sie die Gateway-Netzwerkverbindung

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Konsole des Amazon EC2 EC2-Gateways an.

2. Von derAWSAppliance-Aktivierung - KonfigurationHauptmenü, geben Sie die entsprechende Zahl ein, um auszuwählenTesten der Netzwerkkonnektivitätaus.

   Wenn Ihr Gateway bereits aktiviert wurde, beginnt der Konnektivitätstest sofort. Für Gateways, die noch nicht aktiviert wurden, müssen Sie den Endpunkttyp angeben undAWS-Regionwie in den folgenden Schritten beschrieben.
3. Wenn Ihr Gateway noch nicht aktiviert ist, geben Sie die entsprechende Zahl ein, um den Endpunkttyp für Ihr Gateway auszuwählen.
4. Wenn Sie den Typ des öffentlichen Endpunkts ausgewählt haben, geben Sie die entsprechende Zahl ein, um dieAWS-RegionDas willst du testen. Für unterstützteAWS-Regionenund eine ListeAWSService-Endpoints, die Sie mit Storage Gateway verwenden können, sieheAWS Storage Gateway-Endpunkte und -KontingenteimAWS– Allgemeine Referenzaus.

Während der Test fortschreitet, wird jeder Endpunkt entweder angezeigt[BESTANDEN]oder[FEHLGESCHLAGEN]und gibt den Status der Verbindung wie folgt an:

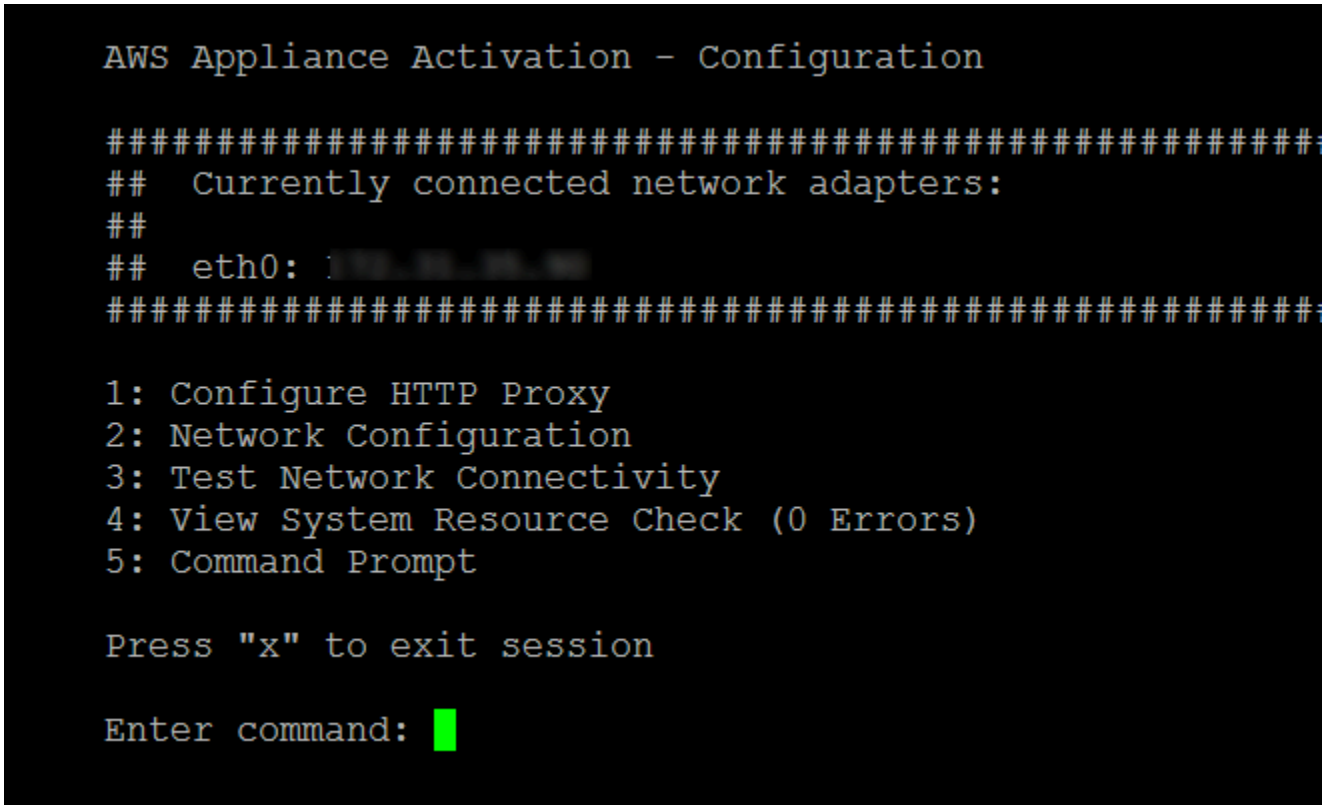
Fehlermeldung	Description
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über eine Netzwerkv erbindung.
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway verfügt über keine Netzwerkk onnektivität.

Anzeigen des Ressourcenstatus Ihres Gateway-Syst

Beim Starten überprüft Ihr Gateway seine virtuellen CPU-Kerne, Stamm-Volume-Größe und RAM. Er kann dann bestimmen, ob ausreichend Systemressourcen für die ordnungsgemäße Funktionsweise Ihres Gateways verfügbar sind. Sie können die Ergebnisse dieser Prüfung auf der lokalen Gateway-Konsole anzeigen.

So zeigen Sie den Status einer Systemressourcenprüfung an

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Konsole des Amazon EC2 EC2-Gateways an.
2. In derStorage Gateway KonfigurationHauptmenü, geben Sie**4**So zeigen Sie die Ergebnisse einer Systemressourcenprüfung an.



Die Konsole zeigt für jede Ressource [OK], [WARNING] ([WARNUNG]) oder [FAIL] ([FEHLGESCHLAGEN]) an (siehe folgende Tabelle).

Fehlermeldung	Description
[OK]	Die Ressource hat die Systemressourcenprüfung bestanden.
[WARNING] ([WARNUNG])	Die Ressource erfüllt nicht die empfohlenen Anforderungen, aber das Gateway ist weiterhin funktionsfähig. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.

Fehlermeldung	Description
[FAIL] ([FEHLGESCHLAGEN])	Die Ressource erfüllt nicht die Mindestan forderungen. Das Gateways funktioniert möglicherweise nicht ordnungsgemäß. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressource nprüfung an.

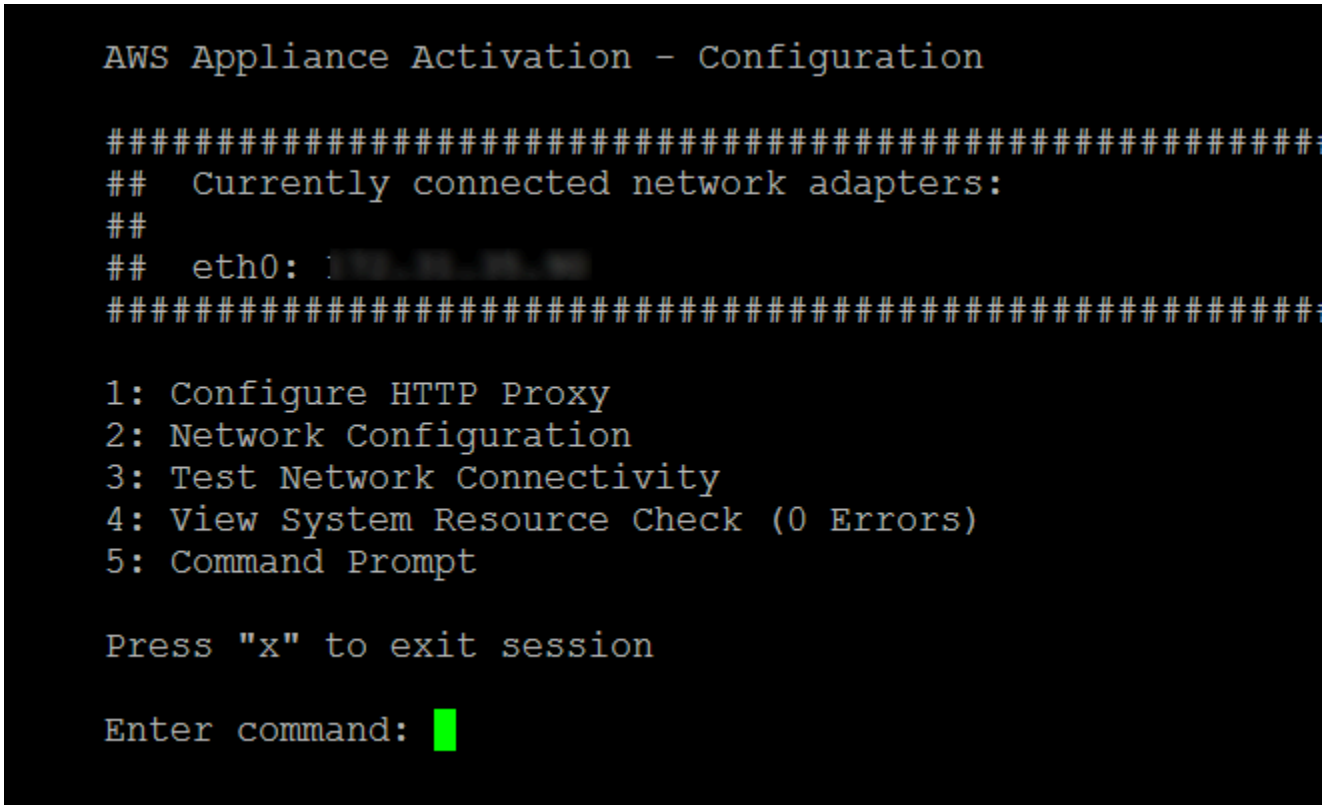
Die Konsole zeigt die Anzahl der Fehler und Warnungen neben der Menüoption für die Ressourcenprüfung an.

Ausführen von Storage Gateway Gateway-Befehlen auf der

Die AWS Storage Gateway-Konsole stellt eine sichere Umgebung für die Konfiguration und Diagnose von Problemen mit dem Gateway dar. Mithilfe der Konsolenbefehle können Sie Wartungsaufgaben wie das Speichern von Routing-Tabellen oder das Herstellen einer Verbindung mit dem Amazon Web Services Support durchführen.

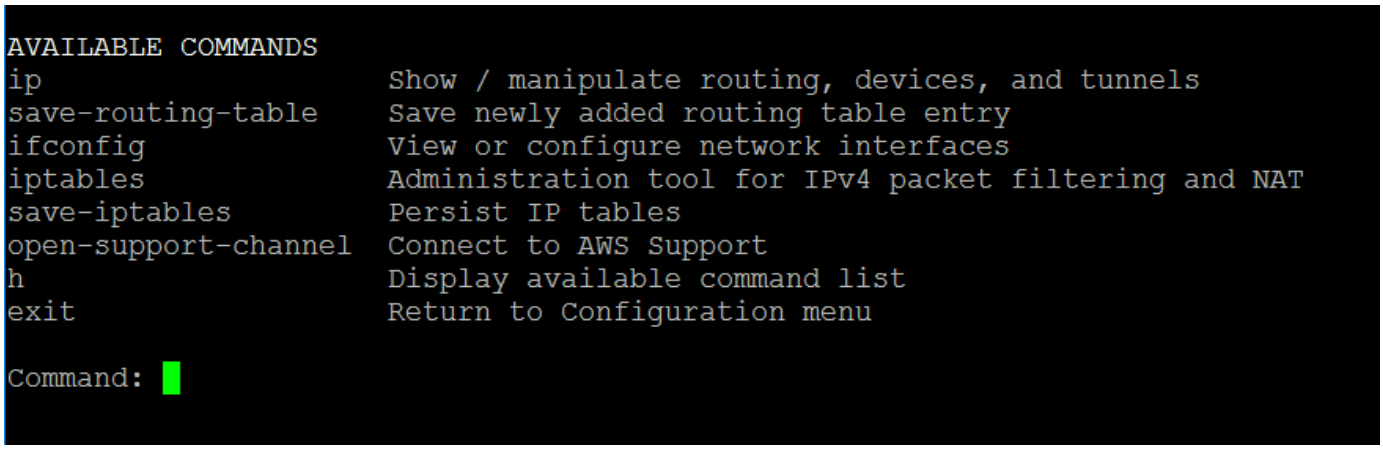
So führen Sie eine Konfiguration oder einen Diagnosebefehl aus

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Konsole des Amazon EC2 EC2-Gateways an.
2. In derAWSAppliance-AktivierungHauptmenü, geben Sie**5**zumGateways Konsoleaus.



3. Geben Sie an der Eingabeaufforderung **h** ein und drücken Sie anschließend die Eingabetaste.

   Die Konsole zeigt das Menü AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) mit den verfügbaren Befehlen an. Nach dem Menü wird die Eingabeaufforderung der Gateway-Konsole angezeigt (siehe Abbildung).



4. Geben Sie in der Befehlszeile den Befehl ein, den Sie verwenden möchten, und befolgen Sie die Anweisungen.

Wenn Sie weitere Informationen erhalten möchten, geben Sie in der Befehlszeile den Namen des Befehls ein.

Zugreifen auf die lokale Konsole des Gateways

Auf welche Weise Sie auf die lokale Konsole der VM zugreifen, ist davon abhängig, auf welcher Art von Hypervisor Sie Ihre Gateway-VM bereitgestellt haben. In diesem Abschnitt finden Sie Informationen zum Zugriff auf die lokale VM-Konsole mit Linux Kernel-basierter virtueller Maschine (KVM), VMware ESXi und Microsoft Hyper-V Manager.

Themen

Zugreifen auf die lokale Konsole des Gateways mit Linux KVM

Je nach verwendeter Linux-Verteilung gibt es verschiedene Möglichkeiten, virtuelle Maschinen auf KVM zu konfigurieren. Anweisungen für den Zugriff auf die KVM-Konfigurationsoptionen über die Befehlszeile folgen. Die Anweisungen können je nach KVM-Implementierung unterschiedlich sein.

So greifen Sie mithilfe von KVM auf die lokale Konsole des Gateways zu

1. Verwenden Sie den folgenden Befehl, um die VMs aufzulisten, die derzeit in KVM verfügbar sind.

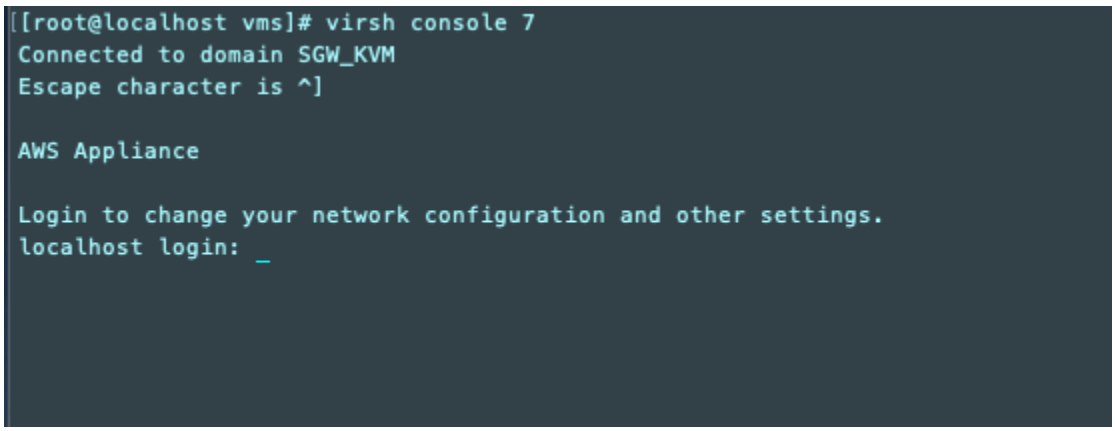
   ```
   # virsh list
   ```

   Sie können verfügbare VMs nach `Id` auswählen.

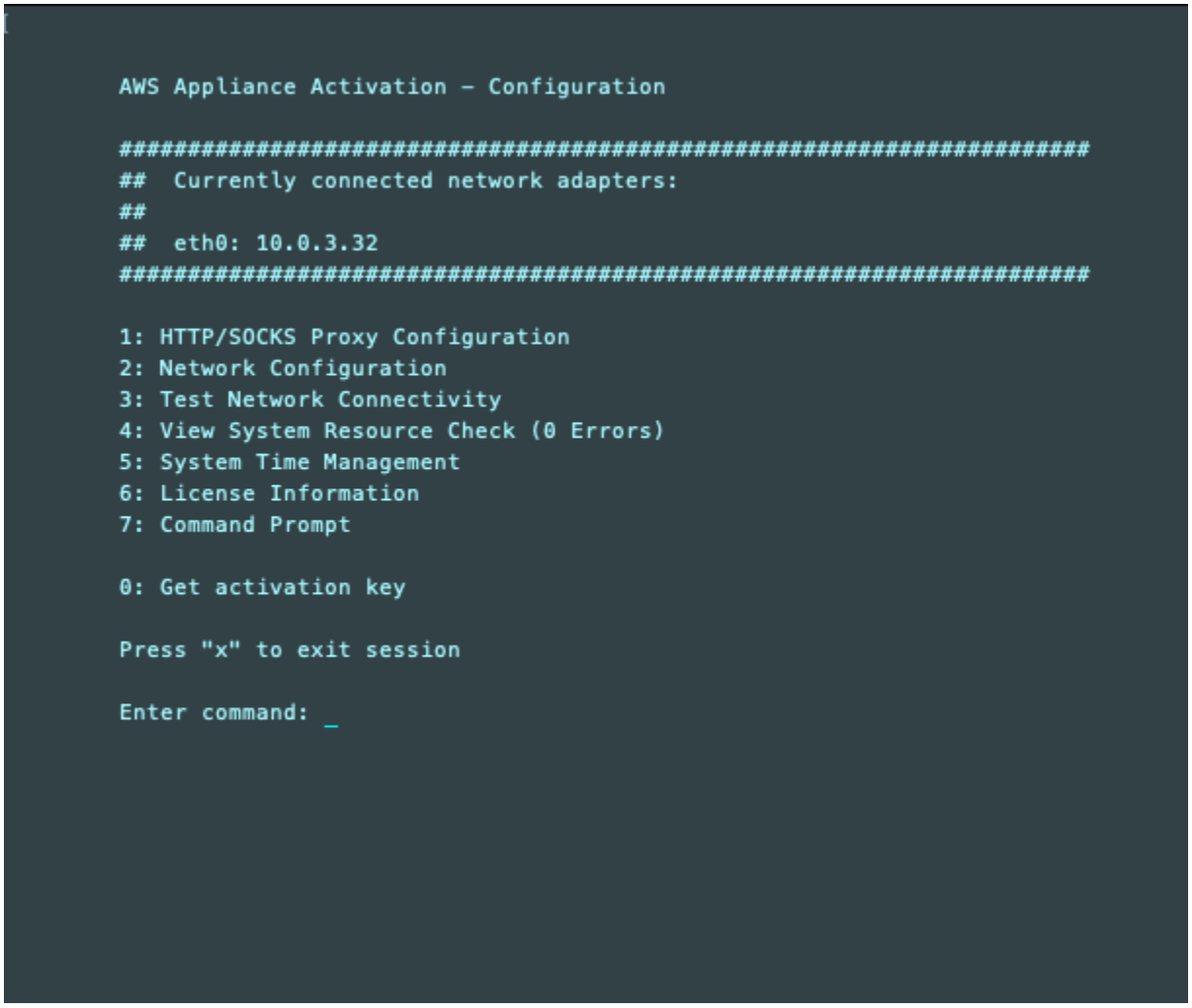
   

2. Verwenden Sie den folgenden Befehl, um auf die lokale Konsole zuzugreifen.

```
# virsh console VM_Id
```



3. Standardanmeldeinformationen für die Anmeldung bei der lokalen Konsole finden Sie unter Anmelden an der lokalen Konsole des File Gateways.
4. Nachdem Sie sich angemeldet haben, können Sie Ihr Gateway aktivieren und konfigurieren.

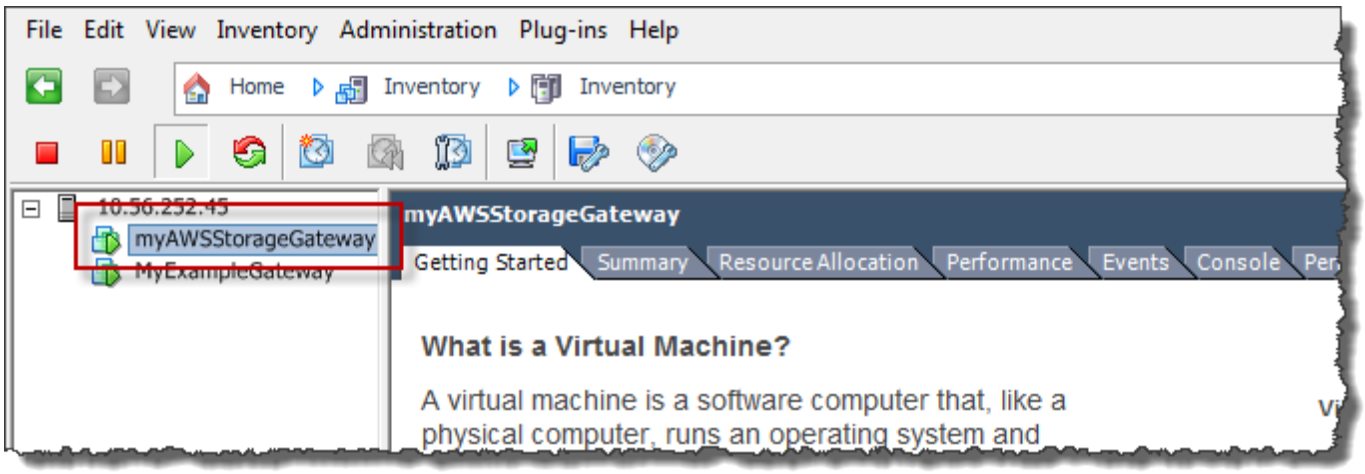


Zugreifen auf die lokale Konsole mit VMware ESXi

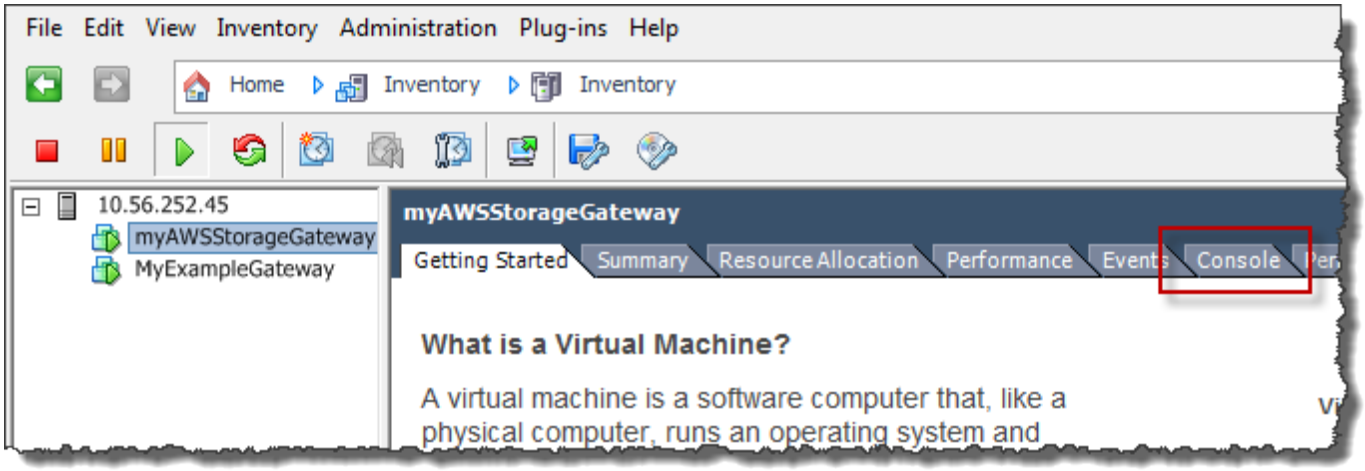
So greifen Sie mithilfe von VMware ESXi auf die lokale Konsole des Gateways zu

1. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM.
2. Stellen Sie sicher, dass das Gateway aktiviert ist.

> **Note**
>
> Wenn Ihre Gateway-VM aktiviert ist, erscheint wie im folgenden Screenshot dargestellt ein grünes Pfeilsymbol mit dem VM-Symbol. Wenn Ihre Gateway-VM nicht aktiviert ist, wählen Sie das Symbol Power On (Energie ein) im Menü Toolbar (Symbolleiste), um sie zu aktivieren.



3. Wählen Sie die Registerkarte Console (Konsole).



Nach einem kurzen Augenblick können Sie sich an die VM anmelden.

> **Note**
>
> Drücken Sie Ctrl+Alt (Strg+Alt), um den Mauszeiger aus dem Konsolenfenster freizugeben.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

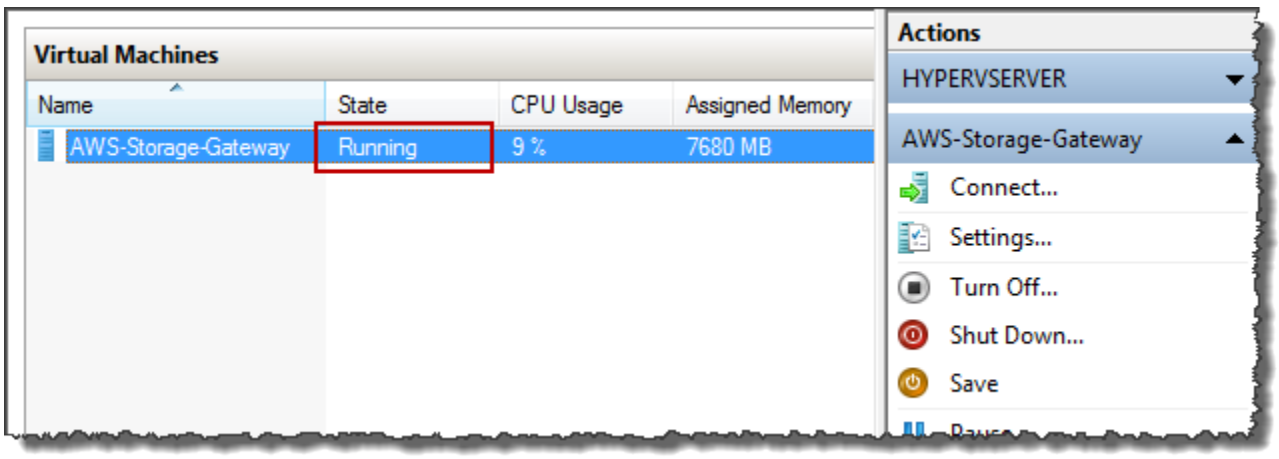
4. Um sich mit den Standard-Anmeldeinformationen anzumelden, fahren Sie mit dem Verfahren Anmelden an der lokalen Konsole des File Gateways fort.

Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V

Zugreifen auf die lokale Gateway-Konsole (Microsoft Hyper-V)

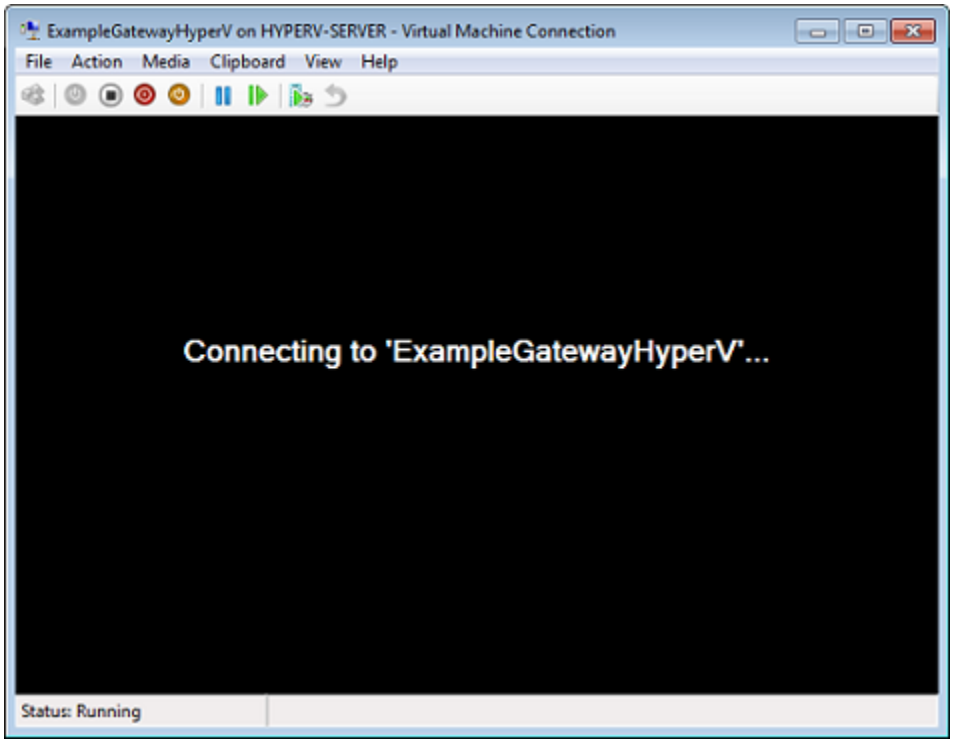
1. Wählen Sie in der Liste Virtual Machines (Virtuelle Maschinen) im Microsoft Hyper-V Manager Ihre Gateway-VM aus.
2. Stellen Sie sicher, dass das Gateway aktiviert ist.

> **Note**
>
> Wenn Ihre Gateway-VM aktiviert ist, wird `Running` als State (Status) der VM angezeigt, wie im folgenden Screenshot dargestellt. Wenn Ihre Gateway-VM nicht aktiviert ist, wählen Sie Start im Fenster Actions (Aktionen), um sie zu aktivieren.

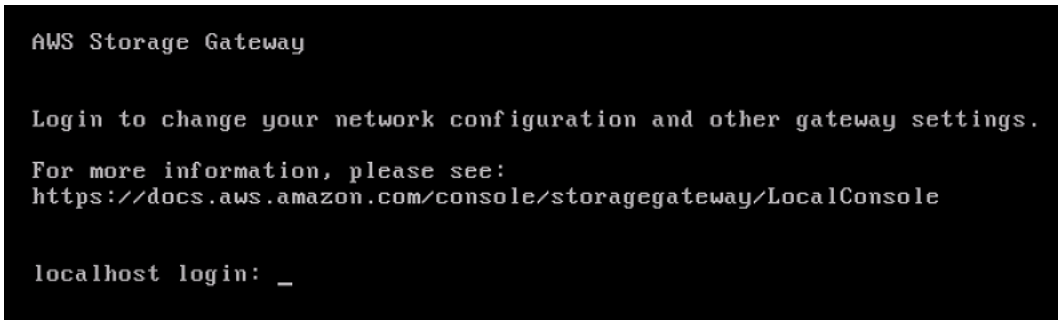


3. Wählen Sie im Fenster Actions (Aktionen) die Option Connect (Verbinden).

   Das Fenster Virtual Machine Connection (Verbindung der virtuellen Maschine) wird angezeigt. Wenn ein Authentifizierungsfenster angezeigt wird, geben Sie den Benutzernamen und das Passwort ein, die Sie vom Hypervisor-Administrator erhalten haben.



   Nach einem kurzen Augenblick können Sie sich an die VM anmelden.



4. Um sich mit den Standard-Anmeldeinformationen anzumelden, fahren Sie mit dem Verfahren Anmelden an der lokalen Konsole des File Gateways fort.

Konfigurieren von Networkadaptern für Ihr Gateway

In diesem Abschnitt finden Sie Informationen zum Konfigurieren von mehreren Netzwerkadaptern für Ihr Gateway.

Themen

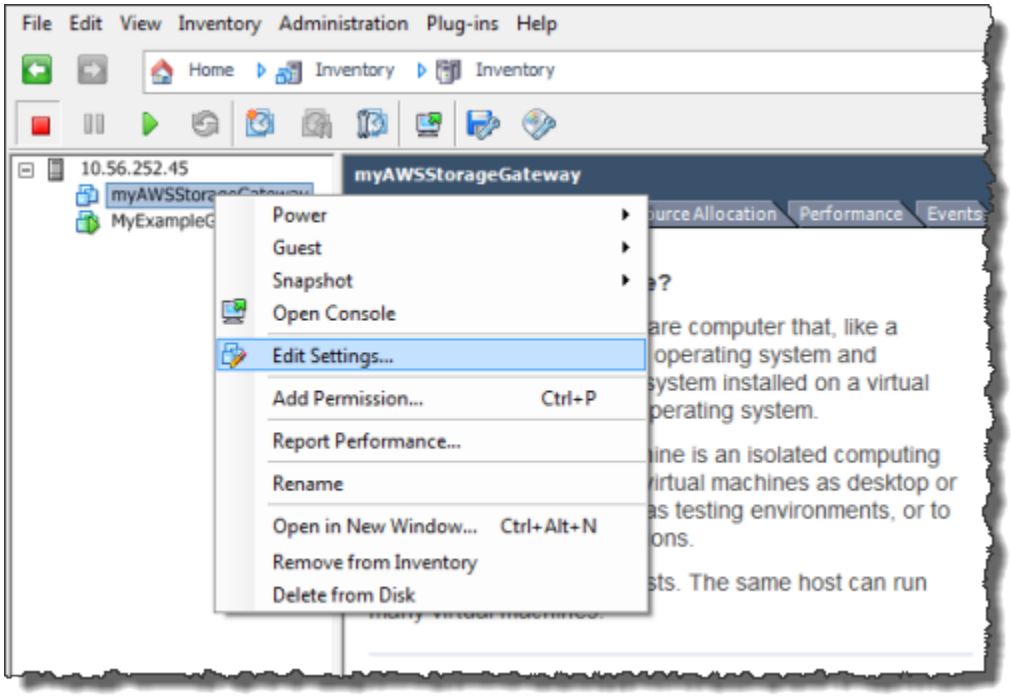
Konfigurieren des Gateways für mehrere NICs in einem VMware-ESXi-Host

Im folgenden Verfahren wird davon ausgegangen, dass für Ihre Gateway-VM bereits ein Netzwerkadapter definiert wurde und Sie einen zweiten Adapter hinzufügen. Im folgenden Verfahren wird gezeigt, wie Sie einen Adapter für VMware ESXi hinzufügen.

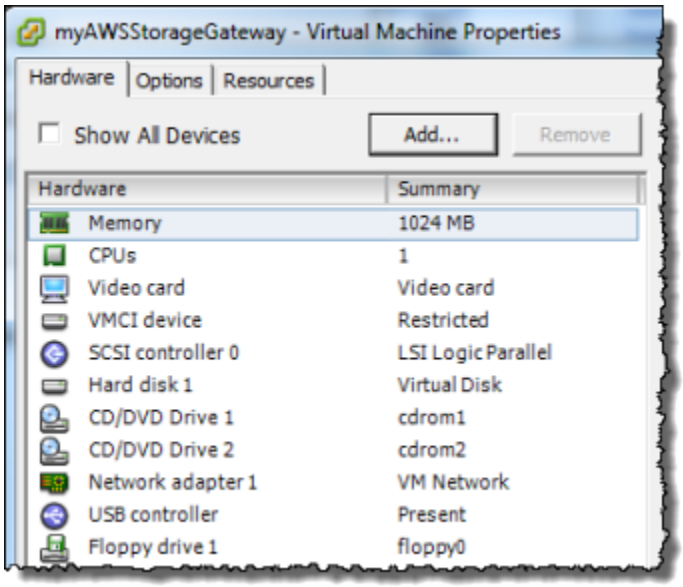
So konfigurieren Sie das Gateway für einen zusätzlichen Netzwerkadapter im VMware-ESXi-Host

1. Fahren Sie das Gateway herunter.
2. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM.

   Die VM kann für die Dauer dieses Verfahrens aktiviert bleiben.
3. Öffnen Sie im Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM, und wählen Sie Edit Settings (Einstellungen bearbeiten).

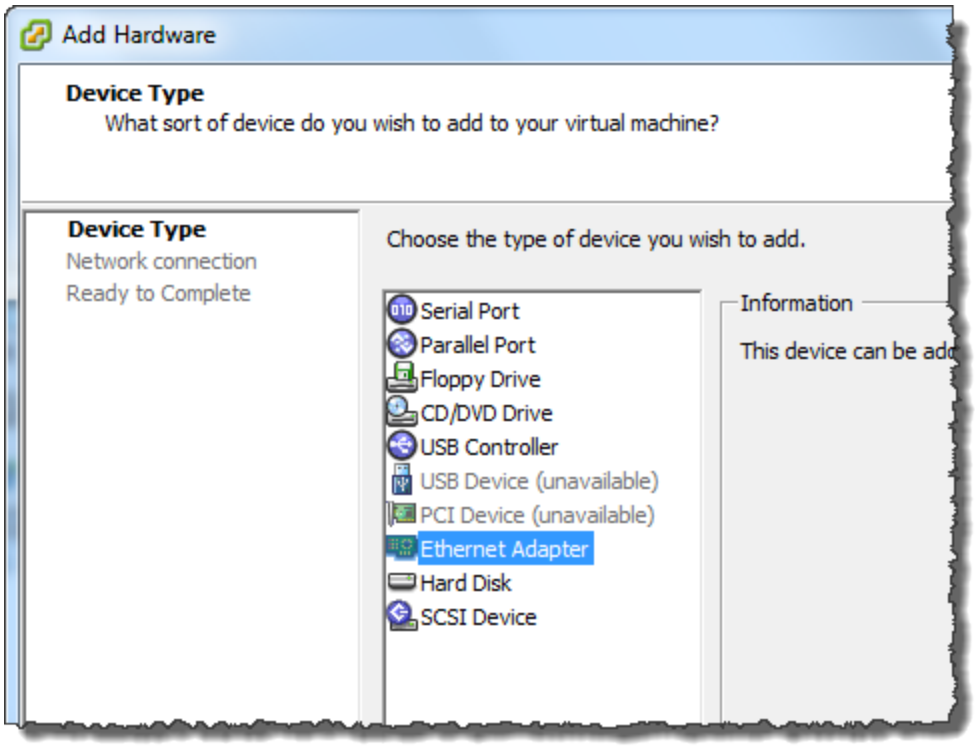


4. Wählen Sie auf der Registerkarte Hardware im Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) die Option Add (Hinzufügen), um ein Gerät hinzuzufügen.



5. Befolgen Sie die Anweisungen des Hardware-Assistenten zum Hinzufügen eines Netzwerkadapters.

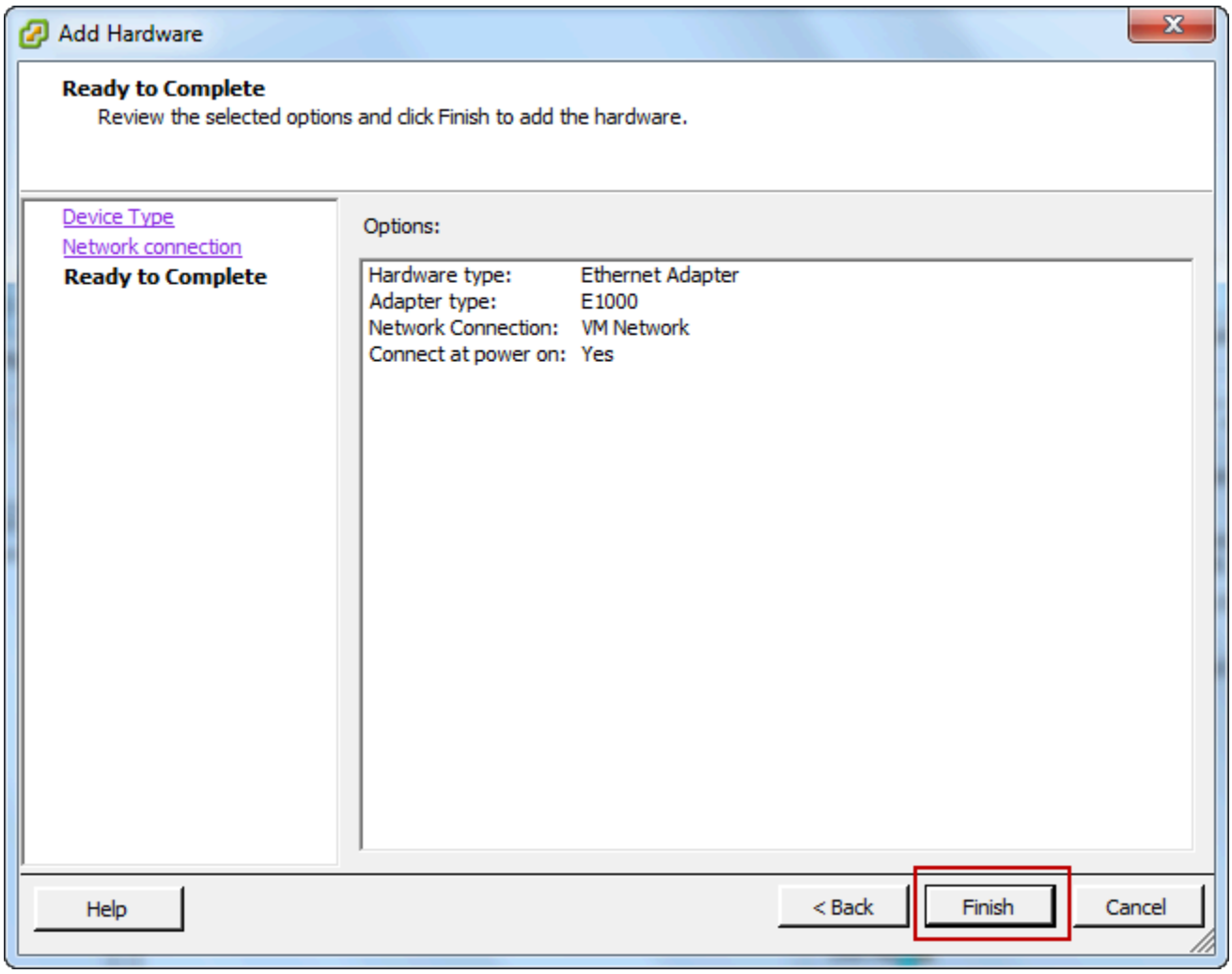
a. Wählen Sie im Fenster Device Type (Gerätetyp) die Option Ethernet Adapter, um einen Adapter hinzuzufügen, und wählen Sie dann Next (Weiter).



b. Stellen Sie sicher, dass im Fenster Network Type (Netzwerktyp) die Option Connect at power on (Verbindung bei Einschalten der Energie herstellen) für Type (Typ) ausgewählt ist, und wählen Sie dann Next (Weiter).

   Wir empfehlen, dass Sie den mit E1000-Netzwerkadapter mit Storage Gateway verwenden. Weitere Informationen zu den Adaptertypen, die ggf. in der Adapter-Liste aufgeführt werden, finden Sie unter den Netzwerkadapter-Typen in der ESXi und vCenter Server-Dokumentation.

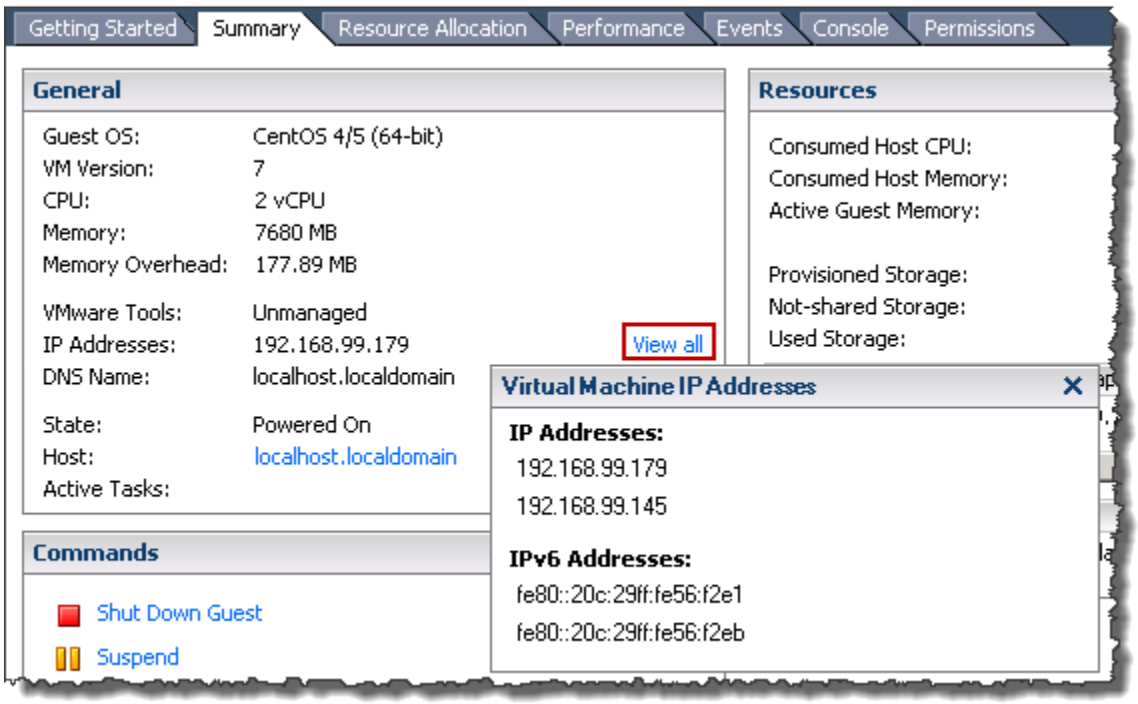
c. Prüfen Sie im Fenster Ready to Complete (Bereit zum Abschließen) die Informationen und wählen Sie Finish (Fertigstellen).



6. Wählen Sie die Registerkarte Summary (Übersicht) der VM und anschließend View All (Alle anzeigen) neben dem Kontrollkästchen IP Address (IP-Adresse). Das Fenster Virtual Machine IP Addresses (IP-Adresse der virtuellen Maschine) zeigt alle IP-Adressen an, die Sie für den Zugriff auf das Gateway verwenden können. Vergewissern Sie sich, dass für das Gateway eine zweite IP-Adresse gelistet ist.

> **Note**
>
> Es kann einige Minuten dauern, bis die Adapteränderungen wirksam und die zusammenfassenden VM-Informationen aktualisiert werden.

Die folgende Abbildung dient lediglich der Veranschaulichung. In der Praxis ist eine IP-Adresse die Adresse, über die das Gateway mit AWS kommuniziert, und die andere Adresse ist eine Adresse in einem anderen Subnetz.



7. Schalten Sie an der Storage Gateway Gateway-Konsole das Gateway ein.
8. In derNavigationBereich der Storage Gateway Gateway-Konsole wählen-GatewaysUnd wählen Sie das Gateway, dem Sie den Adapter hinzugefügt haben. Vergewissern Sie sich, dass die zweite IP-Adresse in der Registerkarte Details aufgeführt wird.

Weitere Informationen zu Aufgaben für die lokale Konsole, die für VMware-, Hyper-V- und KVM-Hosts typisch sind, finden Sie unter Ausführen von Aufgaben in der lokalen VM-Konsole (File Gateway).

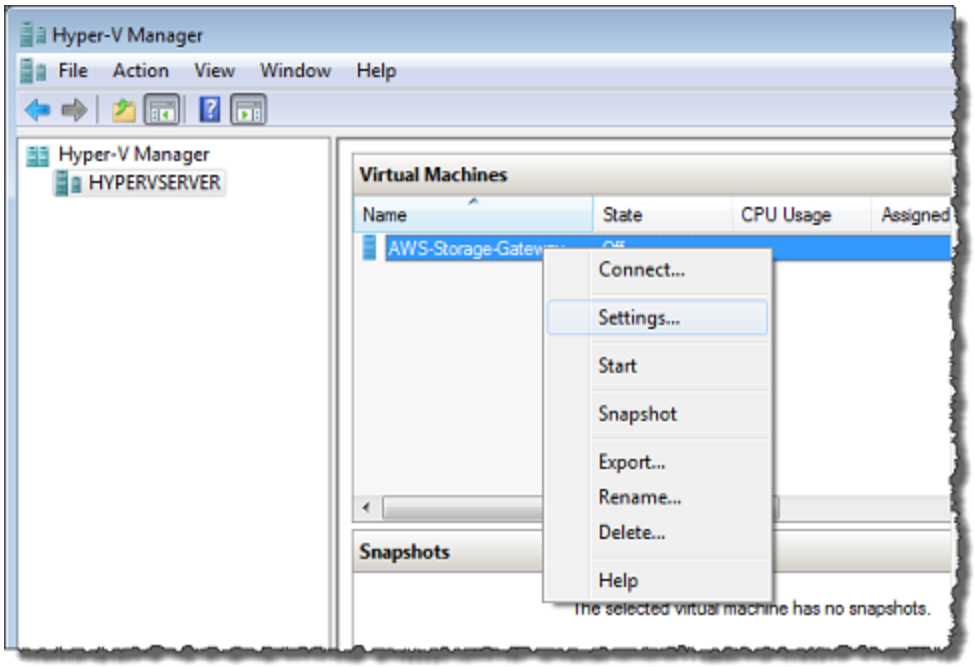
Konfigurieren des Gateways für mehrere NICs in einem Microsoft-Hyper-V-Host

Im folgenden Verfahren wird davon ausgegangen, dass für Ihre Gateway-VM bereits ein Netzwerkadapter definiert wurde und Sie einen zweiten Adapter hinzufügen. In diesem Verfahren wird zeigt, wie Sie einen Adapter für einen Microsoft Hyper-V-Host hinzufügen.

So konfigurieren Sie Ihr Gateway für einen zusätzlichen Netzwerkadapter in einem Microsoft Hyper-V-Host

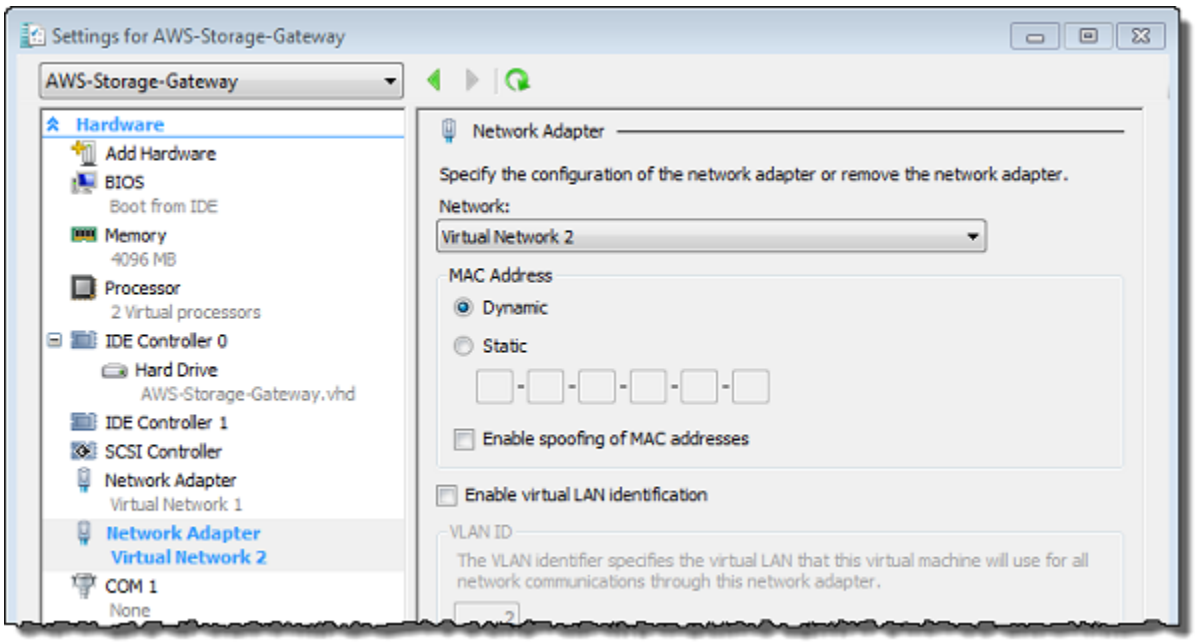
1. Schalten Sie an der Storage Gateway Gateway-Konsole das Gateway aus.
2. Wählen Sie im Microsoft Hyper-V ManagerIhre Gateway-VM.
3. Wenn die VM nicht bereits deaktiviert ist, öffnen Sie das Kontextmenü (rechte Maustaste) für Ihr Gateway und wählen Sie Turn Off (Deaktivieren).

4. Öffnen Sie im Client das Kontextmenü für Ihre Gateway-VM und wählen Sie Settings (Einstellungen).



5. Wählen Sie im Dialogfeld Settings (Einstellungen) der VM für Hardware die Option Add Hardware (Hardware hinzufügen).
6. Wählen Sie im Fenster Add Hardware (Hardware hinzufügen) die Option Network Adapter (Netzwerkadapter) und anschließend Add (Hinzufügen), um ein Gerät hinzuzufügen.
7. Konfigurieren Sie den Netzwerkadapter, und wählen Sie dann Apply (Anwenden), um die Einstellungen anzuwenden.

   Im folgenden Beispiel wird Virtual Network 2 (Virtuelles Netzwerk 2) für den neuen Adapter gewählt.



8. Vergewissern Sie sich, dass im Dialogfeld Settings (Einstellungen) für Hardware der zweite Adapter hinzugefügt wurde, und wählen Sie dann OK.
9. Schalten Sie an der Storage Gateway Gateway-Konsole das Gateway ein.
10. Wählen Sie im Fenster Navigation die Option Gateways und anschließend das Gateway, dem Sie den Adapter hinzugefügt haben. Vergewissern Sie sich, dass die zweite IP-Adresse in der Registerkarte Details aufgeführt wird.

Weitere Informationen zu Aufgaben für die lokale Konsole, die für VMware-, Hyper-V- und KVM-Hosts typisch sind, finden Sie unter Ausführen von Aufgaben in der lokalen VM-Konsole (File Gateway).

Löschen des Gateways über die AWS Storage Gateway-Konsole und Bereinigen zugehöriger Ressourcen

Wenn Sie ein Gateway nicht weiter verwenden möchten, können Sie dieses zusammen mit den zugehörigen Ressourcen löschen. Durch das Entfernen von Ressourcen wird verhindert, dass Gebühren für Ressourcen entstehen, die Sie voraussichtlich nicht weiter verwenden werden, und Ihre monatliche Rechnung wird gesenkt.

Wenn Sie ein Gateway löschen, wird es nicht mehr in der AWS Storage Gateway-Managementkonsole angezeigt und die iSCSI-Verbindung zum Initiator wird geschlossen. Die Schritte zum Löschen eines Gateways sind für alle Gateway-Typen gleich. Abhängig von dem Typ

des Gateways, das Sie löschen möchten, und dem Host, auf dem es bereitgestellt ist, führen Sie jedoch spezifische Anweisungen zum Entfernen zugehöriger Ressourcen aus.

Sie können ein Gateway mithilfe der Storage Gateway Gateway-Konsole oder programmgesteuert löschen. Im Folgenden finden Sie Informationen zum Löschen eines Gateways mit der Storage Gateway Gateway-Konsole. Informationen zum programmgesteuerten Löschen eines Gateways finden Sie unterAWS Storage Gateway-API-Referenzaus.

Themen

Löschen eines Gateways mithilfe der Storage Gateway Gateway-Konsole

Die Schritte zum Löschen eines Gateways sind für alle Gateway-Typen gleich. Abhängig von dem Typ des Gateways, das Sie löschen möchten, und dem Host, auf dem es bereitgestellt ist, müssen Sie jedoch möglicherweise zusätzliche Aufgaben zum Entfernen von dem Gateway zugeordneten Ressourcen ausführen. Durch das Entfernen dieser Ressourcen wird verhindert, dass Sie für Ressourcen zahlen, die Sie voraussichtlich nicht mehr verwenden werden.

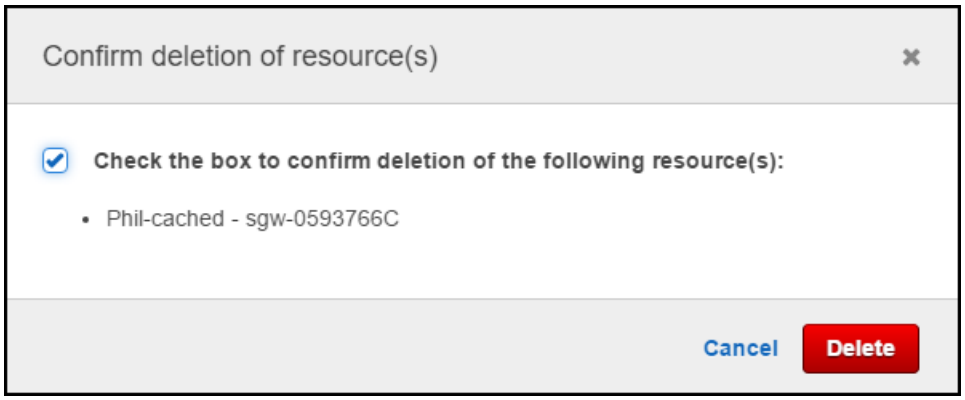
> **Note**
>
> Bei Gateways, die auf einer Amazon EC2 EC2-Instance bereitgestellt werden, existiert die Instance weiterhin, bis Sie sie löschen.
> Bei Gateways, die auf einer virtuellen Maschine (VM) bereitgestellt sind, ist die Gateway-VM nach dem Löschen des Gateways weiterhin in der Virtualisierungsumgebung vorhanden. Zum Entfernen der Vm verwenden Sie den VMware vSphere-Client, Microsoft Hyper-V Manager oder Linux Kernel-basierte virtuelle Maschine (KVM)-Client, um eine Verbindung mit dem Host herzustellen und die VM zu entfernen. Beachten Sie, dass Sie die gelöschte Gateway-VM nicht erneut verwenden können, um ein neues Gateway zu aktivieren.

So löschen Sie ein Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie im Navigationsbereich erst Gateways und anschließend das Gateway, das Sie löschen möchten.
3. Wählen Sie für Actions (Aktionen) die Option Delete gateway (Gateway löschen) aus.
4. **Warning**

   Bevor Sie diesen Schritt ausführen, stellen Sie sicher, dass derzeit keine Anwendungen in die Gateway-Volumes schreiben. Wenn Sie das Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten.
   Wenn ein Gateway gelöscht wird, gibt es keine Möglichkeit, es wiederherzustellen.

   Aktivieren Sie im Bestätigungsdialogfeld, das angezeigt wird, das Kontrollkästchen zum Bestätigen des Löschvorgangs. Stellen Sie sicher, dass die aufgelistete Gateway-ID das Gateway angibt, das Sie löschen möchten, und wählen Sie dann Delete (Löschen).



Important

Sie bezahlen nach dem Löschen eines Gateways keine Gebühren mehr für die Software, jedoch bleiben Ressourcen wie virtuelle Bänder, Amazon Elastic Block Store (Amazon EBS) -Snapshots und Amazon EC2 EC2-Instances bestehen. Diese Ressourcen werden Ihnen weiterhin berechnet. Sie können Amazon EC2-Instances und Amazon EBS-Snapshots entfernen, indem Sie Ihr Amazon EC2 EC2-Abonnement stornieren. Wenn Sie Ihr Amazon

EC2 EC2-Abonnement behalten möchten, können Sie Ihre Amazon EBS-Snapshots mithilfe der Amazon EC2 EC2-Konsole löschen.

Entfernen von Ressourcen von einem lokal bereitgestellten Gateway

Anhand der folgenden Anweisungen können Sie Ressourcen von einem Gateway entfernen, das lokal bereitgestellt ist.

Entfernen von Ressourcen von einem auf einer VM bereitgestellten Volume Gateway

Wenn das Gateway, das Sie löschen möchten, auf einer virtuellen Maschine (VM) bereitgestellt ist, sollten Sie die folgenden Aktionen ausführen, um die Ressourcen zu bereinigen:

- Löschen Sie das Gateway.

Entfernen von Ressourcen von einem auf einer Amazon EC2 EC2-Instance bereitgestellten Gateway

Wenn Sie ein Gateway löschen möchten, das Sie auf einer Amazon EC2 EC2-Instance bereitgestellt haben, empfehlen wir, dass Sie dieAWSAuf diese Weise können Sie Ressourcen, die mit dem Gateway verwendet wurden, können Sie ungeplante nutzungsbedingte Gebühren vermeiden.

Entfernen von Ressourcen aus auf Amazon EC2 bereitgestellten Cached-Volumes

Wenn Sie ein Gateway mit Cached-Volumes auf EC2 bereitgestellt haben, schlagen wir vor, dass Sie die folgenden Schritte ausführen, um das Gateway zu löschen und seine Ressourcen zu bereinigen:

1. Löschen Sie in der Storage Gateway Gateway-Konsole das Gateway wie unterLöschen eines Gateways mithilfe der Storage Gateway Gateway-Konsoleaus.
2. Stoppen Sie in der Amazon EC2 EC2-Konsole die EC2-Instance, wenn Sie die Instance erneut verwenden möchten. Andernfalls beenden Sie die Instance. Wenn Sie das Löschen von Volumes planen, notieren Sie sich die Blockgeräte, die der Instance zugeordnet sind, sowie die Geräte-IDs, bevor Sie die Instance beenden. Diese benötigen Sie zur Identifizierung der Volumes, die Sie löschen möchten.
3. Entfernen Sie in der Amazon EC2 EC2-Konsole alle Amazon EBS -Volumes, die der Instance angefügt sind, wenn Sie sie nicht erneut verwenden möchten. Weitere Informationen finden Sie

unterBereinigen Ihrer Instance und des VolumesimAmazon EC2-Benutzerhandbuch für Linux-Instancesaus.

Ersetzen Sie Ihr vorhandenes File Gateway durch eine neue Instanz

Sie können ein vorhandenes File Gateway durch eine neue Instanz ersetzen, wenn Ihre Daten- und Leistungsanforderungen steigen oder wenn Sie eineAWS-Benachrichtigung zur Migration des Gateways. Möglicherweise müssen Sie dies tun, wenn Sie Ihr Gateway auf eine bessere Host-Plattform oder neuere Amazon EC2 EC2-Instanzen verschieben oder die zugrunde liegende Serverhardware aktualisieren möchten.

Es gibt zwei Methoden, um ein vorhandenes File Gateway zu ersetzen. In der folgenden Tabelle werden die Vor- und Nachteile jeder Methode beschrieben. Wählen Sie anhand dieser Informationen die für Ihre Gateway-Umgebung am besten geeignete Methode aus, und lesen Sie dann die Vorgehensschritte im entsprechenden Abschnitt unten.

	Methode 1: Migrieren Sie den Cache-Datenträger und die Gateway-ID auf	Methode 2: Ersatzinstanz mit leerer Cache-Festplatte und neuer Gateway-ID
Cache-Festplattendaten	Die Daten auf dem Cache-Datenträger bleiben erhalten. Diese Methode ist nützlich, wenn Ihr Gateway über eine große Cache-Festplatte verfügt oder wenn Ihre Anwendungen empfindlich auf die Verzögerung reagieren , die durch Lesevorgä nge außerhalb des Cache verursacht wird.	Daten im Cache werden von derAWS-Wolke. Diese Methode ist optimal für schreiblastige Workloads , wenn Ihre Anwendungen die Verzögerung tolerieren können, die durch Lesevorgä nge außerhalb des Caches verursacht wird.
Ausfallzeit	Ihr Gateway ist während des Migrationsprozesses für 1-2 Stunden offline.	Keine Ausfallzeiten. Das vorhandene Gateway kann gleichzeitig mit dem Ersatz-Gateway verwendet werden, bis Sie es löschen möchten. Mehrere Autoren werden nicht

	Methode 1: Migrieren Sie den Cache-Datenträger und die Gateway-ID auf	Methode 2: Ersatzinstanz mit leerer Cache-Festplatte und neuer Gateway-ID
		unterstützt, während beide Gateways verwendet werden.
Gateway ID	Das neue Gateway erbt die Gateway-ID von dem Gateway, das es ersetzt.	Das bestehende Gateway und das Ersatz-Gateway haben separate, eindeutige Gateway-IDs.

> **Note**
>
> Daten können nur zwischen Gateways desselben Typs verschoben werden.

Methode 1: Migrieren Sie den Cache-Datenträger und die Gateway-ID auf

So migrieren Sie die Cache-Festplatte und die Gateway-ID Ihres File Gateways zu einer Ersatzinstanz

1. Halten Sie alle Anwendungen an, die in das vorhandene Datei-Gateway schreiben.
2. Stellen Sie sicher, dass das`CachePercentDirty`-Metrik auf demÜberwachungfür das vorhandene Datei-Gateway ist`0`aus.
3. Fahren Sie das vorhandene Datei-Gateway herunter, indem Sie die virtuelle Maschine (VM) des Hosts mit ihren Hypervisor-Steuerelementen ausschalten.

   Weitere Informationen zum Herunterfahren einer Amazon EC2 EC2-Instance finden Sie unterAnhalten und Starten Ihrer InstanceimBenutzerhandbuch für Amazon EC2aus.

   Weitere Informationen zum Herunterfahren einer KVM-, VMware- oder Hyper-V-VM finden Sie in der Hypervisor-Dokumentation.
4. Trennen Sie alle Festplatten, einschließlich Root-Datenträger, Cache-Festplatten und laden Sie Pufferdisketten von der alten Gateway-VM hoch.

> **Note**
>
> Notieren Sie sich die Volume-ID des Root-Datenträgers sowie die Gateway-ID, die diesem Root-Datenträger zugeordnet ist. Sie müssen diese Festplatte in einem späteren Schritt vom neuen Storage Gateway-Hypervisor trennen.

Wenn Sie eine Amazon EC2 EC2-Instanz als VM für Ihr Datei-Gateway verwenden, lesen SieTrennen eines Amazon EBS-Volumes von einer Windows-InstanceoderTrennen eines Amazon EBS-Volumes von einer Linux-InstanceimBenutzerhandbuch für Amazon EC2aus.

Informationen zum Trennen von Festplatten von einer KVM-, VMware- oder Hyper-V-VM finden Sie in der Dokumentation für Ihren Hypervisor.

5. Erstellen eines neuenAWSStorage Gateway Hypervisor-VM-Instanz, aber aktivieren Sie sie nicht als Gateway. In einem späteren Schritt wird diese neue VM die Identität des alten Gateways übernehmen.

   Weitere Informationen zum Erstellen einer neuen Storage Gateway Gateway-Hypervisor-VM finden Sie unterAuswählen einer Host-Plattform und Herunterladen der VMaus.

   > **Note**
   >
   > Fügen Sie keine Cache-Festplatten für die neue VM hinzu. Diese VM verwendet dieselben Cache-Festplatten, die von der alten VM verwendet wurden.

6. Konfigurieren Sie Ihre neue Storage Gateway Gateway-VM so, dass sie dieselben Netzwerkeinstellungen wie die alte VM verwendet.

   Die Standard-Netzwerkkonfiguration für das Gateway ist das Dynamic Host Configuration Protocol (DHCP). Mit dem DHCP wird Ihr Gateway automatisch einer IP-Adresse zugewiesen.

   Wenn Sie eine statische IP-Adresse für Ihre Gateway-VM manuell konfigurieren müssen, finden Sie unterKonfigurieren Ihres Gateway-Netzwerksaus.

   Wenn Ihre Gateway-VM einen Socket Secure Version 5 (SOCKS5) Proxy verwenden muss, um eine Verbindung mit dem Internet herzustellen, siheWeiterleiten Ihres lokalen Gateways über einen Proxyaus.

7. Starten Sie die neue Storage Gateway Gateway-VM.

8. Schließen Sie die Festplatten an, die Sie von der alten Gateway-VM getrennt haben, an die neue Gateway-VM an. Trennen Sie die vorhandene Stammdiskette nicht von der neuen Gateway-VM.

   > **Note**
   >
   > Um erfolgreich migrieren zu können, müssen alle Festplatten unverändert bleiben. Das Ändern der Festplattengröße oder anderer Werte führt zu Inkonsistenzen in Metadaten, die eine erfolgreiche Migration verhindern.

9. Initiieren Sie den Gateway-Migrationsprozess, indem Sie eine Verbindung zur neuen VM mit einer URL herstellen, die das folgende Format verwendet:

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

   Sie können dieselbe IP-Adresse für die neue Gateway-VM verwenden, die Sie für die alte Gateway-VM verwendet haben. Ihre URL sollte dem folgenden Beispiel ähneln:

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

   Verwenden Sie diese URL von einem Browser oder über die Befehlszeile mit cURL.

   Wenn die Gateway-Migration erfolgreich initiiert wurde, wird die folgende Meldung angezeigt:

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

10. Warten Sie bis der Gateway-Status als angezeigt wirdAusführen vonimAWSStorage Gateway Gateway-Konsole Je nach verfügbarer Bandbreite kann dies bis zu 10 Minuten dauern.
11. Stoppen Sie die neue Storage Gateway VM.
12. Trennen Sie die Stammdiskette des alten Gateways, dessen Volume-ID Sie zuvor notiert haben, vom neuen Gateway.
13. Starten Sie die neue Storage Gateway Gateway-VM.
14. Wenn Ihr Gateway mit einer Active Directory-Domäne verbunden war, treten Sie der Domäne erneut bei. Detaillierte Anweisungen finden Sie unterKonfigurieren des Microsoft Active Directory-Zugriffsaus.

> **Note**
>
> Sie müssen diesen Schritt auch dann ausführen, wenn der Status des Datei-Gateways alsJoined (Beigetreten)aus.

15. Vergewissern Sie sich, dass Ihre Freigaben unter der IP-Adresse der neuen Gateway-VM verfügbar sind, und löschen Sie dann die alte Gateway-VM.

> **Warning**
>
> Wenn ein Gateway gelöscht wird, gibt es keine Möglichkeit, es wiederherzustellen.

Weitere Informationen zum Löschen einer Amazon EC2 EC2-Instance finden Sie unterBeenden Ihrer InstanceimBenutzerhandbuch für Amazon EC2aus. Weitere Informationen zum Löschen einer KVM-, VMware- oder Hyper-V-VM finden Sie in der Dokumentation für Ihren Hypervisor.

Methode 2: Ersatzinstanz mit leerer Cache-Festplatte und neuer Gateway-ID

So richten Sie eine Ersatz-File Gateway-Instanz mit leerer Cache-Festplatte und neuer Gateway-ID

1. Halten Sie alle Anwendungen an, die in das vorhandene Datei-Gateway schreiben. Stellen Sie sicher, dass das`CachePercentDirty`-Metrik auf demÜberwachungTabulator ist`0`bevor Sie Dateifreigaben auf dem neuen Gateway einrichten.
2. Verwenden derAWS Command Line Interface(AWS CLI) um die Konfigurationsinformationen über Ihr vorhandenes Datei-Gateway und Dateifreigaben zu sammeln und zu speichern, indem Sie folgende Schritte ausführen:

   a. Speichern Sie die Gateway-Konfigurationsinformationen für das Datei-Gateway.

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

Dieser Befehl gibt einen JSON-Block aus, der Metadaten über das Gateway enthält, z. B. seinen Namen, Netzwerkschnittstellen, die konfigurierte Zeitzone und seinen Status (unabhängig davon, ob das Gateway ausgeführt wird).

b. Speichern Sie die SMB (Server Message Block) Einstellungen des Datei-Gateways.

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

Dieser Befehl gibt einen JSON-Block aus, der Metadaten zur SMB-Dateifreigabe enthält, z. B. den Domänennamen, den Microsoft Active Directory-Status, die Festlegung des Gastkennworts und die Art der Sicherheitsstrategie.

c. Speichern Sie Dateifreigabeinformationen für jede SMB- und Network File System (NFS-Dateifreigabe) des Datei-Gateways:

- Verwenden Sie den folgenden Befehl für SMB-Dateifreigaben.

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

Dieser Befehl gibt einen JSON-Block aus, der Metadaten zur NFS-Dateifreigabe enthält, z. B. Name, Speicherklasse, Status, IAM-Rolle Amazon Resource Name (ARN), eine Liste der Clients, die auf das Datei-Gateway zugreifen dürfen, und den vom SMB-Client zur Identifizierung des Einhängepunkts verwendeten Pfad.

- Verwenden Sie den folgenden Befehl für NFS-Dateifreigaben.

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

Dieser Befehl gibt einen JSON-Block aus, der Metadaten zur NFS-Dateifreigabe enthält, z. B. Name, Speicherklasse, Status, IAM-Rollen-ARN, eine Liste der Clients, die auf das Datei-Gateway zugreifen dürfen, und den vom NFS-Client zur Identifizierung des Einhängepunkts verwendeten Pfad.

3. Stoppen Sie das vorhandene Datei-Gateway wie folgt:

a. Halten Sie alle Anwendungen an, die in das vorhandene Datei-Gateway schreiben. Stellen Sie sicher, dass das`CachePercentDirty`-Metrik auf demÜberwachungTabulator ist`0`bevor Sie Dateifreigaben auf dem neuen Gateway einrichten.

b. Stoppen Sie das vorhandene Datei-Gateway, indem Sie die virtuelle Maschine (VM) ausschalten, die das Gateway hostet.

4. Erstellen Sie ein neues File Gateway.
5. Hängen Sie die Dateifreigaben ein, die auf dem alten Gateway konfiguriert wurden.
6. Vergewissern Sie sich, dass Ihr neues Gateway ordnungsgemäß funktioniert, und löschen Sie dann das alte Gateway von der Storage Gateway Gateway-Konsole.

> **Important**
>
> Bevor Sie ein Gateway löschen, stellen Sie sicher, dass derzeit keine Anwendungen in den Cache dieses Datei-Gateways schreiben. Wenn Sie ein Datei-Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten.

> **Warning**
>
> Wenn ein Gateway gelöscht wird, gibt es keine Möglichkeit, es wiederherzustellen.

7. Löschen Sie die alte virtuelle Gateway-Maschine oder EC2-Instanz.

Leistung

In diesem Abschnitt finden Sie Informationen zur Leistung von Storage Gateway Gateway-Leistung.

Themen

Leitfaden zur Leistung von Datei-Gateways

In diesem Abschnitt finden Sie eine Konfigurationsanleitung für die Bereitstellung von Hardware für Ihre File Gateway-VM. Die -Instance-Größen und -Typen, die in der Tabelle aufgeführt sind, sind Beispiele und dienen als Referenz.

Für eine optimale Leistung muss die Größe der Cache-Festplatte auf die Größe der aktiven Datensätze abgestimmt werden. Die Verwendung mehrerer lokaler Festplatten für den Cache erhöht die Schreibleistung durch Parallelisierung des Zugriffs auf Daten und führt zu höheren IOPS.

In den folgenden TabellenCache-TrefferLeseoperationen sind Lesevorgänge aus den Dateifreigaben, die vom Cache bearbeitet werden. Cache-FehlerLeseoperationen sind Lesevorgänge aus den Dateifreigaben, die von Amazon S3 bereitgestellt werden.

> **Note**
>
> Wir raten davon ab, flüchtigen Speicher zu verwenden. Weitere Informationen zur Verwendung des flüchtigen Speichers finden Sie unter Verwenden von kurzlebigem Speicher mit EC2-Gateways.

Im Folgenden finden Sie Beispielkonfigurationen für Datei-Gateways.

S3 File Gateway Leistung auf Linux-Clients

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz Cache-Treffer	Cache-Fehler-Lesevorsatz
Root-Datenträger: 80, GB io1, 4.000 IOPS Cache-Datenträger: 512 GiB Cache, io1, 1.500 bereitgestellte IOPS Minimale Netzwerkleistung: 10 Gbit/s CPU: 16 vCPU | RAM: 32 GB Für Linux empfohlenes NFS-Protokoll	nfsV3 - 1 Faden	110 MiB/Sek (0,92 Gbit/s)	590 MiB/s (4,9 Gbit/s)	310 MiB/s (2,6 Gbit/s)
	nfsV3 - 8 Themen	160 MiB/s (1,3 Gbit/s)	590 MiB/s (4,9 Gbit/s)	335 MiB/s (2,8 Gbit/s)
	NFSv4 - 1 Faden	130 MiB/Sek (1,1 Gbit/s)	590 MiB/s (4,9 Gbit/s)	295 MiB/s (2,5 Gbit/s)
	NFSv4 - 8 Themen	160 MiB/s (1,3 Gbit/s)	590 MiB/s (4,9 Gbit/s)	335 MiB/s (2,8 Gbit/s)
	SMBV3 - 1 Faden	115 MiB/s (1,0 Gbit/s)	325 MiB/s (2,7 Gbit/s)	255 MiB/Sek (2,1 Gbit/s)
	SMBV3 - 8 Themen	190 MiB/Sek (1,6 Gbit/s)	590 MiB/s (4,9 Gbit/s)	335 MiB/s (2,8 Gbit/s)
Storage Gateway-Hardware-Appliance Minimale Netzwerkleistung: 10 Gbit/s	nfsV3 - 1 Faden	265 MiB/s (2,2 Gbit/s)	590 MiB/s (4,9 Gbit/s)	310 MiB/s (2,6 Gbit/s)
	nfsV3 - 8 Themen	385 MiB/Sek (3,1 Gbit/s)	590 MiB/s (4,9 Gbit/s)	335 MiB/s (2,8 Gbit/s)
	NFSv4 - 1 Faden	310 MiB/s (2,6 Gbit/s)	590 MiB/s (4,9 Gbit/s)	295 MiB/s (2,5 Gbit/s)
	NFSv4 - 8 Themen	385 MiB/Sek (3,1 Gbit/s)	590 MiB/s (4,9 Gbit/s)	335 MiB/s (2,8 Gbit/s)

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz Cache-Treffer	Cache-Fehler-Lesevorsatz
	SMBV3 - 1 Faden	275 MiB/s (2,4 Gbit/s)	325 MiB/s (2,7 Gbit/s)	255 MiB/Sek (2,1 Gbit/s)
	SMBV3 - 8 Themen	455 MiB/s (3,8 Gbit/s)	590 MiB/s (4,9 Gbit/s)	335 MiB/s (2,8 Gbit/s)
Root-Datenträger: 80 GB, io1 SSD, 4.000 IOPS Cache-Datenträger: 4 x 2 TB NVME-Cache-Festplatten Minimale Netzwerkleistung: 10 Gbit/s CPU: 32 vCPU | RAM: 244 GB Für Linux empfohlenes NFS-Protokoll	nfsV3 - 1 Faden	300 MiB/s (2,5 Gbit/s)	590 MiB/s (4,9 Gbit/s)	325 MiB/s (2,7 Gbit/s)
	nfsV3 - 8 Themen	585 MiB/s (4,9 Gbit/s)	590 MiB/s (4,9 Gbit/s)	580 MiB/s (4,8 Gbit/s)
	NFSv4 - 1 Faden	355 MiB/s (3,0 Gbit/s)	590 MiB/s (4,9 Gbit/s)	340 MiB/s (2,9 Gbit/s)
	NFSv4 - 8 Themen	575 MiB/s (4,8 Gbit/s)	590 MiB/s (4,9 Gbit/s)	575 MiB/s (4,8 Gbit/s)
	SMBV3 - 1 Faden	230 MiB/s (1,9 Gbit/s)	325 MiB/s (2,7 Gbit/s)	245 MiB/s (2,0 Gbit/s)
	SMBV3 - 8 Themen	585 MiB/s (4,9 Gbit/s)	590 MiB/s (4,9 Gbit/s)	580 MiB/s (4,8 Gbit/s)

Leistung des Datei-Gateways auf Windows-Clients

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz Cache-Treffer	Cache-Fehler-Lesevorsatz
Root-Datenträger: 80, GB io1, 4.000 IOPS Cache-Datenträger: 512 GiB Cache, io1, 1.500 bereitgestellte IOPS Minimale Netzwerkleistung: 10 Gbit/s CPU: 16 vCPU | RAM: 32 GB Für Windows empfohlenes SMB-Protokoll	SMBV3 - 1 Faden	150 MiB/s (1,3 Gbit/s)	180 MiB/s (1,5 Gbit/s)	20 MiB/s (0,2 Gbit/s)
	SMBV3 - 8 Themen	190 MiB/Sek (1,6 Gbit/s)	335 MiB/s (2,8 Gbit/s)	195 MiB/Sek (1,6 Gbit/s)
	nfsV3 - 1 Faden	95 MiB/s (0,8 Gbit/s)	130 MiB/Sek (1,1 Gbit/s)	20 MiB/s (0,2 Gbit/s)
	nfsV3 - 8 Themen	190 MiB/Sek (1,6 Gbit/s)	330 MiB/s (2,8 Gbit/s)	190 MiB/Sek (1,6 Gbit/s)
Storage Gateway-Hardware-Appliance Minimale Netzwerkleistung: 10 Gbit/s	SMBV3 - 1 Faden	230 MiB/s (1,9 Gbit/s)	255 MiB/Sek (2,1 Gbit/s)	20 MiB/s (0,2 Gbit/s)
	SMBV3 - 8 Themen	835 MiB/s (7,0 Gbit/s)	475 MiB/s (4,0 Gbit/s)	195 MiB/Sek (1,6 Gbit/s)
	nfsV3 - 1 Faden	135 MiB/Sek (1,1 Gbit/s)	185 MiB/Sek (1,6 Gbit/s)	20 MiB/s (0,2 Gbit/s)
	nfsV3 - 8 Themen	545 MiB/Sek (4,6 Gbit/s)	470 MiB/s (4,0 Gbit/s)	190 MiB/Sek (1,6 Gbit/s)

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz Cache-Treffer	Cache-Fehler-Lesevorsatz
Root-Datenträger: 80 GB, io1 SSD, 4.000 IOPS Cache-Datenträger: 4 x 2 TB NVME-Cache-Festplatten Minimale Netzwerkleistung: 10 Gbit/s CPU: 32 vCPU | RAM: 244 GB Für Windows empfohlenes SMB-Protokoll	SMBV3 - 1 Faden	230 MiB/s (1,9 Gbit/s)	265 MiB/s (2,2 Gbit/s)	30 MiB/s (0,3 Gbit/s)
	SMBV3 - 8 Themen	835 MiB/s (7,0 Gbit/s)	780 MiB/s (6,5 Gbit/s)	250 MiB/s (2,1 Gbit/s)
	nfsV3 - 1 Faden	135 MiB/Sek (1.1. Gbit/s)	220 MiB/s (1,8 Gbit/s)	30 MiB/s (0,3 Gbit/s)
	nfsV3 - 8 Themen	545 MiB/Sek (4,6 Gbit/s)	570 MiB/s (4,8 Gbit/s)	240 MiB/s (2,0 Gbit/s)

> **Note**
>
> Die Leistung hängt von der Konfiguration Ihrer Hostplattform und der Netzwerkbandbreite ab.

Optimieren der Gateway-Leistung

Sie können Information im Folgenden darüber bekommen, wie die Leistung Ihrer Gateway optimiert werden kann. Die Anleitungen basiert auf Ihr Hinzufügen von Ressourcen zu Ihrem Gateway und auf dem Hinzufügen von Ressourcen auf Ihrem Anwendungsserver.

Hinzufügen von Ressourcen zu Ihrem Gateway

Sie können die Gateway-Leistung optimieren, indem Sie Ihrem Gateway mit einer der folgenden Methoden Ressourcen hinzufügen.

Verwenden von Hochleistungs-Festplatten

Zum Optimieren der Leistung Ihres Gateways können Sie Hochleistungsdatenträger hinzufügen, wie z. B. Solid-State Drives (SSDs) und einen NVMe-Controller. Sie können auch virtuelle Festplatten direkt von einem Storage Area Network (SAN) anstelle des Microsoft Hyper-V NTFS, zu Ihrer VM hinzufügen. Verbesserte Festplattenleistung führt in der Regel zu höherem Durchsatz und zu mehr Ein- und Ausgabe-Operationen pro Sekunde (IOPS). Weitere Informationen zum Hinzufügen von Datenträgern finden Sie unterHinzufügen von Cache-Speicheraus.

Verwenden Sie zum Messen des Durchsatzes die`ReadBytes`und`WriteBytes`-Metriken mit dem`Samples`Statistik von Amazon CloudWatch Beispiel: Mit dem `Samples` Statistik der `ReadBytes` Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie die IOPS. Allgemein gilt, wenn Sie diese Metriken für ein Gateway überprüfen, suchen Sie nach niedrigem Durchsatz und niedrigen IOPS.-Trends um Engpässe im Zusammenhang mit Datenträgern angeben zu können.

> **Note**
>
> CloudWatch-Metriken sind nicht für alle Gateways verfügbar. Weitere Informationen, zu Gateway Metriken, finden Sie unter Überwachen Sie Ihr Datei-Gateway.

Hinzufügen von CPU Ressourcen zu Ihrem Gateway-Host

Die Mindestanforderung für einen Gateway-Host-Server sind vier virtuelle Prozessoren. Um die Gateway-Leistung zu optimieren, vergewissern Sie sich, dass die vier virtuellen Prozessoren, die der Gateway-VM zugeordnet sind, von vier Kernen gestützt werden. Stellen Sie zudem sicher, dass Sie die CPUs des Host-Servers nicht überzeichnen.

Wenn Sie Ihrem Gateway-Host-Server weitere CPUs hinzufügen, erhöhen Sie die Verarbeitungskapazität des Gateways. Dadurch ermöglichen Sie Ihrem Gateway, gleichzeitig sowohl Daten aus Ihrer Anwendung in Ihrem lokalen Speicher zu sichern als auch diese Daten in Amazon S3 hochzuladen. Zusätzliche CPUs helfen auch sicherzustellen, dass Ihr Gateway

genug CPU-Ressourcen erhält, wenn der Host mit anderen VMs geteilt wird. Über genügend CPU-Ressourcen zu verfügen hat den allgemeinen Effekt der Verbesserung des Durchsatzes.

Storage Gateway unterstützt die Verwendung von 24 CPUs in Ihrem Gateway-Host-Server. Sie können mithilfe von 24 CPUs die Leistung Ihres Gateways verbessern. Wir empfehlen die folgenden Gateway-Konfiguration für Ihren Gateway-Host-Server:

- 24 CPUs
- 16 GiB reserviertes RAM für Datei-Gateways
  - 16 GiB reservierter RAM für Gateways mit Cachegröße bis zu 16 TiB
  - 32 GiB reservierter RAM für Gateways mit Cachegröße 16 TiB bis 32 TiB
  - 48 GiB reservierter RAM für Gateways mit Cachegröße 32 TiB bis 64 TiB
- Festplatte 1 zu paravirtual Controller 1 zugeordnet, als Gateway-Cache, wie folgt zu verwenden:
  - SSD unter Verwendung eines NVMe Controllers
- Festplatte 2 zu paravirtual Controller 1 zugeordnet, als Gateway-Upload-Puffer, wie folgt zu verwenden:
  - SSD unter Verwendung eines NVMe Controllers
- Festplatte 3 zu paravirtual Controller 2 zugeordnet, als Gateway-Upload-Puffer, wie folgt zu verwenden:
  - SSD unter Verwendung eines NVMe Controllers
- Netzwerkadapter 1 auf VM Netzwerk 1 konfiguriert:
  - Verwenden Sie VM-Netzwerk 1 und fügen Sie VMXnet3 (10 Gbit/s) zur Verwendung der Aufnahme hinzu.
- Netzwerkadapter 2 auf VM Netzwerk 2 konfiguriert:
  - Verwenden Sie VM-Netzwerk 2 und fügen Sie VMXnet3 (10 Gbit/s) hinzu, um eine Verbindung zu AWS herzustellen.

Sichern von virtuellen Gateway-Festplatten mit getrennten physischen Datenträgern

Bei der Bereitstellung von Gateway-Datenträgern wird dringend empfohlen, keine lokalen Festplatten für lokalen Speicher bereitzustellen, die die gleiche zugrunde liegende physische Speicherresso verwenden. Zum Beispiel, für VMware ESXi, die Zugrunde liegenden physische Speicherressourcen werden als Datenspeicher dargestellt. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-Dateien. Wenn Sie eine virtuelle Festplatte bereitstellen (z. B. als Upload-Puffer), können Sie die virtuelle Festplatte im gleichen Datenspeicher wie die VM oder in einem anderen Datenspeicher speichern.

Wenn Sie über mehr als einen Datenspeicher verfügen, sollten Sie unbedingt einen Datenspeicher für jeden Typ von lokalem Speicher wählen, den sie erstellen. Ein Datenspeicher, der nur durch einen einzigen zugrunde liegenden physischen Datenträger gestützt wird, kann zu einer schlechten Leistung führen. Beispielsweise wenn Sie solch einen Datenträger sowohl zum Stützen des Cache-Speichers als auch des Upload-Puffers in einer Gateway-Konfiguration verwenden. Dementsprechend kann auch ein Datenspeicher, der durch eine leistungsschwächere RAID-Konfiguration gestützt wird, wie z. B. RAID 1, eine schlechte Leistung zur Folge haben.

Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung

Erhöhen der Bandbreite zwischen Ihrem Anwendungsserver und Ihrem Gateway

Zum Optimieren der Gateway-Leistung, stellen Sie sicher, dass die Netzwerkbandbreite zwischen Ihrer Anwendung und dem Gateway, Ihre Anwendungsansprüche unterstützen kann. Sie können das`ReadBytes`und`WriteBytes`Metriken des Gateways zur Messung des gesamten Datendurchsatzes.

Für Ihre Anwendung, vergleichen Sie den gemessenen Durchsatz mit dem gewünschten Durchsatz. Wenn der gemessene Durchsatz weniger als der gewünschte Durchsatz beträgt, dann kann die Erhöhung der Bandbreite zwischen Ihrer Anwendung und dem Gateway die Leistung verbessern können, wenn das Netzwerk der Engpass ist. Ebenso können Sie die Bandbreite zwischen Ihrer VM und Ihren lokalen Festplatten erhöhen, wenn sie nicht direkt angeschlossenen sind.

Hinzufügen von CPU-Ressourcen zu Ihrer Anwendungsumgebung

Kann Ihre Anwendung zusätzliche CPU-Ressourcen verwenden, kann das Hinzufügen weiterer CPUs dazu beitragen, dass Ihre Anwendung die E/A-Last skaliert.

Verwenden von VMware vSphere High Availability mit Storage Gateway

Storage Gateway bietet eine hohe Verfügbarkeit für VMware durch eine Reihe von Zustandsprüfungen auf Anwendungsebene, die in VMware vSphere High Availability (VMware HA) integriert sind. Dieser Ansatz schützt Speicher-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen. Darüber hinaus schützt er vor Softwarefehlern wie beispielsweise Timeouts während der Verbindung und Nichtverfügbarkeit von Dateifreigaben oder Volumes.

Durch diese Integration wird ein Gateway, das in einer On-Premise-VMware-Umgebung oder in einer VMware Cloud auf AWS bereitgestellt wird, automatisch nach den meisten Serviceunterbrechungen wiederhergestellt. Dies geschieht dies in der Regel in weniger als 60 Sekunden ohne Datenverlust.

Führen Sie die folgenden Schritte aus, um VMware HA mit Storage Gateway zu verwenden.

Themen

Konfigurieren Ihres vSphere VMware HA-Clusters

Erstellen Sie zunächst einen VMware-Cluster, wenn Sie dies noch nicht getan haben. Informationen zum Erstellen eines VMware-Clusters finden Sie unter Erstellen eines vSphere HA-Clusters in der VMware-Dokumentation.

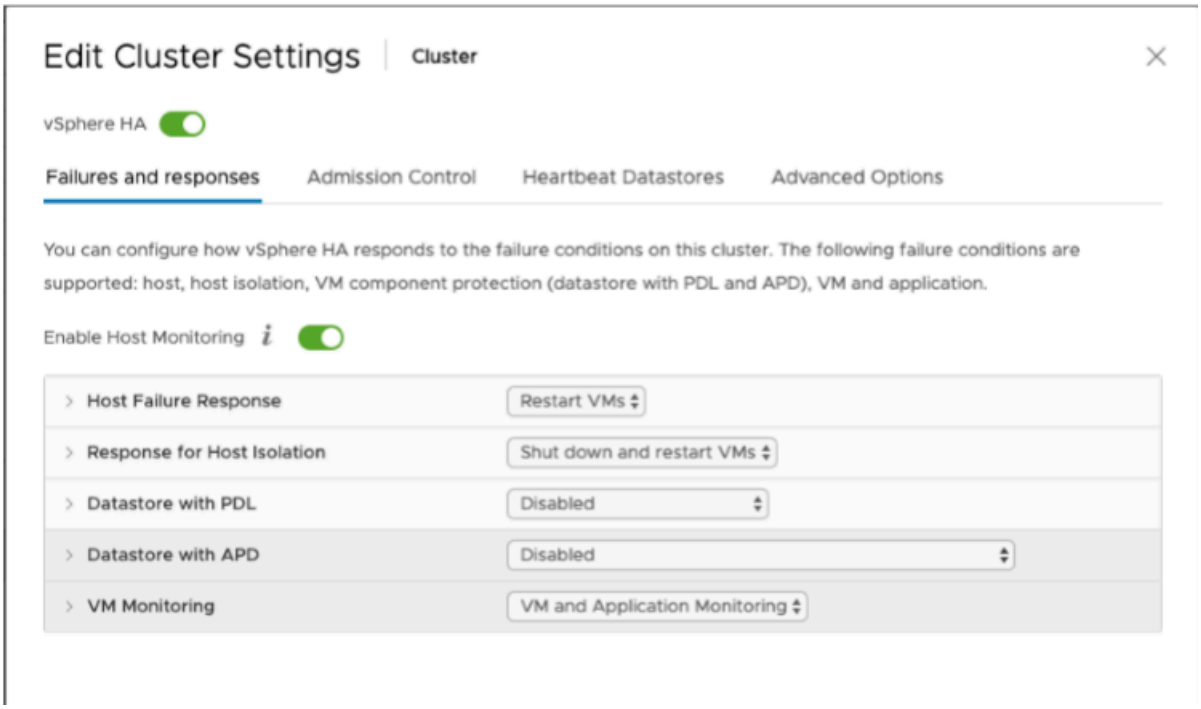
Konfigurieren Sie anschließend Ihren VMware-Cluster für die Arbeit mit Storage Gateway.

So konfigurieren Sie Ihren VMware-Cluster

1. Stellen Sie auf der Seite Edit Cluster Settings (Clustereinstellungen bearbeiten) in VMware vSphere sicher, dass die VM-Überwachung für die VM- und Anwendungsüberwachung konfiguriert ist. Legen Sie hierzu die folgenden Optionen wie aufgeführt fest:

   - Host-Fehlerantwort: Restart VMs
   - Antwort für Host-Isolation: VMs herunterfahren und neu starten
   - Datastore mit PDL: Deaktiviert
   - Datastore mit APD: Deaktiviert
   - VM-Überwachung: Überwachung von VM und Application Monitoring

   Im folgenden Screenshot sehen Sie ein Beispiel.



2. Optimieren Sie die Empfindlichkeit des Clusters, indem Sie die folgenden Werte anpassen:

   - Fehlerintervall— Nach diesem Intervall wird die VM neu gestartet, wenn kein VM-Heartbeat empfangen wird.
   - Minimale Betriebszeit— Der Cluster wartet so lange, nachdem eine VM mit der Überwachung der Heartbeat von VM-Tools begonnen hat.
   - Maximale Zurücksetzungen pro VM— Der Cluster startet die VM innerhalb des Zeitfensters für maximale Zurückstellungen maximal so viele Male.
   - Maximum resets time window— Das Zeitfenster, in dem die maximalen Zurücksetzungen pro VM gezählt werden sollen.

   Wenn Sie nicht sicher sind, welche Werte Sie festlegen sollen, verwenden Sie die folgenden Beispieleinstellungen:

   - Failure interval (Fehlerintervall): **30** Sekunden
   - Minimum uptime (Mindestbetriebszeit): **120** Sekunden
   - Maximum per-VM resets (Maximale Zurücksetzungen pro VM): **3**
   - Maximum resets time window (Zeitfenster für maximale Zurücksetzungen): **1** Stunde

Wenn auf dem Cluster andere VMs ausgeführt werden, können Sie diese Werte speziell für Ihre VM festlegen. Dies ist erst möglich, wenn Sie die VM über das OVA-Image bereitstellen. Weitere Hinweise zum Festlegen dieser Werte finden Sie unter (Optional) Hinzufügen von Überschreibungsoptionen für andere VMs auf Ihrem Cluster.

Laden Sie das OVA-Image für Ihren Gateway-Typ herunter

Gehen Sie folgendermaßen vor, um das OVA-Image herunterzuladen.

So laden Sie das OVA-Image für Ihren Gateway-Typ herunter

- Laden Sie das OVA-Image für Ihren Gateway-Typ von einem der folgenden Orte herunter:
  - File Gateway —

Bereitstellen des Gateways

Stellen Sie das OVA-Image in Ihrem konfigurierten Cluster auf einem der Cluster-Hosts bereit.

So stellen Sie das OVA-Image des Gateways bereit

1. Stellen Sie das OVA-Image auf einem der Hosts im Cluster bereit.
2. Stellen Sie sicher, dass die Datenspeicher, die Sie für den Stamm-Datenträger und den Cache wählen, für alle Hosts im Cluster verfügbar sind.

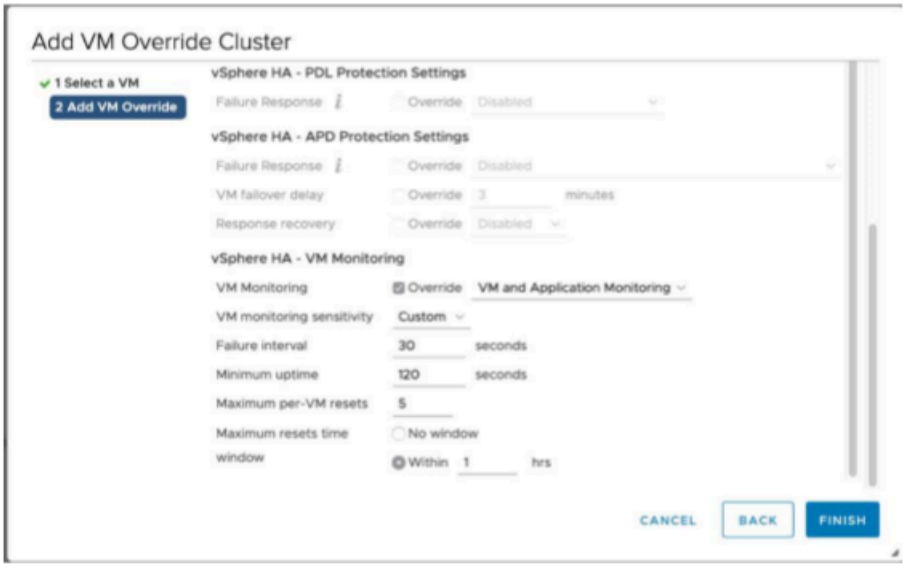
(Optional) Hinzufügen von Überschreibungsoptionen für andere VMs auf Ihrem Cluster

Wenn auf Ihrem Cluster andere VMs ausgeführt werden, können Sie die Clusterwerte speziell für jede einzelne VM festlegen.

So fügen Sie Überschreibungsoptionen für andere VMs in Ihrem Cluster hinzu

1. Wählen Sie Ihren Cluster auf der Seite Summary (Zusammenfassung), um die Clusterseite zu öffnen, und wählen Sie dann Configure (Konfigurieren).
2. Wählen Sie die Registerkarte Configuration (Konfiguration) und dann VM Overrides (VM-Überschreibungen)aus.
3. Fügen Sie eine neue VM-Überschreibungsoption hinzu, um die einzelnen Werte zu ändern.

Im folgenden Screenshot sehen Sie Überschreibungsoptionen.



Aktivieren des Gateways

Nachdem das OVA-Image für Ihr Gateway bereitgestellt wurde, aktivieren Sie Ihr Gateway. Die entsprechenden Anweisungen unterscheiden sich je nach Gateway-Typ.

So aktivieren Sie das Gateway

- Befolgen Sie die Anweisungen zur Aktivierung für Ihren Gateway-Typ.
  - File Gateway —

Testen der Konfiguration von VMware High Availability

Testen Sie Ihre Konfiguration, nachdem Sie Ihr Gateway aktiviert haben.

So testen Sie Ihre Konfiguration für VMware HA

1. Öffnen Sie die Speicher-Gateway-Konsole unterhttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie im Navigationsbereich Gateways und anschließend das Gateway aus, das Sie auf VMware HA testen möchten.

3. Wählen Sie unter Actions (Aktionen) die Option Verify VMware HA (Überprüfen von VMware HA) aus.
4. Wählen Sie im Feld Verify VMware High Availability Configuration (Überprüfen der Konfiguration von VMware High Availability), das jetzt angezeigt wird, die Option OK.

   > **Note**
   >
   > Wenn Sie die Konfiguration für VMware HA testen, wird Ihre Gateway-VM neu gestartet und die Verbindung zu Ihrem Gateway unterbrochen. Der Test kann einige Minuten in Anspruch nehmen.

   Wenn der Test erfolgreich abgeschlossen wurde, wird der Status Verified (Überprüft) auf der Registerkarte "Details" des Gateways in der Konsole angezeigt.
5. Wählen Sie Exit (Beenden) aus.

Informationen zu VMware HA-Ereignissen finden Sie in den Amazon CloudWatch CloudWatch-Protokollgruppen. Weitere Informationen finden Sie unter Abrufen von Datei-Gateway-Integritätsprotokollen mit CloudWatch.

Sicherheit inAWSStorage Gateway

Die Sicherheit in der Cloud hat AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sichherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Um mehr über die Compliance-Programme zu erfahren, die für geltenAWSStorage Gateway finden Sie unterAWSProgramm in Scope nach Compliance-Programmaus.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Storage Gateway angewendet werden kann. Die folgenden Themen veranschaulichen, wie Sie Storage Gateway konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren außerdem, wie Sie andere verwendenAWS-Services, um Ihre Storage Gateway Gateway-Ressourcen zu überwachen und zu schützen.

Themen

Datenschutz inAWSStorage Gateway

DieAWS Modell der übergeordneten Verantwortunggilt für den Datenschutz inAWSStorage Gateway Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt enthält die Sicherheitskonfigurations- und Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und die GDPR im Blog zur AWS-Sicherheit.

Wir empfehlen aus Gründen des Datenschutzes, dass Sie AWS-Konto-Anmeldeinformationen schützen und die Benutzerkonten jeweils mit AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentication (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Storage Gateway oder einem anderen arbeitenAWSDienste, die die Konsole verwenden, API,AWS CLI, oderAWSSDKs. Alle Daten, die Sie in Tags (Markierungen) oder Freiformfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, Sie

keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung mitAWS KMS

Storage Gateway verwendet für die Verschlüsselung von Daten, die zwischen Ihrer Gateway-Appliance übertragen werden, SSL/TLS (Secure Socket Layers/Transport Layer Security) verschlüsselt werden.AWS-Speicher. Standardmäßig verwendet Storage Gateway Amazon S3-verwaltete Verschlüsselungsschlüssel, um alle in Amazon S3 gespeicherten Daten serverseitig zu verschlüsseln. Sie können die Storage Gateway-API verwenden, um Ihr Gateway so zu konfigurieren, dass in der Cloud gespeicherte Daten mithilfe der serverseitigen Verschlüsselung verschlüsselt werden.AWS Key Management Service(SSE-KMS) Kundenmasterschlüssel (CMKs).

> **Important**
>
> Wenn Sie eineAWS KMSFür serverseitige Verschlüsselung müssen Sie einen symmetrischen CMK wählen. Storage Gateway bietet keine Unterstützung für asymmetrische CMKs. Weitere Informationen finden Sie unter Using Symmetric and Asymmetric Keys (Verwenden von symmetrischen und asymmetrischen Schlüsseln) im AWS Key Management Service-Benutzerhandbuch.

Verschlüsseln einer Dateifreigabe

Für eine Dateifreigabe können Sie Ihr Gateway so konfigurieren, dass Ihre Objekte mit verschlüsselt werdenAWS KMS—verwaltete Schlüssel unter Verwendung von SSE-KMS. Weitere Informationen zur Verwendung der Storage Gateway Gateway-API zum Verschlüsseln von Daten in einer Dateifreigabe finden Sie unterCreateNFSFileShareimAWS Storage Gateway-API-Referenzaus.

Verschlüsseln eines Dateisystems

Weitere Informationen finden Sie unterDatenverschlüsselung in Amazon FSximBenutzerhandbuch für Amazon FSx for Windows File Serveraus.

Wenn Sie AWS KMS verwenden, um Ihre Daten zu verschlüsseln, müssen Sie Folgendes beachten:

- Ihre Daten werden im Ruhezustand in der Cloud verschlüsselt. Das heißt, die Daten werden in Amazon S3 verschlüsselt.

- IAM-Benutzer müssen über die erforderlichen Berechtigungen zum Aufrufen derAWS KMSAPI-Operationen Weitere Informationen finden Sie unterVerwenden von IAM-Richtlinien mitAWS KMSimAWS Key Management ServiceEntwicklerhandbuchaus.
- Wenn Sie Ihren CMK löschen oder deaktivieren oder das Token für die Berechtigungserteilung widerrufen, können Sie nicht auf die Daten auf dem Volume oder Band zugreifen. Weitere Informationen finden Sie unterLöschen von KundenmasterschlüsselnimAWS Key Management ServiceEntwicklerhandbuchaus.
- Wenn Sie einen Snapshot von einem Volume erstellen, das KMS-verschlüsselt ist, wird der Snapshot verschlüsselt. Der Snapshot erbt den KMS-Schlüssel des Volumes.
- Wenn Sie ein neues Volume aus einem KMS-verschlüsselten Snapshot erstellen, wird der Snapshot verschlüsselt. Sie können einen anderen KMS-Schlüssel für das neue Volume angeben.

> **Note**
>
> Storage Gateway unterstützt derzeit nicht das Erstellen eines unverschlüsselten Volume von einem Wiederherstellungspunkt eines KMS-verschlüsselten Volumes oder eines KMS-verschlüsselten Snapshots.

Weitere Informationen zu AWS KMS finden Sie unter Was ist AWS Key Management Service?

Authentifizierung und Zugriffskontrolle für Storage Gateway

Für den Zugriff auf AWS Storage Gateway werden Anmeldeinformationen benötigt, die AWSzur Authentifizierung Ihrer Anforderungen verwenden kann. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff verfügenAWS-Ressourcen, wie ein Gateway, eine Dateifreigabe, ein Volume oder ein Band. In den folgenden Abschnitten finden Sie Details zur Verwendung vonAWS Identity and Access Management(ICH)und Storage Gateway zum Schutz Ihrer -Ressourcen, indem Sie den Zugriff darauf kontrollieren.

- Authentifizierung
- Zugriffskontrolle

Authentifizierung

Sie können mit einer der folgenden Identitäten auf AWS zugreifen:

- AWS-Konto-Stammbenutzer – Wenn Sie ein AWS-Konto neu erstellen, enthält es zunächst nur eine einzelne Anmeldeidentität, die über kompletten Zugriff auf sämtliche AWS-Services und -Ressourcen im Konto verfügt. Diese Identität wird als AWS-Konto-Stammbenutzer bezeichnet. Um auf den Stammbenutzer zuzugreifen, müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Bleiben Sie stattdessen bei dem bewährten Verfahren, den Stammbenutzer nur zu verwenden, um Ihren ersten IAM-Benutzer zu erstellen. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.
- IAM-Benutzer— EinIAM-Benutzerist eine Identität in IhremAWS-Kontowelche über bestimmte benutzerdefinierte Berechtigungen verfügen (z. B. Berechtigungen zum Erstellen eines Gateways in Storage Gateway). Sie können einen IAM-Benutzernamen und ein Passwort für die Anmeldung bei sicheren AWS-Webseiten verwenden. Dazu zählen beispielsweise die AWS Management Console, AWS-Diskussionsforen und das AWS -Support Center.

  Zusätzlich zu einem Benutzernamen und Passwort können Sie Zugriffsschlüssel für jeden Benutzer erstellen. Sie können diese Schlüssel verwenden, wenn Sie auf AWS-Services programmatisch zugreifen, entweder über eines der verschiedenen SDKs oder mit der AWS Command Line Interface (CLI). Das SDK und die CLI-Tools verwenden die Zugriffsschlüssel, um Ihre Anfrage verschlüsselt zu signieren. Wenn Sie keine AWS-Tools verwenden, müssen Sie die Anforderung selbst signieren. Storage Gateway unterstütztSignaturversion 4, ein Protokoll für die Authentifizierung eingehender API-Anfragen. Weitere Informationen zur Authentifizierung von Anforderungen Sie unter Signaturprozess mit Signaturversion 4 in der Allgemeinen AWS-Referenz.

- IAM-Rolle – Eine IAM-Rolle ist eine IAM-Identität, die Sie in Ihrem Konto mit bestimmten Berechtigungen erstellen können. Eine IAM-Rolle ist einem IAM-Benutzer ähnlich, weil es sich um eine AWS-Identität mit Berechtigungsrichtlinien handelt, die festlegen, welche Aktionen die Identität in AWS ausführen kann und welche nicht. Eine Rolle ist jedoch nicht einer einzigen Person zugeordnet, sondern kann von allen Personen angenommen werden, die diese Rolle benötigen. Einer Rolle sind außerdem keine standardmäßigen, langfristigen Anmeldeinformationen (Passwörter oder Zugriffsschlüssel) zugeordnet. Wenn Sie eine Rolle annehmen, erhalten Sie stattdessen temporäre Anmeldeinformationen für Ihre Rollensitzung. IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundener Benutzerzugriff – Statt einen IAM-Benutzer zu erstellen, können Sie bereits vorhandene Identitäten von AWS Directory Service, vom Benutzerverzeichnis Ihres Unternehmens oder von einem Web-Identitätsanbieter verwenden. Diese werden als verbundene Benutzer bezeichnet. AWS weist einem verbundenen Benutzer eine Rolle zu, wenn der Zugriff über einen Identitätsanbieter angefordert wird. Weitere Informationen zu verbundenen Benutzern finden Sie unter Verbundene Benutzer und Rollen im IAM-Benutzerhandbuch.

- AWS Zugriff auf -Services – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Konto für Sie auszuführen. Ein IAM-Administrator kann eine Servicerolle in IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle nutzen, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI oder AWS-API-Anforderungen durchführen. Das ist empfehlenswerter als Zugriffsschlüssel innerhalb der EC2 Instance zu speichern. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Zugriffskontrolle

Sie können über gültige Anmeldeinformationen zur Authentifizierung Ihrer Anfragen verfügen, doch Sie können die Storage-Gateway-Ressourcen nur mit entsprechenden Berechtigungen erstellen oder darauf zugreifen. Beispielsweise müssen Sie die Berechtigung zum Erstellen eines Gateways in Storage Gateway besitzen.

In den folgenden Abschnitten wird die Verwaltung von Berechtigungen für Storage Gateway beschrieben. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- Übersicht über die Verwaltung von Zugriffsberechtigungen für Ihr Storage Gateway

- Identitätsbasierte Richtlinien (IAM-Richtlinien)

Übersicht über die Verwaltung von Zugriffsberechtigungen für Ihr Storage Gateway

EVERYAWS-Ressource ist Eigentum eines Amazon Web Services Services-Kontos und die Berechtigungen für die Erstellung einer Ressource oder den Zugriff darauf werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann IAM-Identitäten (d. h. Benutzer, Gruppen und Rollen) Berechtigungsrichtlinien zuweisen. Manche Services (z. B. AWS Lambda) unterstützen auch die Zuweisung von Berechtigungsrichtlinien zu Ressourcen.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorrechten. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Beim Erteilen von Berechtigungen entscheiden Sie, wer die Berechtigungen erhält, für welche Ressourcen die Berechtigungen gelten und welche Aktionen an diesen Ressourcen gestattet werden sollen.

Themen

Storage Gateway Gateway-Ressourcen und Operationen

In Storage Gateway ist die primäre Ressource einToraus. Storage Gateway unterstützt auch die folgenden zusätzlichen Ressourcentypen: Dateifreigabe- Volume, virtuelles Band, iSCSI-Ziel und VTL-Gerät (Virtual Tape Library). Diese werden als Subressourcen bezeichnet und existieren nur, wenn sie mit einem Gateway verknüpft sind.

Diesen Ressourcen und Unterressourcen sind eindeutige Amazon-Ressourcennamen (ARN) zugeordnet, wie in der folgenden Tabelle zu sehen ist.

Ressourcentyp	ARN-Format
Gateway-ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
Dateifreigabe-ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

> **Note**
>
> Storage Gateway Gateway-Ressourcen-IDs werden in Großbuchstaben geschrieben. Wenn Sie diese Ressourcen-IDs mit der Amazon EC2-API verwenden, erwartet Amazon EC2 Ressourcen-IDs in Kleinbuchstaben. Sie müssen Ihre Ressourcen-ID in Kleinbuchstaben ändern, um Sie mit der EC2-API verwenden zu können. Bei einem Storage Gateway beispielsweise könnte die ID für ein Volume `vol-1122AABB` lauten. Wenn Sie diese ID mit der EC2-API verwenden, müssen Sie sie zu `vol-1122aabb` ändern. Andernfalls verhält sich die EC2-API möglicherweise nicht wie erwartet.
> ARNs für Gateways, die vor dem 2. September 2015 aktiviert wurden, enthalten den Gateway-Namen anstelle der Gateway-ID. Verwenden Sie die `DescribeGatewayInformation`-API-Operation, um den ARN für das Gateway zu erhalten.

Zur Erteilung von Berechtigungen für bestimmte API-Operationen, wie z. B. das Erstellen eines Bands, bietet Storage Gateway eine Reihe von API-Aktionen, mit denen Sie diese Ressourcen und Subressourcen erstellen und verwalten können. Eine Liste der API-Aktionen finden Sie unterAktionenimAWS Storage Gateway-API-Referenzaus.

Zum Erteilen von Berechtigungen für bestimmte API-Operationen, wie z. B. das Erstellen eines Bands, definiert Storage Gateway eine Reihe von Aktionen, die Sie in einer Berechtigungsrichtlinie angeben können, um Berechtigungen für bestimmte API-Operationen zu erteilen. Für eine API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein. Eine Tabelle mit allen Storage Gateway Gateway-API-Aktionen und den Ressourcen, für die diese gelten, finden Sie unterSpeicher-Gateway-API-Berechtigungen: Referenz für Aktionen, Ressourcen und Bedingungsschlüsselaus.

Grundlegendes zum Eigentum an Ressourcen

EINRessourcenbesitzerist das Amazon Web Services Services-Konto, das die Ressource erstellt hat. Das heißt, der Ressourceneigentümer ist das Amazon Web Services Services-Konto desHaupteinheit(das Root-Konto, ein IAM-Benutzer oder eine IAM-Rolle), welche die Anforderung, die die Ressource erstellt, authentifiziert. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie die Stammkonto-Anmeldeinformationen Ihres Amazon Web Services Services-Kontos zum Aktivieren eines Gateways verwenden, ist Ihr Amazon Web Services Services-Konto Eigentümer der Ressource (in Storage Gateway ist die Ressource das Gateway).
- Wenn Sie einen IAM-Benutzer in Ihrem Amazon Web Services Services-Konto erstellen und Berechtigungen für die`ActivateGateway`-Aktion für diesen Benutzer kann der Benutzer ein Gateway aktivieren. Eigentümer der Gateway-Ressource ist jedoch das Amazon Web Services Services-Konto, zu dem der Benutzer gehört.
- Wenn Sie in Ihrem Amazon Web Services Services-Konto eine IAM-Rolle mit Berechtigungen zum Aktivieren eines Gateways erstellen, kann jeder, der die Rolle übernimmt, ein Gateway aktivieren. Eigentümer der Gateway-Ressource ist immer das Amazon Web Services Services-Konto, zu dem die Rolle gehört.

Verwalten des Zugriffs auf Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> Dieser Abschnitt behandelt die Verwendung von IAM um Zusammenhang mit Storage Gateway. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unterWas ist IAMimIAM-BenutzerhandbuchFür Informationen über die Syntax und Beschreibungen von AWS-IAM-Richtlinien lesen Sie die IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Richtlinien, die einer IAM-Identität zugeordnet sind, werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet, während Richtlinien, die einer Ressource zugeordnet sind,

ressourcenbasierte Richtlinien genannt werden. Storage Gateway unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

Identitätsbasierte Richtlinien (IAM-Richtlinien)

Richtlinien können IAM-Identitäten angefügt werden. Sie können z. B. Folgendes tun:

- Anfügen von Berechtigungsrichtlinien zu Benutzern oder Gruppen in Ihrem Konto— Ein Kontoadministrator kann eine Berechtigungsrichtlinie verwenden, die einem bestimmten Benutzer zugeordnet ist, um diesem Benutzer Berechtigungen zum Erstellen einer Storage Gateway Gateway-Ressource zu erteilen, zum Beispiel eines Gateways, eines Volumes oder eines Bands.
- Einer Rolle eine Berechtigungsrichtlinie zuweisen (kontoübergreifende Berechtigungen gewähren) – Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Berechtigungen zu erteilen. Beispielsweise kann der Administrator in Konto A eine Rolle erstellen, um einem anderen Amazon Web Services-Konto (z. B. Konto B) oder einem anderen Amazon Web Services Services-Konto (z. B. Konto B) kontoübergreifende Berechtigungen zu erteilen.AWSService wie folgt:

  1. Der Administrator von Konto A erstellt eine IAM-Rolle und fügt ihr eine Berechtigungsrichtlinie an, die Berechtigungen für Ressourcen in Konto A erteilt.
  2. Der Administrator von Konto A weist der Rolle eine Vertrauensrichtlinie zu, die Konto B als den Prinzipal identifiziert, der die Rolle übernehmen kann.
  3. Der Administrator von Konto B kann nun Berechtigungen zur Übernahme der Rolle an alle Benutzer in Konto B delegieren. Daraufhin können die Benutzer in Konto B auf Ressourcen von Konto A zugreifen. Der Prinzipal in der Vertrauensrichtlinie kann auch ein AWS-Service-Prinzipal sein. Somit können Sie auch einem AWS-Service die Berechtigungen zur Übernahme der Rolle erteilen.

  Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

Es folgt ein Beispiel für eine Richtlinie, die Berechtigungen für alle `List*`-Aktionen für alle Ressourcen erteilt. Diese Aktion ist eine schreibgeschützte Aktion. Daher lässt die Richtlinie nicht zu, dass der Benutzer den Status der Ressourcen ändert.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllListActionsOnAllResources",
            "Effect": "Allow",
            "Action": [
                "storagegateway:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zur Verwendung von identitätsbasierten Richtlinien mit Storage Gateway finden Sie unterVerwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für Storage Gatewayaus. Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Andere Services, z. B. Amazon S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem S3 Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. Storage Gateway bietet keine Unterstützung für ressourcenbasierte Richtlinien.

Angeben von Richtlinienelementen: Aktionen, Effekte, Ressourcen und Prinzipale

Für jede Storage Gateway Gateway-Ressource (siheSpeicher-Gateway-API-Berechtigungen: Referenz für Aktionen, Ressourcen und Bedingungsschlüssel) definiert der Dienst eine Reihe von API-Operationen (sieheAktionen) enthalten. Zur Erteilung von Berechtigungen für diese API-Operationen definiert Storage Gateway eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können. Für die Storage Gateway Gateway-Ressource beispielsweise sind die folgenden Aktionen definiert:`ActivateGateway`,`DeleteGateway`, und`DescribeGatewayInformation`aus. Zur Durchführung einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- Ressource – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt. Für Storage Gateway Gateway-Ressourcen verwenden Sie immer das Platzhalterzeichen(*)in IAM-Richtlinien. Weitere Informationen finden Sie unter Storage Gateway Gateway-Ressourcen und Operationen.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Zum Beispiel abhängig von dem angegebenen`Effect`, der`storagegateway:ActivateGateway`berechtigt oder verweigert Benutzerberechtigungen für die Durchführung des Storage Gateway`ActivateGateway`verwenden.
- Auswirkung – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten ("Allow"), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.
- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). Storage Gateway bietet keine Unterstützung für ressourcenbasierte Richtlinien.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der AWS-IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Eine Tabelle mit allen -Storage Gateway-API-Aktionen finden Sie unterSpeicher-Gateway-API-Berechtigungen: Referenz für Aktionen, Ressourcen und Bedingungsschlüsselaus.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie beim Erteilen von Berechtigungen wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema Bedingung im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Für Storage Gateway gibt es keine speziellen Bedingungsschlüssel. Stattdessen können Sie nach Bedarf die AWS-weiten

Bedingungsschlüssel verwenden. Eine vollständige Liste der AWS-weiten Schlüssel enthält der Abschnitt Verfügbare Schlüssel im IAM Benutzerhandbuch.

Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für Storage Gateway

In diesem Thema finden Sie Beispiele für identitätsbasierte Richtlinien, in denen ein Kontoadministrator den IAM-Identitäten (Benutzer, Gruppen und Rollen) Berechtigungsrichtlinien anfügen kann.

> **Important**
>
> Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die Grundkonzepte und für Sie verfügbaren Optionen zum Verwalten des Zugriffs auf Ihre Storage Gateway Gateway-Ressourcen erläutert werden. Weitere Informationen finden Sie unter Übersicht über die Verwaltung von Zugriffsberechtigungen für Ihr Storage Gateway.

Das Thema besteht aus folgenden Abschnitten:

- Erforderliche Berechtigungen für die Verwendung der Storage Gateway
- AWSverwaltete Richtlinien für Storage Gateway
- Beispiele für vom Kunden verwaltete Richtlinien

Hier ein Beispiel für eine Berechtigungsrichtlinie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ActivateGateway",
                "storagegateway:ListGateways"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

Die Richtlinie enthält zwei Anweisungen (beachten Sie die Elemente `Action` und `Resource` in beiden Anweisungen):

- Die erste Anweisung erteilt Berechtigungen für zwei Storage Gateway Gateway-Aktionen (`storagegateway:ActivateGatewayundstoragegateway:ListGateways`) auf einer Gateway-Ressource.

  Das Platzhalterzeichen (*) bedeutet, dass diese Anweisung jeder Ressource entsprechen kann. In diesem Fall erlaubt die -Anweisung die`storagegateway:ActivateGatewayundstoragegateway:ListGatewaysAktionen` auf jedem Gateway. Das Platzhalterzeichen wird hier verwendet, da Sie die Ressourcen-ID erst nach Erstellen des Gateways kennen. Weitere Informationen zur Verwendung eines Platzhalterzeichens (*) in einer Richtlinie finden Sie unter Beispiel 2: Zulassen schreibgeschützten Zugriff auf ein Gateway.

  > **Note**
  >
  > ARNs identifizieren eindeutigAWSRessourcen schätzen. Weitere Informationen finden Sie unter Amazon-Ressourcenname (ARNs) und AWS Service-Namespaces in der Allgemeinen AWS-Referenz.

  Um Berechtigungen für eine bestimmte Aktion auf ein bestimmtes Gateway zu beschränken, erstellen Sie eine separate Anweisung für diese Aktion in der Richtlinie und geben Sie die Gateway-ID in der Anweisung an.

- Die zweite Anweisung erteilt Berechtigungen für die Aktionen `ec2:DescribeSnapshots` und `ec2:DeleteSnapshot`. Diese Amazon Elastic Compute Cloud (Amazon EC2) -Aktionen erfordern Berechtigungen, da von Storage Gateway generierte Snapshots im Amazon Elastic Block Store (Amazon EBS) gespeichert und als Amazon EC2 EC2-Ressourcen verwaltet werden. Daher erfordern sie entsprechende EC2-Aktionen. Weitere Informationen finden Sie unterAktionenimAmazon EC2 EC2-API-Referenzaus. Da diese Amazon EC2 EC2-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, ist in der Richtlinie das Platzhalterzeichen (*) als`Resource`value statt einen Gateway-ARN anzugeben.

Eine Tabellenliste mit allen Storage Gateway Gateway-API-Aktionen und den Ressourcen, für die diese gelten, finden Sie hier:Speicher-Gateway-API-Berechtigungen: Referenz für Aktionen, Ressourcen und Bedingungsschlüsselaus.

Erforderliche Berechtigungen für die Verwendung der Storage Gateway

Zum Verwenden der Storage Gateway Gateway-Konsole müssen Sie Leseberechtigungen erteilen. Wenn Sie vorhaben, Snapshots zu beschreiben, müssen Sie auch Berechtigungen für zusätzliche Aktionen gewähren, wie in der folgenden Berechtigungsrichtlinie gezeigt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Diese zusätzliche Berechtigung ist erforderlich, da die von Storage Gateway generierten Amazon EBS-Snapshots als Amazon EC2 EC2-Ressourcen verwaltet werden.

Informationen zum Einrichten von Mindestberechtigungen für die Navigation in der Storage Gateway Gateway-Konsole finden Sie unterBeispiel 2: Zulassen schreibgeschützten Zugriff auf ein Gatewayaus.

AWSverwaltete Richtlinien für Storage Gateway

Amazon Web Services deckt viele häufige Anwendungsfälle ab, indem es eigenständige IAM-Richtlinien bereitstellt, die von erstellt und administriert werden.AWSaus. Die verwalteten Richtlinien erteilen die erforderlichen Berechtigungen für viele häufige Anwendungsfälle, sodass Sie nicht mühsam ermitteln müssen, welche Berechtigungen erforderlich sind. Weitere Informationen zuAWSVerwaltete Richtlinien finden Sie unterAWS-verwaltete RichtlinienimIAM User Guideaus.

FolgendesAWSverwaltete Richtlinien, die Sie an Benutzer in Ihrem Konto anhängen können, gelten speziell für Storage Gateway:

- AWSStorageGatewayReadOnlyAccess – Gewährt Lesezugriff auf AWS Storage Gateway-Ressourcen.
- AWSStorageGatewayFullAccess – Gewährt Vollzugriff auf AWS Storage Gateway-Ressourcen.

> **Note**
>
> Sie können diese Berechtigungsrichtlinien prüfen, indem Sie sich bei der IAM-Konsole anmelden und dort nach bestimmten Richtlinien suchen.

Sie können auch Ihre eigenen benutzerdefinierten IAM-Richtlinien erstellen, um Berechtigungen für AWS Storage Gateway-API-Aktionen zu gewähren. Die benutzerdefinierten Richtlinien können Sie dann den IAM-Benutzern oder -Gruppen zuweisen, die diese Berechtigungen benötigen.

Beispiele für vom Kunden verwaltete Richtlinien

In diesem Abschnitt finden Sie Beispiele für Benutzerrichtlinien, die Berechtigungen für diverse Storage Gateway-Aktionen gewähren. Diese Richtlinien sind nur wirksam, wenn SieAWSSDKs und dasAWS CLIaus. Bei Verwendung der Konsole müssen Sie zusätzliche konsolenspezifische Berechtigungen erteilen, die im Abschnitt Erforderliche Berechtigungen für die Verwendung der Storage Gateway erläutert werden.

> **Note**
>
> In allen Beispielen werden die Region USA West (Oregon) (`us-west-2`) und fiktive Konto-IDs verwendet.

Themen

Beispiel 1: Zulassen von Storage Gateway Gateway-Aktionen auf allen Gateways

Mit der folgenden Richtlinie können Benutzer alle Storage Gateway Gateway-Aktionen durchführen. Mit der Richtlinie können Benutzer außerdem Amazon EC2 EC2-Aktionen durchführen (DescribeSnapshotsundDeleteSnapshot) auf den Amazon EBS-Snapshots, die von Storage Gateway generiert wurden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllAWSStorageGatewayActions",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {You can use Windows ACLs only with file shares that are enabled for Active
 Directory.
            "Sid": "AllowsSpecifiedEC2Actions",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Beispiel 2: Zulassen schreibgeschützten Zugriff auf ein Gateway

Mit der folgenden Richtlinie können alle `List*`- und `Describe*`-Aktionen für alle Ressourcen durchgeführt werden. Beachten Sie, dass diese Aktionen schreibgeschützt sind. Somit lässt die Richtlinie nicht zu, dass der Benutzer den Status von Ressourcen ändert. Sie verhindert also, dass Benutzer Aktionen wie `DeleteGateway`, `ActivateGateway` und `ShutdownGateway` ausführen.

Die Richtlinie lässt außerdem die Amazon EC2-Aktion `DescribeSnapshots` zu. Weitere Informationen finden Sie unterDescribeSnapshotsimAmazon EC2 EC2-API-Referenzaus.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

In der obigen Richtlinie können Sie statt der Verwendung eines Platzhalterzeichens (*) den Umfang der von der Richtlinie betroffenen Ressourcen auf ein bestimmtes Gateway beschränken, wie im folgenden Beispiel gezeigt. Die Richtlinie lässt die Aktionen dann nur in dem spezifischen Gateway zu.

```
"Resource": [
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
```

```
            ]
```

Innerhalb eines Gateways können Sie den Umfang der Ressourcen auf nur Gateway-Volumes einschränken, wie in dem folgenden Beispiel gezeigt:

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/
*"
```

Beispiel 3: Zugriff auf ein bestimmtes Gateway gewähren

Die folgende Richtlinie lässt alle Aktionen auf einem spezifischen Gateway zu. Der Benutzerzugriff auf andere Gateways, die Sie möglicherweise bereitgestellt haben, ist eingeschränkt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
```

```
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

Die obige Richtlinie greift, wenn der Benutzer, dem die Richtlinie angefügt ist, entweder die API oder einAWSSDK für den Zugriff auf das Gateway. Wenn der Benutzer allerdings die Storage Gateway Gateway-Konsole verwenden, müssen Sie auch Berechtigungen erteilen, um den`ListGateways`-Aktion, wie im folgenden Beispiel gezeigt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Beispiel 4: Einem Benutzer den Zugriff auf ein bestimmtes Volume ermöglichen

Die folgende Richtlinie lässt zu, dass ein Benutzer alle Aktionen für ein spezifisches Volume auf einem Gateway durchführt. Da ein Benutzer standardmäßig keine Berechtigungen erhält, beschränkt die Richtlinie den Zugriff des Benutzers auf ein bestimmtes Volume.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Die obige Richtlinie greift, wenn der Benutzer, dem die Richtlinie angefügt ist, entweder die API oder einAWSSDK für den Zugriff auf das Volume. Wenn dieser Benutzer jedoch dieAWS Storage Gateway-Konsole müssen Sie auch Berechtigungen erteilen, um die`ListGateways`-Aktion, wie im folgenden Beispiel gezeigt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
```

```
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Beispiel 5: Alle Aktionen auf Gateways mit einem bestimmten Präfix zulassen

Mit der folgenden Richtlinie können Benutzer alle Storage Gateway Gateway-Aktionen für Gateways mit Namen durchführen, die mit beginnen`DeptX`aus. Die Richtlinie lässt außerdem das`DescribeSnapshots`Amazon EC2 EC2-Aktion, die zum Beschreiben von Snapshots erforderlich ist.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Die obige Richtlinie greift, wenn der Benutzer, dem die Richtlinie angefügt ist, entweder die API oder einAWSSDK für den Zugriff auf das Gateway. Wenn dieser Benutzer jedoch vorhat, dieAWS Storage Gateway-Konsole erteilen, müssen Sie zusätzliche Berechtigungen erteilen, wie in beschrieben.Beispiel 3: Zugriff auf ein bestimmtes Gateway gewährenaus.

Verwenden von Tags zur Steuerung des Zugriffs auf Ihr Gateway und Ihre -Ressourcen

Um den Zugriff auf Gateway-Ressourcen und -Aktionen zu steuern, können Sie AWS Identity and Access Management (IAM)-Richtlinien basierend auf Tags verwenden. Sie können die Steuerung auf zwei Arten bereitstellen:

1. Bestimmen des Zugriffs auf Gateway-Ressourcen basierend auf den Tags für diese Ressourcen
2. Bestimmen, welche Tags in einer IAM-Anfragebedingung weitergeleitet werden können

Informationen zur Bestimmung des Zugriffs mithilfe von Tags finden Sie unter Zugriffssteuerung mit Tags.

Zugriffssteuerung auf der Grundlage von Tags einer -Ressource

Zum Bestimmen, welche Aktionen ein Benutzer oder eine Rolle für eine Gateway-Ressource ausführen kann, können Sie Tags für die Gateway-Ressource verwenden. So können Sie beispielsweise bestimmte API-Operationen für eine File Gateway-Ressource basierend auf dem Schlüssel-Wert-Paar des Tags für die Ressource zulassen oder verweigern.

Das folgende Beispiel erlaubt es einem Benutzer oder einer Rolle, die Aktionnen `ListTagsForResource`, `ListFileShares` und `DescribeNFSFileShares` für alle Ressourcen auszuführen. Die Richtlinie gilt nur, wenn der Schlüssel des Tags in der Ressource auf `allowListAndDescribe` und der Wert auf `yes` festgelegt ist.

```
{
  "Version": "2012-10-17",
   "Statement": [
      {
          "Effect": "Allow",
                    "Action": [
                        "storagegateway:ListTagsForResource",
                        "storagegateway:ListFileShares",
                        "storagegateway:DescribeNFSFileShares"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/allowListAndDescribe": "yes"
                        }
```

```
                    }
      },
      {
          "Effect": "Allow",
          "Action": [
              "storagegateway:*"
          ],
          "Resource": "arn:aws:storagegateway:region:account-id:*/*"
      }
  ]
}
```

Zugriffssteuerung auf der Grundlage von Tags in einer IAM-Anfrage

Sie können anhand der Bedingungen in einer auf Tags basierenden IAM-Richtlinie bestimmen, welche Aktionen ein IAM-Benutzer für eine File Gateway-Ressource ausführen kann. Beispiel: Sie können eine Richtlinie schreiben, die einem IAM-Benutzer die Ausführung bestimmter API-Operationen basierend auf dem von ihm beim Erstellen der Ressource bereitgestellten Tag erlaubt oder verweigert.

Im folgenden Beispiel ermöglicht die erste Anweisung einem Benutzer das Erstellen eines Gateways nur dann, wenn das Schlüssel-Wert-Paar des beim Erstellen des angegebenen Gateways von ihm bereitgestellten Tags **`Department`** und **`Finance`** lautet. Wenn Sie die API-Operation verwenden, fügen Sie dieses Tag der Aktivierungsanforderung hinzu.

Die zweite Anweisung erlaubt dem Benutzer nur dann das Erstellen einer NFS- (Network File Systems) oder SMB-Dateifreigabe (Server Message Block) in einem Gateway, wenn das Schlüssel-Wert-Paar des Tags auf dem Gateway mit übereinstimmt**`Department`**und**`Finance`**aus. Zudem muss der Benutzer ein Tag zur Dateifreigabe hinzufügen, und das Schlüssel-Wert-Paar des Tags muss **`Department`** und **`Finance`** lauten. Tags werden einer Dateifreigabe bei deren Erstellung hinzugefügt. Es gibt keine Berechtigungen für die `AddTagsToResource`- oder `RemoveTagsFromResource`-Operationen, d. h., der Benutzer kann diese Operationen nicht auf dem Gateway oder der Dateifreigabe ausführen.

```
{
   "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"
            }
         }
      }
   ]
}
```

Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe

Amazon S3 File Gateway unterstützt zwei verschiedene Methoden zum Steuern des Zugriffs auf Dateien und Verzeichnisse, die über eine SMB-Dateifreigabe gespeichert werden: POSIX-Berechtigungen oder Windows-ACLs.

In diesem Abschnitt finden Sie Informationen zur Verwendung von Microsoft Windows-Zugriffskontrolllisten (Access Control Lists, ACLs) auf SMB-Dateifreigaben, die mit Microsoft Active Directory (AD) aktiviert sind. Durch die Verwendung von Windows-ACLs können Sie fein abgestimmte Berechtigungen für Dateien und Ordner in Ihrer SMB-Dateifreigabe festlegen.

Im Folgenden finden Sie einige wichtige Merkmale von Windows-ACLs auf SMB-Dateifreigaben:

- Windows-ACLs sind standardmäßig für SMB-Dateifreigaben ausgewählt, wenn Ihr File Gateway einer Active Directory-Domäne zugeordnet ist.

- Wenn ACLs aktiviert sind, sind die ACL-Informationen in Amazon S3 S3-Objektmetadaten persistent.
- Die Gateway bewahrt bis zu 10 ACLs pro Datei oder Ordner auf.
- Wenn Sie eine mit ACLs aktivierte SMB-Dateifreigabe für den Zugriff auf S3-Objekte verwenden, die außerhalb Ihres Gateways erstellt wurden, erben die Objekte die Informationen der ACLs aus dem übergeordneten Ordner.
- Die Standard-Stamm-ACL für eine SMB-Dateifreigabe bietet allen vollständigen Zugriff, Sie können die Berechtigungen der Stamm-ACL aber ändern. Sie können Root-ACLs zum Steuern des Zugriffs auf die Dateifreigabe verwenden. Sie können festlegen, wer die Dateifreigabe mounten (das Laufwerk zuordnen) kann und welche Berechtigungen der Benutzer rekursiv für die Dateien und Ordner in der Dateifreigabe erhält. Wir empfehlen jedoch, dass Sie diese Berechtigung im Ordner der obersten Ebene im S3-Bucket festlegen, sodass Ihre ACL dauerhaft gespeichert wird.

Sie können Windows-ACLs mithilfe der API-Operation CreateSMBFileShare beim Erstellen einer neuen SMB-Dateifreigabe aktivieren. Oder Sie können Windows-ACLs mithilfe der API-Operation UpdateSMBFileShare auf einer vorhandenen SMB-Dateifreigabe aktivieren.

Aktivieren von Windows-ACLs auf einer neuen SMB-Dateifreigabe

Führen Sie die folgenden Schritte aus, um Windows-ACLs auf einer neuen SMB-Dateifreigabe zu aktivieren.

So aktivieren Sie Windows-ACLs beim Erstellen einer neuen SMB-Dateifreigabe

1. Erstellen Sie ein File Gateway, sofern noch nicht geschehen. Weitere Informationen finden Sie unter .
2. Wenn das Gateway keiner Domäne beigetreten ist, fügen Sie es einer Domäne hinzu. Weitere Informationen finden Sie unter .
3. Erstellen Sie eine SMB-Dateifreigabe
4. Aktivieren Sie die Windows-ACL für die Dateifreigabe über die Storage Gateway Gateway-Konsole.

   Gehen Sie wie folgt vor, um die Storage Gateway Gateway-Konsole zu verwenden:

   a. Wählen Sie die Dateifreigabe aus und klicken Sie auf Edit file share (Dateifreigabe bearbeiten).

b. Wählen Sie für die Option File/directory access controlled by (Datei-/Verzeichniszugriff kontrolliert von) die Option Windows Access Control List (Windows-Zugriffskontrollliste) aus.

5. (Optional) Fügen Sie einen Admin-Benutzer zu AdminUsersList hinzu, wenn Sie möchten, dass der Admin-Benutzer zum Aktualisieren von ACLs für alle Dateien und Ordnern in der Dateifreigabe berechtigt ist.
6. Aktualisieren Sie die ACLs für die übergeordneten Ordner unter dem Stammverzeichnis. Hierzu konfigurieren Sie mithilfe von Windows-Explorer die ACLs in den Ordnern in der SMB-Dateifreigabe.

   > **Note**
   >
   > Wenn Sie die ACLs anstatt im übergeordneten Order unter dem Stammverzeichnis im Stammverzeichnis selbst konfigurieren, sind die ACL-Berechtigungen in Amazon S3 nicht persistent.

   Wir empfehlen Ihnen, ACLs im Ordner der obersten Ebene unter dem Stammverzeichnis Ihrer Dateifreigabe festzulegen, anstatt ACLs direkt im Stammverzeichnis der Dateifreigabe festzulegen. Bei diesem Ansatz sind die Informationen als Objekt-Metadaten in Amazon S3 persistent.
7. Aktivieren Sie die Vererbung entsprechend.

   > **Note**
   >
   > Die Vererbung kann für Dateifreigaben aktiviert werden, die nach dem 8. Mai 2019 erstellt wurden.

Wenn Sie die Vererbung aktivieren und die Berechtigungen rekursiv aktualisieren, aktualisiert Storage Gateway alle Objekte im S3-Bucket. Je nach der Anzahl der Objekte im Bucket kann die Aktualisierung einige Zeit in Anspruch nehmen.

Aktivieren von Windows-ACLs auf einer vorhandenen SMB-Dateifreigabe

Führen Sie die folgenden Schritte aus, um Windows-ACLs auf einer vorhandenen SMB-Dateifreigabe mit POSIX-Berechtigungen zu aktivieren.

So aktivieren Sie Windows-ACLs für eine vorhandene SMB-Dateifreigabe mithilfe der Storage Gateway Gateway-Konsole

1. Wählen Sie die Dateifreigabe aus und klicken Sie auf Edit file share (Dateifreigabe bearbeiten).
2. Wählen Sie für die Option File/directory access controlled by (Datei-/Verzeichniszugriff kontrolliert von) die Option Windows Access Control List (Windows-Zugriffskontrollliste) aus.
3. Aktivieren Sie die Vererbung entsprechend.

> **Note**
>
> Es wird nicht empfohlen, die ACLs auf der Stammebene festzulegen, da Sie die ACLs in diesem Fall erneut zurücksetzen müssen, wenn Sie das Gateway löschen.

Wenn Sie die Vererbung aktivieren und die Berechtigungen rekursiv aktualisieren, aktualisiert Storage Gateway alle Objekte im S3-Bucket. Je nach der Anzahl der Objekte im Bucket kann die Aktualisierung einige Zeit in Anspruch nehmen.

Einschränkungen bei der Verwendung von Windows-ACLs

Beachten Sie die folgenden Einschränkungen bei der Verwendung von Windows-ACLs zum Steuern des Zugriffs auf SMB-Dateifreigaben:

- Windows-ACLs werden nur auf Dateifreigaben unterstützt, die für Active Directory aktiviert sind, wenn Sie mit Windows-SMB-Clients auf die Dateifreigaben zugreifen.
- File Gateways unterstützt maximal 10 ACL-Einträge für die einzelnen Dateien und Ordner.
- Datei-Gateways unterstützen nicht`Audit`und`Alarm`Einträge, bei denen es sich um Einträge einer System-Zugriffskontrollliste (System Access Control List, File Gateways unterstützen `Allow`- und `Deny`-Einträge, bei denen es sich um Einträge einer besitzerverwalteten Zugriffskontrollliste (Discretionary Access Control List, DACL) handelt.
- Die Stamm-ACL-Einstellungen von SMB-Dateifreigaben befinden sich nur auf dem Gateway, und die Einstellungen sind über Gateway-Aktualisierungen und -Neustarts hinweg persistent.

> **Note**
>
> Wenn Sie die ACLs anstatt im übergeordneten Order unter dem Stammverzeichnis im Stammverzeichnis selbst konfigurieren, sind die ACL-Berechtigungen in Amazon S3 nicht persistent.

Stellen Sie angesichts dieser Bedingungen sicher, dass Sie die folgenden Schritte ausführen:

- Wenn Sie mehrere Gateways für den Zugriff auf denselben Amazon S3 S3-Bucket konfigurieren, konfigurieren Sie die Stamm-ACL auf jedem der Gateways, um die Berechtigungen konsistent zu halten.
- Wenn Sie eine Dateifreigabe löschen und sie auf demselben Amazon S3 S3-Bucket neu erstellen, stellen Sie sicher, dass Sie denselben Satz von Stamm-ACLs verwenden.

Speicher-Gateway-API-Berechtigungen: Referenz für Aktionen, Ressourcen und Bedingungsschlüssel

Wenn Sie die Zugriffskontrolle einrichten und Berechtigungsrichtlinien für eine IAM-Identität (identitätsbasierte Richtlinie) verfassen, können Sie die folgende Tabelle als Referenz verwenden. In der Tabelle werden alle Storage Gateway Gateway-API-Operationen sowie die zugehörigen Aktionen aufgeführt, für die Sie Berechtigungen zum Ausführen der -Aktion erteilen können, undAWS-Ressource, für die Sie die Berechtigungen erteilen können. Die Aktionen geben Sie im Feld `Action` und den Wert für die Ressource im Feld `Resource` der Richtlinie an.

Sie könnenAWS-weite Bedingungsschlüssel in Ihren Storage Gateway Gateway-Richtlinien, um Bedingungen auszudrücken. Eine vollständige Liste der AWS-weiten Schlüssel enthält der Abschnitt Verfügbare Schlüssel im IAM Benutzerhandbuch.

> **Note**
>
> Um eine Aktion anzugeben, verwenden Sie das Präfix `storagegateway:` gefolgt vom Namen der API-Operation (z. B. `storagegateway:ActivateGateway`). Für jede Storage Gateway Gateway-Aktion können Sie ein Platzhalterzeichen (*) als Ressource angeben.

Eine Liste der Storage Gateway Gateway-Ressourcen mit deren ARN-Format finden Sie unterStorage Gateway Gateway-Ressourcen und Operationenaus.

Die Storage Gateway Gateway-API und erforderlichen Berechtigungen für Aktionen lauten folgendermaßen.

ActivateGateway

Aktion(en): `storagegateway:ActivateGateway`

Ressource: *

AddCache

Aktion(en): `storagegateway:AddCache`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

AddTagsToResource

Aktion(en): `storagegateway:AddTagsToResource`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

oder

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

oder

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:tape/`*`tapebarcode`*

AddUploadBuffer

Aktion(en): `storagegateway:AddUploadBuffer`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

AddWorkingStorage

Aktion(en): `storagegateway:AddWorkingStorage`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

CancelArchival

Aktion(en): `storagegateway:CancelArchival`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:tape/`*`tapebarcode`*

CancelRetrieval

Aktion(en): `storagegateway:CancelRetrieval`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:tape/`*`tapebarcode`*

CreateCachediSCSIVolume

Aktion(en): `storagegateway:CreateCachediSCSIVolume`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

CreateSnapshot

Aktion(en): `storagegateway:CreateSnapshot`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

CreateSnapshotFromVolumeRecoveryPoint

Aktion(en): `storagegateway:CreateSnapshotFromVolumeRecoveryPoint`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

CreateStorediSCSIVolume

Aktion(en): `storagegateway:CreateStorediSCSIVolume`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

CreateTapes

Aktion(en): `storagegateway:CreateTapes`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteBandwidthRateLimit

Aktion(en): `storagegateway:DeleteBandwidthRateLimit`

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteChapCredentials

Aktion(en): storagegateway:DeleteChapCredentials

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DeleteGateway

Aktion(en): storagegateway:DeleteGateway

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteSnapshotSchedule

Aktion(en): storagegateway:DeleteSnapshotSchedule

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DeleteTape

Aktion(en): storagegateway:DeleteTape

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

Aktion(en): storagegateway:DeleteTapeArchive

Ressource: *

DeleteVolume

Aktion(en): storagegateway:DeleteVolume

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeBandwidthRateLimit

Aktion(en): storagegateway:DescribeBandwidthRateLimit

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCache

Aktion(en): `storagegateway:DescribeCache`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeCachediSCSIVolumes

Aktion(en): `storagegateway:DescribeCachediSCSIVolumes`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeChapCredentials

Aktion(en): `storagegateway:DescribeChapCredentials`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

DescribeGatewayInformation

Aktion(en): `storagegateway:DescribeGatewayInformation`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeMaintenanceStartTime

Aktion(en): `storagegateway:DescribeMaintenanceStartTime`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeSnapshotSchedule

Aktion(en): `storagegateway:DescribeSnapshotSchedule`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeStorediSCSIVolumes

Aktion(en): `storagegateway:DescribeStorediSCSIVolumes`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeTapeArchives

Aktion(en): `storagegateway:DescribeTapeArchives`

Ressource: *

DescribeTapeRecoveryPoints

Aktion(en): `storagegateway:DescribeTapeRecoveryPoints`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeTapes

Aktion(en): `storagegateway:DescribeTapes`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeUploadBuffer

Aktion(en): `storagegateway:DescribeUploadBuffer`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeVTLDevices

Aktion(en): `storagegateway:DescribeVTLDevices`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeWorkingStorage

Aktion(en): `storagegateway:DescribeWorkingStorage`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DisableGateway

Aktion(en): `storagegateway:DisableGateway`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListGateways

Aktion(en): `storagegateway:ListGateways`

Ressource: *

ListLocalDisks

Aktion(en): `storagegateway:ListLocalDisks`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListTagsForResource

Aktion(en): `storagegateway:ListTagsForResource`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

oder

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

oder

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:tape/`*`tapebarcode`*

ListTapes

Aktion(en): `storagegateway:ListTapes`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListVolumeInitiators

Aktion(en): `storagegateway:ListVolumeInitiators`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

ListVolumeRecoveryPoints

Aktion(en): `storagegateway:ListVolumeRecoveryPoints`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListVolumes

Aktion(en): `storagegateway:ListVolumes`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

RemoveTagsFromResource

Aktion(en): `storagegateway:RemoveTagsFromResource`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

oder

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

oder

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ResetCache

Aktion(en): `storagegateway:ResetCache`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

RetrieveTapeArchive

Aktion(en): `storagegateway:RetrieveTapeArchive`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

RetrieveTapeRecoveryPoint

Aktion(en): `storagegateway:RetrieveTapeRecoveryPoint`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ShutdownGateway

Aktion(en): `storagegateway:ShutdownGateway`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

StartGateway

Aktion(en): `storagegateway:StartGateway`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateBandwidthRateLimit

Aktion(en): `storagegateway:UpdateBandwidthRateLimit`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateChapCredentials

Aktion(en): `storagegateway:UpdateChapCredentials`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

UpdateGatewayInformation

Aktion(en): `storagegateway:UpdateGatewayInformation`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateGatewaySoftwareNow

Aktion(en): `storagegateway:UpdateGatewaySoftwareNow`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateMaintenanceStartTime

Aktion(en): `storagegateway:UpdateMaintenanceStartTime`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateSnapshotSchedule

Aktion(en): `storagegateway:UpdateSnapshotSchedule`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

UpdateVTLDeviceType

Aktion(en): `storagegateway:UpdateVTLDeviceType`

Ressource: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/device/`*`vtldevice`*

Verwandte Themen

- Zugriffskontrolle
- Beispiele für vom Kunden verwaltete Richtlinien

Verwenden von serviceverknüpften Rollen für Storage Gateway

Storage Gateway verwendetAWS Identity and Access Management(ICH)Serviceverknüpfte Rollenaus. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Storage Gateway verknüpft ist. Serviceverknüpfte Rollen werden von Storage Gateway vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer erfordertAWS-Services in Ihrem Namen.

Eine serviceverknüpfte Rolle vereinfacht die Einrichtung von Storage Gateway, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Storage Gateway definiert die Berechtigungen seiner serviceverknüpften Rollen und sofern nicht anders definiert, kann nur Storage Gateway die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die servicegebundene Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Servicegebundene Rolle angegeben ist. Wählen Sie über einen Link Yes (Ja) aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Storage Gateway

Storage Gateway verwendet die serviceverknüpfte Rolle namensawsServiceRoleforStorageGateway— awsServiceRoleforStorageGateway.

Die serviceverknüpfte Rolle AWSServiceRoleForStorageGateway vertraut, dass die folgenden Services die Rolle übernehmen:

- `storagegateway.amazonaws.com`

Die Rollenberechtigungsrichtlinie erlaubt Storage Gateway die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

- Aktion: `fsx:ListTagsForResource` für `arn:aws:fsx:*:*:backup/*`

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen und bearbeiten können. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Storage Gateway

Sie müssen eine servicegebundene Rolle nicht manuell erstellen. Wenn Sie ein Storage Gateway erstellen`AssociateFileSystem`API-Aufruf imAWS Management Console, derAWS CLIoder dasAWS-API, Storage Gateway erstellt die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Funktionen verwendet. Wenn Sie den Storage Gateway-Service vor dem 31. März 2021 verwendet haben, als er begann, serviceverknüpfte Rollen zu unterstützen, dann hat Storage Gateway die Rolle AWSServiceRoleForStorageGateway in Ihrem Konto erstellt. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie ein Storage Gateway erstellen`AssociateFileSystem`API-Aufruf erstellt Storage Gateway die serviceverknüpfte Rolle erneut für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit derawsServiceRoleforStorageGatewayAnwendungsfall. Erstellen Sie in der AWS CLI oder der AWS-API eine servicegebundene Rolle mit dem Servicenamen `storagegateway.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer servicegebundenen Rolle im IAM-Leitfaden. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für Storage Gateway

Mit Storage Gateway können Sie die serviceverknüpfte Rolle AWSServiceRoleForStorageGateway nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer servicegebundenen Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Storage Gateway

Storage Gateway löscht die Rolle AWSServiceRoleForStorageGateway nicht automatisch. Um die Rolle „awsServiceRoleforStorageGateway“ zu löschen, müssen Sie die`iam:DeleteSLR`API. Wenn keine Speicher-Gateway-Ressourcen vorhanden sind, die von der dienstverknüpften Rolle abhängen, ist das Löschen erfolgreich, andernfalls schlägt das Löschen fehl. Wenn Sie die dienstverknüpfte Rolle löschen möchten, müssen Sie IAM-APIs verwenden`iam:DeleteRole`oder`iam:DeleteServiceLinkedRole`aus. In diesem Fall müssen Sie die Storage Gateway Gateway-APIs verwenden, um zuerst Gateways oder Dateisystemzuordnungen im Konto zu löschen und dann die dienstverknüpfte Rolle mithilfe von`iam:DeleteRole`oder`iam:DeleteServiceLinkedRole`API. Wenn Sie die dienstverknüpfte Rolle mit IAM löschen, müssen Sie Storage Gateway verwenden`DisassociateFileSystemAssociation`API, um zuerst alle Dateisystemzuordnungen im Konto zu löschen. Andernfalls schlägt der Löschvorgang fehl.

> **Note**
>
> Wenn der Storage Gateway Gateway-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die von AWSServiceRoleForStorageGateway verwendeten Storage Gateway-Ressourcen

1. Verwenden Sie unsere Servicekonsole, CLI oder API, um einen Aufruf zu tätigen, der die Ressourcen bereinigt und die Rolle löscht, oder verwenden Sie die IAM-Konsole, CLI oder API zum Löschen. In diesem Fall müssen Sie Storage Gateway Gateway-APIs verwenden, um zuerst Gateways und Dateisystemzuordnungen im Konto zu löschen.
2. Wenn Sie die IAM-Konsole, -CLI oder API verwenden, löschen Sie die serviceverknüpfte Rolle mithilfe von IAM`DeleteRole`oder`DeleteServiceLinkedRole`API.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole,AWS CLIoder dasAWSAPI zum Löschen der serviceverknüpften Rolle AWSServiceRoleForStorageGateway. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für servicegebundene Storage Gateway Gateway-Rollen

Storage Gateway unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS-Service-Endpunkte.

Storage Gateway unterstützt die Verwendung von serviceverknüpften Rollen nicht in allen Regionen, in denen der Service verfügbar ist. Sie können die Rolle AWSServiceRoleForStorageGateway in den folgenden Regionen verwenden.

Name der Region	Regions-ID	Support im Storage Gateway
USA Ost (Nord-Virginia)	us-east-1	Yes (Ja)
USA Ost (Ohio)	us-east-2	Yes (Ja)
USA West (Nordkalifornien)	us-west-1	Yes (Ja)
USA West (Oregon)	us-west-2	Yes (Ja)
Asien-Pazifik (Mumbai)	ap-south-1	Yes (Ja)
Asien-Pazifik (Osaka)	ap-northeast-3	Yes (Ja)
Asien-Pazifik (Seoul)	ap-northeast-2	Yes (Ja)
Asien-Pazifik (Singapore)	ap-southeast-1	Yes (Ja)
Asien-Pazifik (Sydney)	ap-southeast-2	Yes (Ja)
Asien-Pazifik (Tokyo)	ap-northeast-1	Yes (Ja)
Kanada (Zentral)	ca-central-1	Yes (Ja)
Europa (Frankfurt)	eu-central-1	Yes (Ja)
Europa (Ireland)	eu-west-1	Yes (Ja)
Europa (London)	eu-west-2	Yes (Ja)
Europa (Paris)	eu-west-3	Yes (Ja)

Name der Region	Regions-ID	Support im Storage Gateway
Südamerika (São Paulo)	sa-east-1	Yes (Ja)
AWS GovCloud (US)	us-gov-west-2	Yes (Ja)

Protokollieren und Überwachen in AWS Storage Gateway

Storage Gateway ist integriert mitAWS CloudTrail, ein Service, der die Aktionen eines Benutzers, einer Rolle oder einesAWSDienst im Storage Gateway. CloudTrail erfasst alle API-Aufrufe für Storage Gateway als Ereignisse. Die erfassten Aufrufe umfassen Aufrufe von der Storage Gateway Gateway-Konsole und Code-Aufrufe der Storage Gateway Gateway-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Storage Gateway. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Anhand der von CloudTrail erfassten Informationen können Sie die an Storage Gateway gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Storage Gateway Gateway-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Wenn eine Aktivität in Storage Gateway auftritt, wird diese Aktivität zusammen mit anderen in einem CloudTrail-Ereignis aufgezeichnetAWSService-Ereignisse inEreignisverlauf deraus. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Für eine fortlaufende Aufzeichnung von Ereignissen in IhremAWSerstellen Sie einen Trail, einschließlich Ereignissen für Storage Gateway. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Pfads
- Siehe Von CloudTrail unterstützte Services und Integrationen.
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Storage Gateway Gateway-Aktionen werden protokolliert und in derAktionen-Thema. Zum Beispiel generieren Aufrufe der Aktionen `ActivateGateway`, `ListGateways` und `ShutdownGateway` Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde.
- Whether the request was made by another AWS service.

Weitere Informationen finden Sie unter dem CloudTrail userIdentity-Element.

Grundlagen zu den - Storage Gateway Gateway-

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket übermittelt werden. CloudTrail log files contain one or more log entries. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die Aktion demonstriert.

```
{ "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"
            }]
}
```

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die Aktion ListGateways demonstriert.

```
{
 "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"
             }]
}
```

Compliance-Validierung fürAWSStorage Gateway

Externe Auditoren bewerten die Sicherheit und Compliance vonAWSStorage Gateway als Teil von mehrerenAWSCompliance-Programme Dazu gehören SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR und HITRUST CSF.

Eine Liste der AWS-Services im Bereich bestimmter Compliance-Programme finden Sie unter AWS-Services im Bereich nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Compliance-Verantwortung bei Verwendung von Storage Gateway hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab.AWSstellt die folgenden Ressourcen bereit, um die Compliance zu unterstützen:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- Bewertung von Ressourcen mit Regeln im AWS Config Developer Guide - Das AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Ausfallsicherheit inAWSStorage Gateway

Im Zentrum der globalen AWS Infrastruktur stehen die AWS-Regionen und Availability Zones (Verfügbarkeitszonen, AZs). AWS -Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

Weitere Informationen über AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zu denAWSStorage Gateway globale -Infrastruktur bietet verschiedene Funktionen, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden.

- Verwenden Sie VMware vSphere High Availability (VMware HA), um Speicher-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen zu schützen. Weitere Informationen finden Sie unterVerwenden von VMware vSphere High Availability mit Storage Gatewayaus.
- Verwenden Sie AWS Backup zum Sichern Ihrer Volumes. Weitere Informationen finden Sie unterbenutzenAWS Backupum Ihre Volumes zu sichernaus.

- Klonen Sie Ihr Volume von einem Wiederherstellungspunkt aus. Weitere Informationen finden Sie unterKlonen eines Volumesaus.
- Archivieren Sie virtuelle Bänder in Amazon S3 Glacier. Weitere Informationen finden Sie unterArchivierung virtueller Bänderaus.

Sicherheit der Infrastruktur inAWSStorage Gateway

Als Managed ServiceAWSStorage Gateway ist durch dieAWSDie globalen Verfahren zur Netzwerksicherheit, die in derAmazon Web Services: Übersicht über SicherheitsprozesseWhitepaper.

Du benutztAWSveröffentlichte API-Aufrufe, um über das Netzwerk auf Storage Gateway zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Bewährte Sicherheitsmethoden für Storage Gateway

AWSStorage Gateway bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen. Weitere Informationen finden Sie unterAWSBewährte Methoden für die Sicherheitaus.

Fehlerbehebung bei Ihrem Gateway

In den folgenden Abschnitten erhalten Sie Informationen zur Fehlerbehebung bei Problemen im Zusammenhang mit Gateways, Dateifreigaben, Volumes, virtuellen Bändern und Snapshots. Die lokalen Gateway Informationen zur Fehlerbehebung decken Gateways ab, die sowohl auf der VMware ESXi als auch auf den Microsoft Hyper-V Clients bereitgestellt sind. Die Informationen zur Fehlerbehebung für Dateifreigaben gelten für den Amazon S3 File Gateway-Typ. Die Informationen zur Fehlerbehebung für Volumes gelten für den Volume Gateway-Typ. Die Informationen zur Fehlerbehebung für Bänder gelten für den Typ Tape-Gateway. Die Informationen zur Fehlerbehebung für Gateway-Probleme gelten für die Verwendung von CloudWatch-Metriken. Die Informationen zur Fehlerbehebung für Probleme im Zusammenhang mit hoher Verfügbarkeit beziehen sich auf Gateways, die auf der VMware vSphere High Availability(HA)-Plattform ausgeführt werden.

Themen

Behebung von Fehlern bei lokalen Gateway

Im Folgenden werden Informationen über typische Probleme beschrieben, die bei der Arbeit mit Ihren lokalen Gateways auftreten können, und wie Sie diese aktivieren könnenSupportUm bei der Fehlerbehebung bei Ihrem Gateway zu helfen.

Die folgende Tabelle listet typische Probleme auf, die möglicherweise im Umgang mit Ihren lokalen Gateways auftreten.

Problem	Maßnahme
Sie können die IP-Adress e Ihrer Gateway nicht ermitteln.	Verwenden Sie den Hypervisor-Client zum Herstellen einer Verbindung mit Ihrem Host, um die Gateway-IP-Adresse zu ermitteln. • Für die VMware ESXi kann die IP-Adresse der VM im vSphere-Client auf der Registerkarte Summary (Übersicht) gefunden werden. • Für Microsoft Hyper-V, kann die IP-Adresse der VM's gefunden werden, indem man sich auf der lokalen Konsole anmeldet. Wenn Sie immer noch Probleme haben die Gateway-IP-Adresse zu ermitteln: • Stellen Sie sicher, dass der VM aktiviert ist. Nur wenn die VM aktiviert ist, wird dem Gateway eine IP-Adresse zugewiesen. • Warten Sie bis die VM den Startup abgeschlossen hat. Wenn Sie Ihre VM gerade erst aktiviert haben, kann es einige Minuten dauern, bis die Gateways mit der Boot-Sequenz abschließen.
Sie haben Netzwerk- oder Firewall-Probleme.	• Erteilen Sie dem Gateway die Zugriffserlaubnis für die entsprech enden Ports. • Wenn Sie eine Firewall oder einen Router verwenden, um den Netzwerkverkehr zu filtern oder zu begrenzen, müssen Sie Ihre Firewall und Ihren Router so konfigurieren, dass diese Service-Endpunkte für die ausgehende Kommunikation zuAWSaus. Weitere Informationen zum Netzwerk und Firewall-Anforderungen finden Sie unter Netzwerk- und Firewall-Anforderungen.
Die Gateway Aktivieru ng schlägt fehl, wenn Sie aufFahren Sie mit Aktivieru ng fortin der Storage Gateway Management Console.	• Überprüfen Sie, dass auf die Gateway-VM zugegriffen werden kann, indem Sie die VM Ihres Clients anpingen. • Stellen Sie sicher, dass Ihre VM eine Netzwerkverbindung zum Internet hat. Andernfalls müssen Sie die Konfiguration eines SOCKS-Proxy vornehmen. Weitere Informationen zur Verfahren

Problem	Maßnahme
	sweise finden Sie unter Testen der Netzwerkkonnektivität Ihres Gateways. • Stellen Sie sicher, dass die Uhrzeit des Hosts richtig eingestellt ist, dass der Host so konfiguriert ist, dass er die Uhrzeit automatis ch mit einem Network Time Protocol (NTP) Server synchroni siert und dass die Gateway-VM auf die richtige Uhrzeit eingestel lt ist. Weitere Informationen zum Synchronisieren der Uhrzeit des Hypervisor-Hosts und der VMs finden Sie unter Konfigurieren eines Network Time Protocol (NTP) -Servers für Ihr Gateway. • Nachdem Sie diese Schritte befolgt haben, können Sie die Bereitstellung des Gateways wiederholen, indem sie die Storage Gateway Gateway-Konsole und dieGateway einrichten und aktivieren. Assistenten • Stellen Sie sicher, dass Ihre VM über mindestens 7,5 GB RAM verfügen. Die Gateway-Zuweisung schlägt fehl, wenn es weniger als 7,5 GB RAM zur Verfügung stehen. Weitere Informationen finden Sie unter Setup-Anforderungen für das File.
Entfernen Sie eine als Upload-Pufferspeicher zugewiesene Festplatte. Beispielsweise möchten Sie die Anzahl der Upload-Pufferspeicher für ein Gateway reduzieren oder eine Festplatte ersetzen, die als fehlgeschlagener Puffer verwendet wurde.	

Problem	Maßnahme
Sie müssen die Bandbreite zwischen Ihrem Gateway und verbessernAWSaus.	Sie können die Bandbreite Ihres Gateways zu AWS verbessern, indem Sie Ihre Internetverbindung zu AWS auf einem anderen Netzwerkadapter (NIC) als dem zum Herstellen der Verbindung zwischen Ihren Anwendungen und der Gateway-VM einrichten. Diese Strategie ist nützlich, wenn Sie eine hohe Bandbreitenverbindung zu AWS besitzen und Sie Konflikte mit der Bandbreite vermeiden möchten, insbesondere während der Wiederherstellung eines Snapshots. Für Workload-Anforderungen mit hohem Durchsatz können SieAWS Direct ConnectSo stellen Sie eine dedizierte Netzwerkverbindung zwischen Ihrem lokalen Gateway her undAWSaus. Um die Bandbreite der Verbindung vom Gateway zu AWS zu messen, verwenden Sie die Metriken `CloudBytesDownloaded` und `CloudBytesUploaded` des Gateways. Weitere Informationen zu diesem Thema finden Sie unter Leistung. Indem Sie Ihre Internetverbindung verbessern, stellen Sie sicher, dass Ihr Upload-Puffer nicht aufgefüllt wird.

Problem	Maßnahme

Durchsatz zu oder von Ihrem Gateway sinkt auf Null.	• Auf derGatewayStellen Sie sicher, dass in der Storage Gateway Gateway-Konsole, die IP-Adressen für Ihre Gateway-VM identisch mit Ihrer Hypervisor-Client-Software (VMware vSphere Client oder Microsoft Hyper-V Manager) sind. Wenn Sie eine Nichtübereinstimmung finden, starten Sie das Gateway über die Storage Gateway Gateway-Konsole neu, wie unter gezeigtHerunterfahren Ihrer Gateway-VMaus. Nach dem Neustart werden die Adressen imIP-AdressenListe in den Storage Gateway Gateway-KonsolenGatewayDie Registerkarte sollte mit den IP-Adressen Ihres Gateways übereinstimmen, die Sie vom Hypervisor-Client bestimmen.
	  • Für die VMware ESXi kann die IP-Adresse der VM im vSphere-Client auf der Registerkarte Summary (Übersicht) gefunden werden.
	  • Für Microsoft Hyper-V, kann die IP-Adresse der VM's gefunden werden, indem man sich auf der lokalen Konsole anmeldet.
	• Prüfen Sie Ihre Gateway-Konnektivität zu AWS, wie in Testen der Netzwerkkonnektivität Ihres Gateways beschrieben.
	• Prüfen Sie die Netzwerkadapter Konfiguration des Gateways und stellen Sie sicher, dass alle Schnittstellen, die Sie für das Gateway aktiviert haben möchten, aktiviert sind. Um die Netzwerkadapter Konfiguration Ihres Gateways anzuzeigen, befolgen Sie die Anweisungen in Konfigurieren von Netzwerkadaptern für Ihr Gateway und wählen Sie die Option die die Netzwerkkonfiguration Ihres Gateway anzeigt.
	
	Sie können den Durchsatz zu und von Ihrem Gateway über die Amazon CloudWatch CloudWatch-Konsole betrachten. Weitere Informationen zur Messung des Durchsatzes zu und von Ihrem Gateway zu AWS finden Sie unter Leistung.

Problem	Maßnahme
Sie haben Schwierig keiten mit dem Importieren (Bereitstellen) des Storage Gateway auf Microsoft Hyper-V.	Weitere Informationen finden Sie unter Fehlerbehebung bei Microsoft Hyper-V-Setup, in dem einige der gängigen Themen der Bereitstellung einer Gateway auf Microsoft Hyper-V diskutiert werden.
Sie erhalten eine Nachricht mit der Aufschrift: „Die Daten, die auf das Volume in Ihrem Gateway geschrieben wurden, werden nicht sicher unter gespeichertAWS„.	Sie erhalten diese Meldung, wenn Ihre Gateway-VM aus einem Klon oder Snapshot eine andere Gateway-VM erstellt wurde. Wenn dies nicht der Fall ist, wenden Sie sich anSupportaus.

Aktivieren vonSupportum bei der Fehlerbehebung Ihres lokal gehosteten Gateways zu helfen

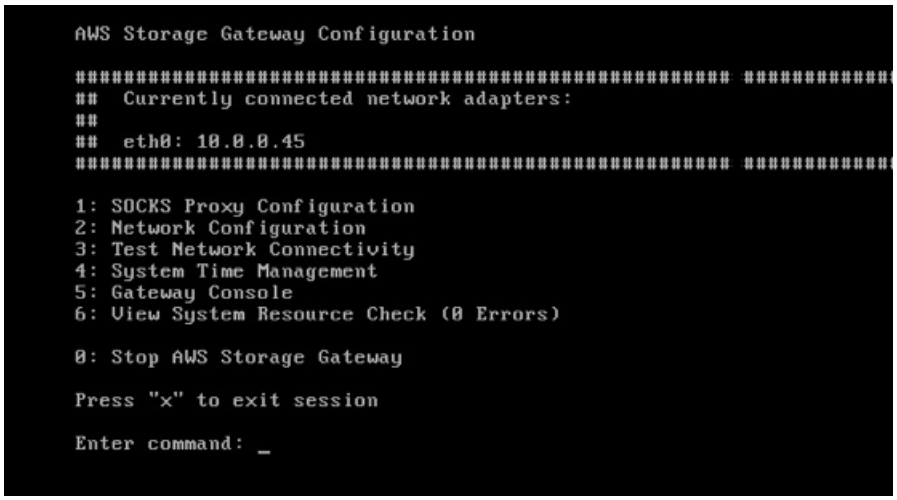
Storage Gateway bietet eine lokale Konsole, die Sie verwenden können, um mehrere Wartungsaufgaben durchzuführen, einschließlich der AktivierungSupportUm auf Ihr Gateway zuzugreifen und Ihnen bei der Lösung von Gateway-Problemen zu helfen. Der Standardwert fürSupportDer Zugriff auf Ihr Gateway ist deaktiviert. Dieser Zugriff wird über die lokale Host-Konsole aktiviert. So geben SieSupportWenn Sie auf Ihr Gateway zugreifen, melden Sie sich zuerst bei der lokalen Konsole für den Host an, navigieren Sie zu der Speicher-Gateway-Konsole und stellen sie dann eine Verbindung mit dem Support-Server her.

So aktivieren SieSupportZugriff auf Ihr Gateway

1. Melden Sie sich bei der lokalen Konsole Ihres Hosts an.

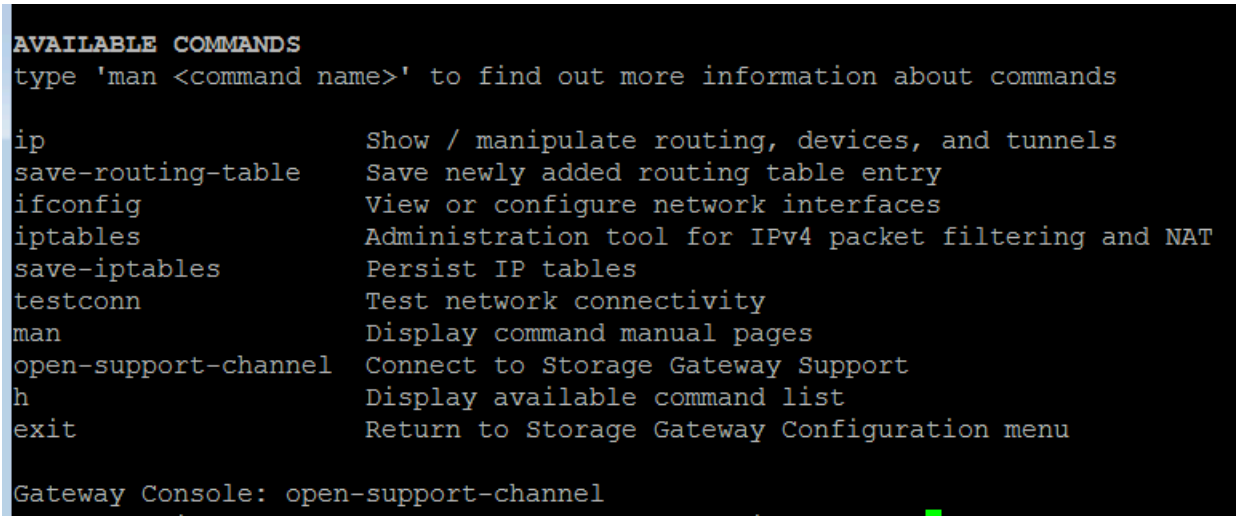
   - VMware ESXi — Weitere Informationen finden Sie unterZugreifen auf die lokale Konsole mit VMware ESXiaus.
   - Microsoft Hyper-V — Weitere Informationen finden Sie unterZugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-Vaus.

Die lokale Konsole sieht aus wie folgt.



2. Geben Sie an der -Eingabeauff**5**So öffnen SieSupportChannel-Konsole.
3. Geben Sie **h** ein, um das Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) zu öffnen.
4. Gehen Sie folgendermaßen vor:

   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, finden Sie imVERFÜGBARE BEFEHLE, geben Sie ein**`open-support-channel`**um eine Verbindung zum Kundensupport für Storage Gateway herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal öffnen könnenAWSaus. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.
   - Wenn Ihr Gateway einen VPC-Endpunkt verwendet, geben Sie im Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) **`open-support-channel`** ein. Wenn Ihr Gateway nicht aktiviert ist, geben Sie den VPC-Endpunkt oder die IP-Adresse ein, um eine Verbindung mit dem Kundenservice für Storage Gateway herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal öffnen könnenAWSaus. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.

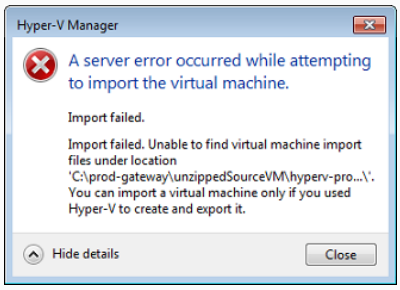
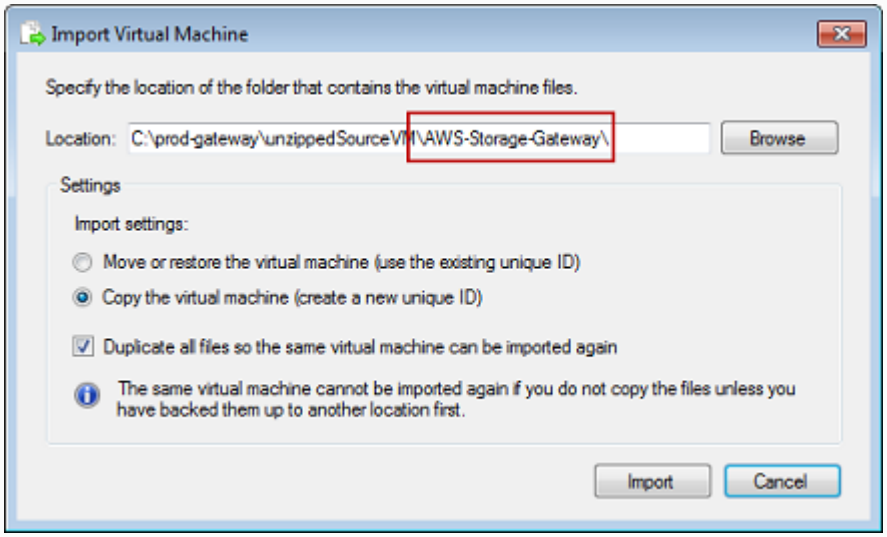


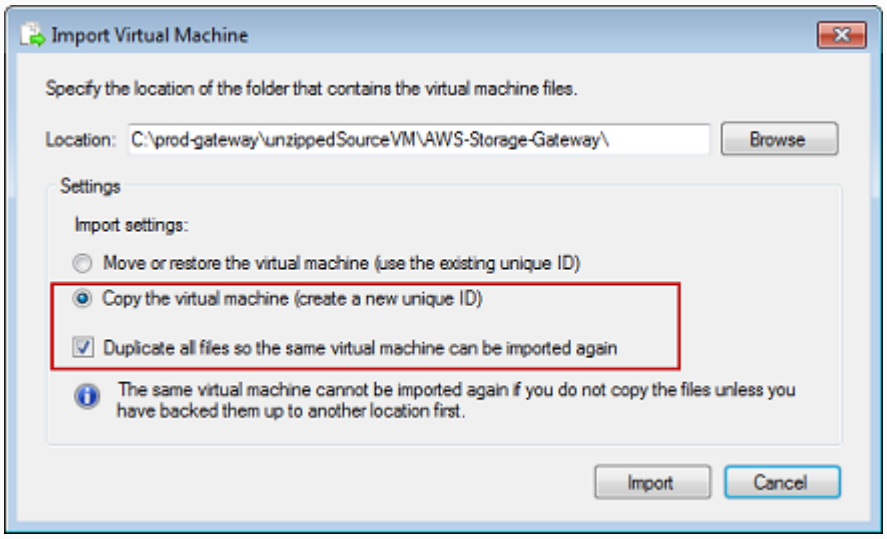
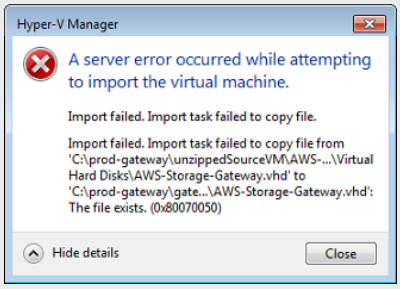
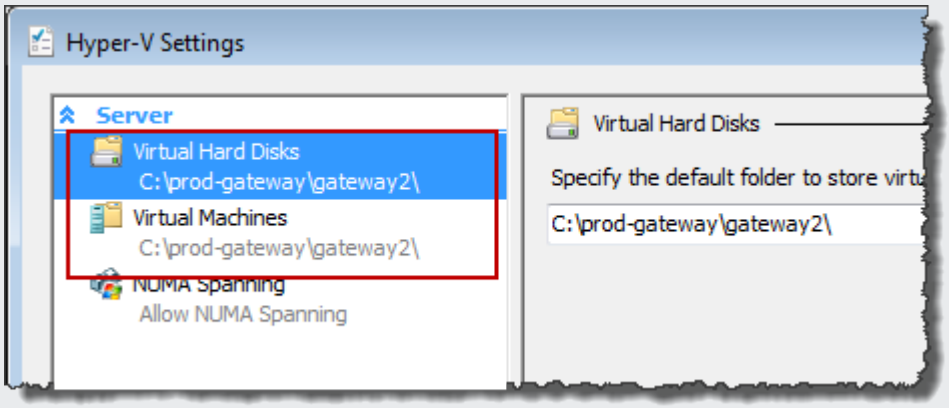
> **Note**
>
> Die Kanalnummer ist keine Transmission Control Protocol/User Datagram Protocol (TCP/UDP) Portnummer. Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP-22) Verbindung zu den Storage Gateway Gateway-Servern her und schafft den Support-Kanal für die Verbindung.

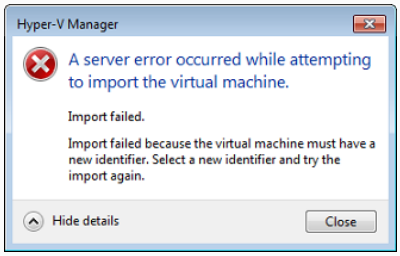
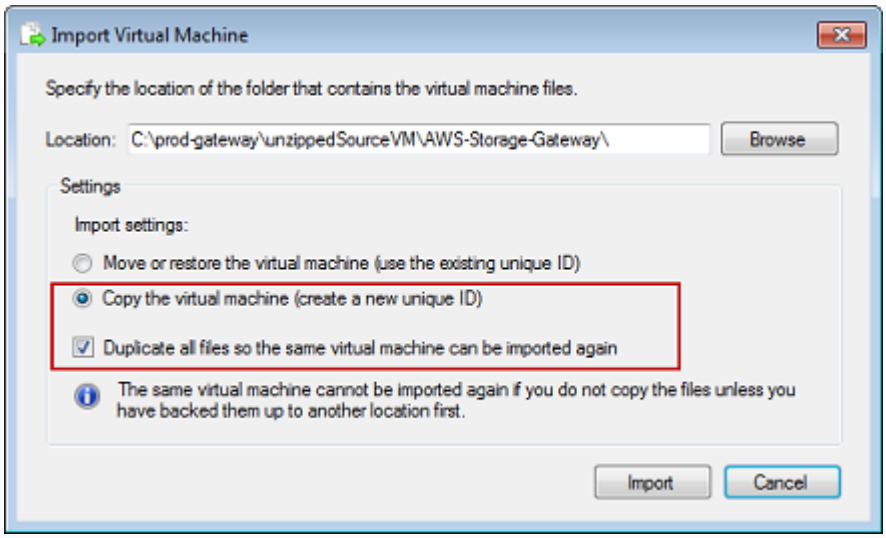
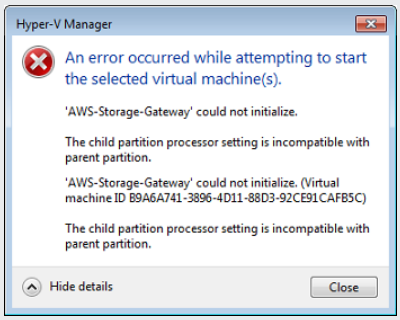
5. Wenn der Support-Kanal hergestellt wurde, geben Sie Ihre Support-Service-Nummer anSupportsoSupportkann Unterstützung bei der Fehlerbehebung leisten.
6. Wenn die Supportsitzung beendet ist, geben Sie **q** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn der Amazon Web Services Support Sie darüber informiert, dass die Supportsitzung abgeschlossen ist.
7. Geben Sie ein.**exit**um sich von der Storage Gateway -Konsole abzumelden.
8. Folgen Sie den Eingabeaufforderungen, um die lokale Konsole zu beenden.

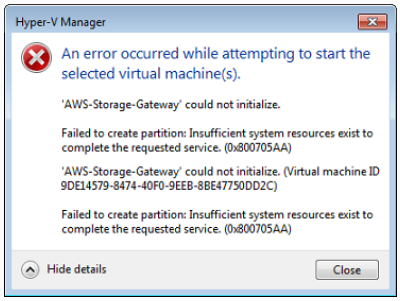
Fehlerbehebung bei Microsoft Hyper-V-Setup

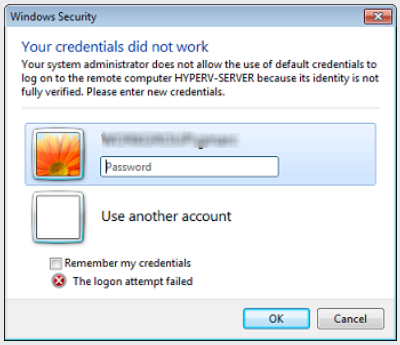
Die folgende Tabelle listet typische Probleme auf, die beim Bereitstellen von Storage Gateway auf die Microsoft Hyper-V Plattform auftreten können.

Problem	Maßnahme
Sie versuchen, ein Gateway zu importieren und erhalten die Fehlermeldung: „Der Import fehlgeschlagen. Die Import-Datei der Virtuellen Maschine wird unter Standort nicht gefunden...". 	Dieser Fehler kann aus folgenden Gründen auftreten: • Wenn Sie nicht auf das Stammverzeichnis der entpackten Gateway-Quell-Dateien zeigen. Der letzte Teil des angegebenen Speicherorts im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) sollte `AWS-Storage-Gateway` lauten, wie im folgenden Beispiel dargestellt:  • Wenn Sie bereits ein Gateway bereitgestellt haben, die Option Copy the virtual machine (virtuelle Maschine kopieren) nicht ausgewählt ist und Sie die Option Duplicate all files (Alle Dateien duplizieren) im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) markiert haben, dann wurde die VM an dem Speicherort erstellt, an dem Sie die Dateien entpackt haben, und Sie können nicht erneut von dort importieren. Zur Behebung dieses Problems, erwerben Sie eine neue Kopie der entpackten Gateway Quell-Dateien und kopieren Sie diese an einen neuen Speicherort. Verwenden Sie den neuen Speicherort als Importquelle. Das folgende Beispiel zeigt die Optionen, die Sie überprüfen müssen, wenn Sie aus einem entpackten Quelldateien-Speicherort mehrere Gateways erstellen möchten.

Problem	Maßnahme
	
Sie versuchen, ein Gateway zu importier en und erhalten die Fehlermeldung: „Der Import fehlgeschlagen. Import Aufgabe zur Kopie der Datei fehlgeschlagen. 	Wenn Sie bereits ein Gateway bereitgestellt haben und Sie versuchen den Standard-Ordner wiederzuverwenden, der die virtuelle Festplatten Dateien und die virtuelle Maschinen-Konfigur ationsdateien speichert, wird dieser Fehler auftreten. Zur Behebung dieses Problems geben Sie neue Speicherorte im Dialogfeld Hyper-V Settings (Hyper-V-Einstellungen) an. 

Problem	Maßnahme
Sie versuchen, ein Gateway zu importier en und erhalten eine Fehlermeldung: „Der Import fehlgeschlagen. Der Import ist fehlgeschlagen, da die virtuelle Maschine über eine neue ID verfügen muss. Wählen Sie eine ID und versuchen Sie erneut zu importieren." 	Wenn Sie das Gateway importieren, stellen Sie sicher, dass Sie die Option Copy the virtual maschine (Virtuelle Maschine kopieren) und die Option Duplicate all files (Alle Dateien duplizieren) im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) auswählen , um eine neue eindeutige ID für die VM zu erstellen. Das folgende Beispiel zeigt die Optionen im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren), die Sie verwenden sollten. 
Sie versuchen, eine Gateway-VM zu starten und erhalten die Fehlermel dung erhalten: "Die untergeordnete Partitions-Prozessor-Einstellung ist nicht kompatibel mit der übergeordneten Partition." 	Dieser Fehler wird wahrscheinlich durch eine CPU-Abweichungen zwischen den erforderlichen CPUs für das Gateway und den verfügbaren CPUs auf dem Host verursacht. Stellen Sie sicher, dass die VM-CPU-Inventur von der zugrunde liegenden Hypervisor unterstützt wird. Weitere Informationen zu den Anforderungen von Storage Gateway; finden Sie unterSetup-Anforderungen für das Fileaus.

Problem	Maßnahme
Sie versuchen, eine Gateway-VM zu starten und erhalten die Fehlermeldung: „Fehler beim Erstellen der Partition: Es gibt unzureichende Ressourcen, um den angeforderten Service abzuschließen.“ 	Dieser Fehler wird wahrscheinlich durch eine RAM-Abweichungen zwischen dem erforderlichen RAM für das Gateway und den verfügbaren RAM auf dem Host verursacht. Weitere Informationen zu den Anforderungen von Storage Gateway; finden Sie unterSetup-Anforderungen für das Fileaus.
Ihre Snapshots und Gateway-Software-Aktualisierungen treten zu geringfügig anderen Zeiten als erwartet auf.	Die Uhr der Gateway-VM, weicht möglicherweise von der tatsächlichen Uhrzeit ab, dies wird als Ganggenauigkeit bezeichnet. Überprüfen und korrigieren Sie die Uhrzeit der VM, indem Sie die Option Synchronisierung der lokalen Gateway-Konsole verwenden. Weitere Informationen finden Sie unter Konfigurieren eines Network Time Protocol (NTP) -Servers für Ihr Gateway.
Sie müssen die entpackten Microsoft Hyper-V Storage Gateway Gateway-Dateien auf das Host-Dateisystem legen.	Greifen Sie auf den Host zu wie Sie auf einen typischen Microsoft Windows Server zugreifen würden. Zum Beispiel: Wenn der Hypervisor Host-Name `hyperv-server` lautet, dann können Sie den folgenden UNC-Pfad wählen `\\hyperv-server\c$` , dieser geht davon aus, dass der Name `hyperv-server` in Ihrer lokalen Host-Datei aufgelöst oder definiert werden kann.

Problem	Maßnahme
Sie werden aufgefordert Anmeldeinformationen anzugeben, wenn Sie eine Verbindung zum Hypervisor herstellen. 	Fügen Sie Ihre Benutzer-Anmeldeinformationen als lokaler Administrator für den Hypervisor-Host mithilfe des Sconfig.cmd Tool hinzu.

Beheben von Problemen mit Amazon EC2 Gateway

In den folgenden Abschnitten werden typische Probleme beschrieben, die bei der Arbeit mit dem Gateway auftreten können, das auf Amazon EC2 bereitgestellt wird. Weitere Informationen zum Unterschied zwischen einem lokalen Gateway und einem Gateway, das in Amazon EC2 bereitgestellt ist, finden Sie unterBereitstellen eines File Gateways auf einem Amazon EC2 EC2-Hostaus.

Weitere Informationen zur Verwendung des flüchtigen Speichers finden Sie unter Verwenden von kurzlebigem Speicher mit EC2-Gateways.

Themen

- Ihre Gateway-Aktivierung ist nach ein paar Augenblicken nicht mehr aufgetreten
- Sie können Ihre EC2-Gateway-Instance in der Instance-Liste nicht finden
- Du willstSupportum bei der Fehlerbehebung bei Ihrem EC2-Gateway zu helfen

Ihre Gateway-Aktivierung ist nach ein paar Augenblicken nicht mehr aufgetreten

Überprüfen Sie in der Amazon EC2 EC2-Konsole Folgendes:

- Port 80 ist in der Sicherheitsgruppe aktiviert, die Sie mit der Instance verknüpft haben. Weitere Informationen zum Hinzufügen einer Sicherheitsgruppenregel finden Sie unterHinzufügen einer Sicherheitsgruppenregelim Amazon EC2-Benutzerhandbuch für Linux-Instancesaus.
- Die Gateway-Instance ist als laufend markiert. In der Amazon EC2 EC2-Konsole wirdBundesstaatDer Wert für die Instance sollte RUNNING sein.
- Stellen Sie sicher, dass der Amazon EC2 EC2-Instance-Typ die unter beschriebenen Mindestanforderungen erfülltSpeicheranforderungenaus.

Versuchen Sie erneut, das Gateway zu aktivieren, nachdem Sie das Problem behoben haben. Öffnen Sie dazu die Storage Gateway -Konsole und wählen SieStellen Sie ein neues Gateway auf Amazon EC2 bereit, und geben Sie die IP-Adresse der -Instance erneut ein.

Sie können Ihre EC2-Gateway-Instance in der Instance-Liste nicht finden

Wenn Sie die Instance nicht mit einem Ressourcen-Tag versehen haben und viele Instances ausführt werden, ist es schwierig, die von Ihnen gestarteten Instances zu benennen. In diesem Fall können Sie die folgenden Aktionen ausführen, um die Gateway Instance zu finden:

- Prüfen Sie den Namen des Amazon Machine Image (AMI) auf der Registerkarte Description (Beschreibung) der Instance. Eine Instance basierend auf der Storage Gateway Gateway-AMI sollte mit dem Text beginnen**`aws-storage-gateway-ami`**aus.
- Wenn Sie mehrere Instanzen basierend auf Storage Gateway AMI haben, prüfen Sie die Startzeit der Instance um die richtige Instance zu finden.

Du willstSupportum bei der Fehlerbehebung bei Ihrem EC2-Gateway zu helfen

Storage Gateway bietet eine lokale Konsole, die Sie verwenden können, um mehrere Wartungsaufgaben durchzuführen, einschließlich der AktivierungSupportUm auf Ihr Gateway zuzugreifen und Ihnen bei der Lösung von Gateway-Problemen zu helfen. Der Standardwert fürSupportDer Zugriff auf Ihr Gateway ist deaktiviert. Sie aktivieren diesen Zugriff über die lokale Amazon EC2 EC2-Konsole. Sie melden sich bei der lokalen Amazon EC2 EC2-Konsole über Secure Shell (SSH) an. Für eine erfolgreiche Anmeldung über SSH, muss die Sicherheitsgruppe Ihrer Instance über eine Regel verfügen, die den TCP-Port 22 öffnet.

> **Note**
>
> Wenn Sie eine neue Regel zu einer vorhandenen Sicherheitsgruppe hinzufügen, gilt die neue Regel für alle Instances, die diese Sicherheitsgruppe nutzen. Weitere Informationen zu Sicherheitsgruppen und zum Hinzufügen einer Sicherheitsgruppenregel finden Sie unterAmazon EC2-SicherheitsgruppenimBenutzerhandbuch für Amazon EC2aus.

So lassen Sie denSupportStellen Sie eine Verbindung mit Ihrem Gateway her, melden Sie sich zuerst bei der lokalen Konsole für die Amazon EC2 EC2-Instance an, navigieren Sie zu der Speicher-Gateway-Konsole und gewähren Sie dann den Zugriff.

So aktivieren SieSupportZugriff auf ein Gateway, das auf einer Amazon EC2 EC2-Instance bereitgestellt wird

1. Melden Sie sich bei der lokalen Konsole für Ihre Amazon EC2 EC2-Instance an. Weitere Informationen finden Sie unterVerbinden Sie sich mit der InstanceimBenutzerhandbuch für Amazon EC2aus.

   Sie können den folgenden Befehl verwenden, um sich bei der lokalen EC2-Konsole der Instance anzumelden.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > Die*PRIVATE-KEY*ist der`.pem`enthält das private Zertifikat des EC2-Schlüsselpaars, das Sie zum Starten der Amazon EC2 EC2-Instance verwendet haben. Weitere Informationen finden Sie unterAbrufen des öffentlichen Schlüssels für Ihr SchlüsselpaarimBenutzerhandbuch für Amazon EC2aus.
   > Die*INSTANCE-PUBLIC-DNS-NAME*ist der öffentliche DNS-Name (Domain Name System) Ihrer Amazon EC2 EC2-Instance, auf dem Ihr Gateway ausgeführt wird. Sie erhalten diesen öffentlichen DNS-Namen, indem Sie die Amazon EC2 EC2-Instance in der EC2-Konsole auswählen und auf dieBeschreibung-Registerkarte

2. Geben Sie an der -Eingabeauff**6 - Command Prompt**So öffnen SieSupportChannel-Konsole.
3. Geben Sie **h** ein, um das Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) zu öffnen.

4. Gehen Sie folgendermaßen vor:

   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, finden Sie imVERFÜGBARE BEFEHLE, geben Sie ein**`open-support-channel`**um eine Verbindung zum Kundensupport für Storage Gateway herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal öffnen könnenAWSaus. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.
   - Wenn Ihr Gateway einen VPC-Endpunkt verwendet, geben Sie im Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) **`open-support-channel`** ein. Wenn Ihr Gateway nicht aktiviert ist, geben Sie den VPC-Endpunkt oder die IP-Adresse ein, um eine Verbindung mit dem Kundenservice für Storage Gateway herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal öffnen könnenAWSaus. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.

   > **Note**
   >
   > Die Kanalnummer ist keine Transmission Control Protocol/User Datagram Protocol (TCP/UDP) Portnummer. Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP-22) Verbindung zu den Storage Gateway Gateway-Servern her und schafft den Support-Kanal für die Verbindung.

5. Wenn der Support-Kanal hergestellt wurde, geben Sie Ihre Support-Service-Nummer anSupportsoSupportkann Unterstützung bei der Fehlerbehebung leisten.
6. Wenn die Supportsitzung beendet ist, geben Sie **`q`** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn der Amazon Web Services Support Sie darüber informiert, dass die Supportsitzung abgeschlossen ist.
7. Geben Sie ein.**`exit`**um die Storage Gateway -Konsole zu verlassen.
8. Befolgen Sie das Menü der Konsole um sich von der Storage Gateway Gateway-Instance abzumelden.

Behebung von Fehlern bei der Hardware-

In den folgenden Themen werden Probleme, die möglicherweise im Zusammenhang mit der Storage Gateway Hardware Appliance auftreten können, sowie Vorschläge zur Behebung von diesen beschrieben.

Sie können die Dienst-IP-Adresse nicht ermitteln

Wenn Sie versuchen, eine Verbindung mit Ihrem Service herzustellen, stellen Sie sicher, dass Sie die Service-IP-Adresse und nicht die Host-IP-Adresse verwenden. Konfigurieren Sie die Service-IP-Adresse in der Servicekonsole und die Host-IP-Adresse in der Hardwarekonsole. Die Hardwarekonsole wird angezeigt, wenn die Hardware-Appliance gestartet wird. Um die Servicekonsole über die Hardwarekonsole zu öffnen, wählen Sie Open Service Console (Servicekonsole öffnen).

Wie führt man einen Werksreset durch?

Wenn Sie Ihre Appliance auf die Werkseinstellungen zurücksetzen müssen, wenden Sie sich an das Storage Gateway Hardware-Appliance-Team, um Support zu erhalten, wie im folgenden Support-Abschnitt beschrieben.

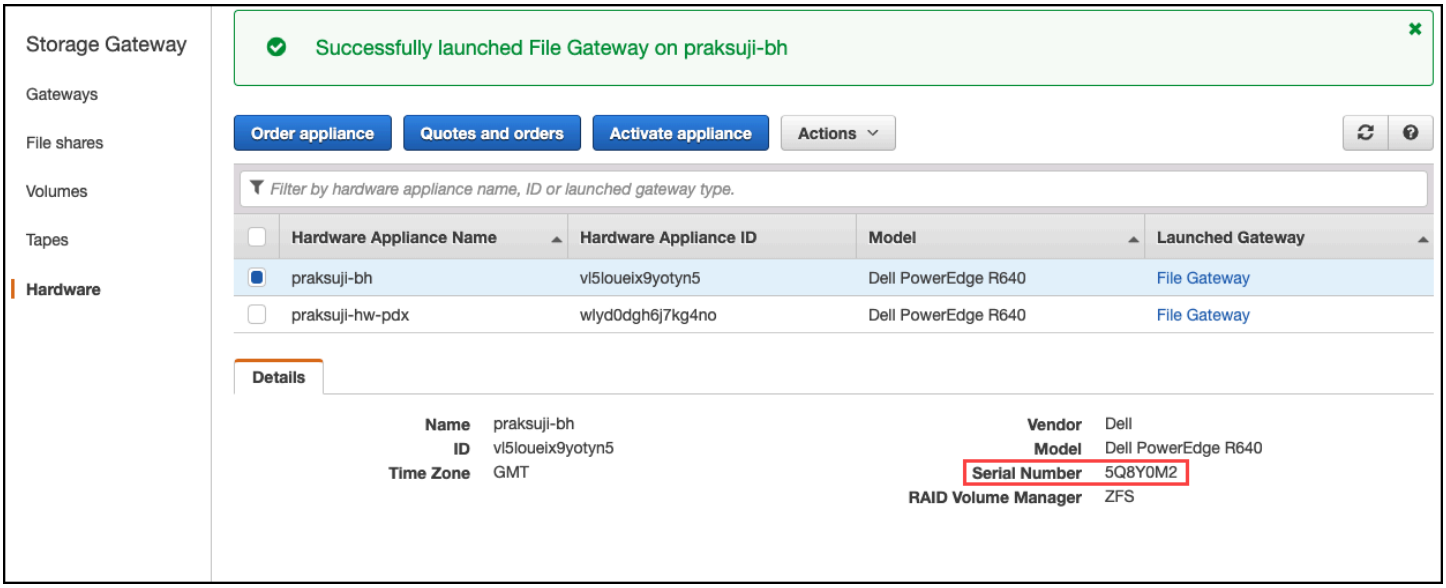
Wo erhalten Sie Dell iDRAC Support?

Der Dell PowerEdge R640-Server wird mit der Dell iDRAC-Verwaltungsschnittstelle bereitgestellt. Wir empfehlen Folgendes:

- Wenn Sie die iDRAC-Verwaltungsschnittstelle verwenden, müssen Sie das Standardpasswort ändern. Weitere Informationen zu den iDrac-Anmeldeinformationen finden Sie unterDell PowerEdge - Was ist der Standardbenutzername und das Passwort für iDRAC?aus.
- Stellen Sie sicher, dass die Firmware auf dem neuesten Stand ist, um Sicherheitsverletzungen zu verhindern.
- Wenn die iDRAC-Netzwerkschnittstelle an einen normalen Port (`em`) verschoben wird, kann dies zu Leistungsproblemen führen oder die normale Funktionsweise der Appliance beeinträchtigen.

Sie können die Seriennummer der Hardware-Appliance nicht finden

Um die Seriennummer der Hardware-Appliance zu suchen, rufen Sie dieHardware (Hardware)Seite in der Storage Gateway Gateway-Konsole, wie im Folgenden dargestellt.



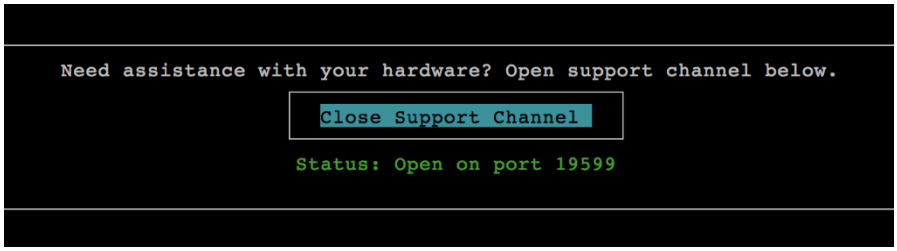
Wo erhalten Sie Unterstützung für Hardware-Appliances

Informationen zum Support für Storage Gateway Hardware Appliance finden Sie unterSupportaus.

DieSupportDas Team bittet Sie möglicherweise darum, den Support-Kanal zu aktivieren, um Ihre Probleme mit dem Gateway remote zu beheben. Dieser Port muss für den normalen Betrieb des Gateways nicht offen sein, für die Fehlerbehebung ist dies jedoch erforderlich. Sie können den Support-Kanal über die Hardware-Konsole aktivieren, wie im folgenden Verfahren dargestellt.

So öffnen Sie einen Support-Kanal fürAWS

1. Öffnen Sie die Hardwarekonsole.
2. Wählen Sie Open Support Channel (Support-Kanal öffnen), wie im Folgenden dargestellt.



   Die zugewiesene Portnummer sollte innerhalb von 30 Sekunden angezeigt werden, sofern keine Probleme mit der Netzwerkverbindung oder der Firewall bestehen.
3. Notieren Sie sich die Portnummer und geben SieSupportaus.

Fehlerbehebung bei File Gateway Problemen

Sie können Ihr File Gateway mit einer Amazon CloudWatch CloudWatch-Protokollgruppe konfigurieren, wenn Sie VMware vSphere High Availability (HA) ausführen. In diesem Fall erhalten Sie Benachrichtigungen über den Zustand Ihres File Gateways und über Fehler, die im File Gateway auftreten. Informationen zu diesen Fehler- und Zustandsbenachrichtigungen finden Sie in CloudWatch Logs.

In den folgenden Abschnitten finden Sie Informationen, die Ihnen helfen können, die Ursache der einzelnen Fehler- und Zustandsbenachrichtigungen zu verstehen und Probleme zu beheben.

Themen

Fehler: InaccessibleStorageClass

Du kannst einen bekommen`InaccessibleStorageClass`Fehler, wenn ein Objekt aus der Amazon S3 S3-Standardspeicherklasse entfernt wurde.

Hier tritt der Fehler in der Regel im File Gateway auf, wenn es versucht, das angegebene Objekt entweder in den S3-Bucket hochzuladen oder das Objekt aus dem S3-Bucket zu lesen. Bei diesem Fehler wurde das Objekt im Allgemeinen zu Amazon S3 Glacier verschoben und befindet sich entweder in der Speicherklasse S3 Glacier oder S3 Glacier Deep Archive.

So beheben Sie einen InAccessibleStorageClass-Fehler

- Verschieben Sie das Objekt aus der Speicherklasse S3 Glacier oder S3 Glacier Deep Archive zurück zu S3.

  Wenn Sie das Objekt in den S3-Bucket verschieben, um einen Upload-Fehler zu beheben, wird die Datei letztendlich hochgeladen. Wenn Sie das Objekt in den S3-Bucket verschieben, um einen Lesefehler zu beheben, kann der SMB- oder NFS-Client des File Gateways die Datei dann lesen.

Fehler: s3AccessDenied

Du kannst einen bekommen`S3AccessDenied`Fehler für den Amazon S3 S3-Bucket-Zugriff einer DateifreigabeAWS Identity and Access Management(IAM) -Rolle. In diesem Fall ist die IAM-Rolle S3-Bucket-Zugriff, die durch`roleArn`Im Fehler lässt die betreffende Operation nicht zu. Der Vorgang ist aufgrund der Berechtigungen für die Objekte im durch das Amazon S3-Präfix angegebenen Verzeichnis nicht zulässig.

So beheben Sie einen S3AccessDenied-Fehler

- Ändern Sie die Amazon S3 S3-Zugriffsrichtlinie, die an angehängt ist`roleArn`Im Datei-Gateway-Zustandsprotokoll, um Berechtigungen für den Amazon S3 S3-Vorgang zu erteilen. Stellen Sie sicher, dass die Zugriffsrichtlinie die Berechtigung für die Operation zulässt, die den Fehler verursacht hat. Erlauben Sie außerdem die Berechtigung für das im Protokoll für `prefix` angegebene Verzeichnis. Weitere Informationen zu Amazon S3 S3-Berechtigungen finden Sie unterAngeben von Berechtigungen in einer RichtlinieinAmazon Simple Storage Service — Benutzerhandbuch.

  Die folgenden Operationen können zum Auftreten des Fehlers `S3AccessDenied` führen.

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

Fehler: InvalidObjectState

Du kannst einen bekommen`InvalidObjectState`Fehler, wenn ein anderer Schreiber als das angegebene File Gateway die angegebene Datei im angegebenen S3-Bucket ändert. Daher

stimmt der Status der Datei für das File Gateway nicht mit dem Status in Amazon S3 überein. Alle nachfolgenden Uploads der Datei zu Amazon S3 oder Abrufe der Datei aus Amazon S3 schlagen fehl.

So beheben Sie einen InvalidObjectState-Fehler

Wenn der Vorgang, der die Datei ändert,`S3Upload`oder`S3GetObject`wie folgt:

1. Speichern Sie die neueste Kopie der Datei im lokalen Dateisystem Ihres SMB- oder NFS-Clients (Sie benötigen diese Dateikopie in Schritt 4). Wenn die Version der Datei in Amazon S3 die neueste Version ist, laden Sie diese Version herunter. Sie können dies über die AWS Management Console oder die AWS CLI ausführen.
2. Löschen Sie die Datei in Amazon S3 mitAWS Management ConsoleoderAWS CLIaus.
3. Löschen Sie die Datei mit Ihrem SMB- oder NFS-Client aus dem Datei-Gateway.
4. Kopieren Sie die neueste Version der Datei, die Sie in Schritt 1 in Amazon S3 mit Ihrem SMB- oder NFS-Client gespeichert haben. Führen Sie dies über den Datei-Gateway aus.

Fehler: ObjectMissing

Du kannst einen bekommen`ObjectMissing`Fehler, wenn ein anderer Schreiber als das angegebene File Gateway die angegebene Datei aus dem S3-Bucket löscht. Alle nachfolgenden Uploads auf Amazon S3 oder Abrufe von Amazon S3 für das Objekt schlagen fehl.

So beheben Sie einen ObjectMissing Fehler

Wenn der Vorgang, der die Datei ändert,`S3Upload`oder`S3GetObject`wie folgt:

1. Speichern Sie die neueste Kopie der Datei im lokalen Dateisystem Ihres SMB- oder NFS-Clients (Sie benötigen diese Dateikopie in Schritt 3).
2. Löschen Sie die Datei mit Ihrem SMB- oder NFS-Client aus dem Datei-Gateway.
3. Kopieren Sie die neueste Version der Datei, die Sie in Schritt 1 gespeichert haben, mit Ihrem SMB- oder NFS-Client. Führen Sie dies über den Datei-Gateway aus.

: Benachrichtigung Neustart

Sie können eine Neustart-Benachrichtigung erhalten, wenn die Gateway-VM neu gestartet wird. Sie können eine Gateway-VM mithilfe der VM Hypervisor-Managementkonsole oder der Storage

Gateway Gateway-Konsole neu starten. Sie können den Neustart auch mithilfe der Gateway-Software während des Wartungszyklus des Gateways ausführen.

Wenn die Zeit des Neustarts innerhalb von 10 Minuten nach der konfigurierten Wartungsstartzeit des Gateways liegt, ist dieser Neustart wahrscheinlich ein normales Ereignis und kein Anzeichen für ein Problem. Wenn der Neustart deutlich außerhalb des Wartungsfensters stattgefunden hat, überprüfen Sie, ob das Gateway manuell neu gestartet wurde.

: Benachrichtigung HardReBoot

Sie können eine `HardReboot`-Benachrichtigung erhalten, wenn die Gateway-VM unerwartet neu gestartet wird. Ein solcher Neustart kann auf Stromausfall, einen Hardwarefehler oder ein anderes Ereignis zurückzuführen sein. Bei VMware-Gateways kann ein Zurücksetzen durch vSphere High Availability Application Monitoring dieses Ereignis auslösen.

Wenn Ihr Gateway in einer solchen Umgebung ausgeführt wird, überprüfen Sie, ob die Benachrichtigung `HealthCheckFailure` vorhanden ist, und konsultieren Sie das VMware-Ereignisprotokoll für die VM.

: Benachrichtigung HealthCheckFailure

Für ein Gateway auf VMware vSphere HA können Sie die Benachrichtigung `HealthCheckFailure` erhalten, wenn eine Zustandsprüfung fehlschlägt und ein Neustart der VM angefordert wird. Dieses Ereignis tritt auch während eines Tests zum Überwachen der Verfügbarkeit auf, der durch die Benachrichtigung `AvailabilityMonitorTest` angezeigt wird. In diesem Fall wird die Benachrichtigung `HealthCheckFailure` erwartet.

> **Note**
>
> Diese Benachrichtigung gilt nur für VMware-Gateways.

Wenn dieses Ereignis wiederholt ohne die Benachrichtigung `AvailabilityMonitorTest` auftritt, überprüfen Sie die VM-Infrastruktur auf Probleme (Speicher, Arbeitsspeicher usw.). Wenn Sie zusätzliche Unterstützung benötigen, wenden Sie sich anSupportaus.

: Benachrichtigung AvailabilityMonitorTest

Du bekommst ein`AvailabilityMonitorTest`Benachrichtigung wenn Siführe einen Test durchderVerfügbarkeit und Anwendungsüberwachung-System auf Gateways, die auf einer VMware vSphere HA-Plattform ausgeführt werden.

Fehler: RoleTrustRelationshipInvalid

Wenn diese Fehlermeldung angezeigt wird, wenn die IAM-Rolle für eine Dateifreigabe eine falsch konfigurierte IAM-Vertrauensstellung aufweist (d. h. die IAM-Rolle vertraut dem Storage Gateway Gateway-Prinzipal mit dem Namen nicht`storagegateway.amazonaws.com`) enthalten. Folglich kann das File Gateway die Anmeldeinformationen nicht abrufen, um Operationen auf dem S3-Bucket auszuführen, der die Dateifreigabe unterstützt.

So beheben Sie einen RoletRustRelationshipInvalid-Fehler

- Verwenden Sie die IAM-Konsole oder die IAM-API, um einzuschließen`storagegateway.amazonaws.com`Als Prinzipal, der von der IamRole Ihrer Dateifreigabe als vertrauenswürdig eingestuft wird. Weitere Informationen zur IAM-Rolle finden Sie unterTutorial: Delegiertenzugriff überAWSKonten mit IAM-Rollenaus.

Fehlerbehebung mit CloudWatch-Metriken

Im Folgenden finden Sie Informationen zu Aktionen zur Behebung von Problemen bei der Verwendung von Amazon CloudWatch CloudWatch-Metriken mit Storage Gateway.

Themen

Ihr Gateway reagiert langsam beim Durchsuchen von Verzeichnissen

Wenn Ihr File-Gateway langsam reagiert, während Sie dielsBefehl oder durchsuchen Sie Verzeichnisse, überprüfen Sie die`IndexFetch`und`IndexEviction`CloudWatch-Metriken:

- Wenn das Symbol`IndexFetch`metrik ist größer als 0, wenn Sie eine`ls`-Befehl oder Suchverzeichnisse, wurde Ihr File Gateway ohne Informationen über den Inhalt des betreffenden Verzeichnisses gestartet und musste auf Amazon S3 zugreifen. Nachfolgende Versuche, den Inhalt dieses Verzeichnisses aufzulisten, sollten schneller ausgeführt werden.
- Wenn das Symbol`IndexEviction`Die Metrik größer als 0 ist, bedeutet dies, dass das File Gateway die maximale Menge erreicht hat, die es zu diesem Zeitpunkt in seinem Cache verwalten kann. In diesem Fall muss Ihr File Gateway Speicherplatz im zuletzt aufgerufenen Verzeichnis freigeben, um ein neues Verzeichnis aufzulisten. Wenn dies häufig auftritt und sich die Leistung beeinträchtigt, wenden Sie sich anSupportaus.

  Diskutieren mitSupportDer Inhalt des zugehörigen S3-Buckets und fragen Sie nach Empfehlungen zur Verbesserung der Leistung basierend auf Ihrem Anwendungsfall.

Ihr Gateway reagiert nicht

Wenn Ihr Datei-Gateway nicht reagiert, gehen Sie folgendermaßen vor:

- Wenn kürzlich ein Neustart oder ein Softwareupdate vorgenommen wurde, überprüfen Sie die Metrik `IOWaitPercent`. Diese Metrik zeigt den Prozentsatz der Zeit, für die die CPU im Leerlauf war, wenn eine ausstehende Datenträger-E/A-Anfrage vorhanden war. In einigen Fällen ist dieser Prozentsatz möglicherweise hoch (10 oder höher) und angestiegen, nachdem der Server neu gestartet oder aktualisiert wurde. In diesen Fällen wird Ihr File Gateway möglicherweise durch einen langsameren Stamm-Datenträger beeinträchtigt, da es den Indexcache in den RAM neu aufbaut. Sie können dieses Problem beheben, indem Sie einen schnelleren physischen Datenträger für den Stamm-Datenträger verwenden.
- Wenn das Symbol`MemUsedBytes`metrik ist bei oder fast identisch mit`MemTotalBytes`Metrik, dann ist nicht mehr verfügbarer RAM für das File Gateway vorhanden. Stellen Sie sicher, dass mindestens der erforderlichen RAM für die Datei-Gateways verfügbar ist. Wenn dies bereits der Fall ist, sollten Sie Ihrem File Gateway je nach Workload und Anwendungsfall mehr RAM hinzufügen.

  Wenn die Dateifreigabe SMB ist, kann dieses Problem auch auf die Anzahl der SMB-Clients zurückzuführen sein, die mit der Dateifreigabe verbunden sind. Überprüfen Sie die Metrik

`SMBV(1/2/3)Sessions`, um die Anzahl der Clients zu sehen, die zu einem bestimmten Zeitpunkt verbunden sind. Wenn viele Clients verbunden sind, müssen Sie Ihrem File Gateway möglicherweise mehr RAM hinzufügen.

Ihr Gateway überträgt Daten an Amazon S3 nur langsam an Amazon S3

Wenn Ihr Datei-Gateway Daten nur langsam an Amazon S3 überträgt, gehen Sie folgendermaßen vor:

- Wenn das Symbol`CachePercentDirty`Die Metrik beträgt 80 oder höher, Ihr File Gateway schreibt Daten schneller auf den Datenträger, als es die Daten auf Amazon S3 hochladen kann. Sie sollten die Bandbreite für den Upload von Ihrem File Gateway erhöhen, einen oder mehrere Cache-Datenträger hinzufügen oder Client-Schreibvorgänge verlangsamen.
- Wenn das Symbol`CachePercentDirty`Metrik ist niedrig,`IoWaitPercent`-Metrik Wenn`IoWaitPercent`ist größer als 10, wird Ihr File Gateway möglicherweise durch die Geschwindigkeit des lokalen Cache-Datenträgers beeinträchtigt. Wir empfehlen lokale SSD-Datenträger (Solid-State-Drive) für den Cache, vorzugsweise NVM Express (NVMe). Wenn solche Datenträger nicht verfügbar sind, verwenden Sie mehrere Cache-Datenträger von separaten physischen Datenträgern, um zu versuchen, die Leistung zu verbessern.
- Wenn`S3PutObjectRequestTime`,`S3UploadPartRequestTime`, oder`S3GetObjectRequestTime`hoch sind, könnte es zu einem Netzwerkengpass kommen. Analysieren Sie Ihr Netzwerk, um sicherzustellen, dass das Gateway die erwartete Bandbreite hat.

Ihr Gateway führt mehr Amazon S3 S3-Vorgänge durch als erwartet

Wenn Ihr Datei-Gateway mehr Amazon S3 S3-Vorgänge als erwartet ausführt, überprüfen Sie die`FilesRenamed`-Metrik Umbenennungsvorgänge sind in Amazon S3 teuer. Optimieren Sie Ihren Workflow, um die Anzahl der Umbenennungsvorgänge zu minimieren.

Sie sehen keine Dateien in Ihrem Amazon S3 S3-Bucket

Wenn Sie feststellen, dass Dateien auf dem Gateway nicht im Amazon S3 S3-Bucket enthalten sind, überprüfen Sie die`FilesFailingUpload`-Metrik Wenn die Metrik meldet, dass einige Dateien nicht hochgeladen werden, überprüfen Sie Ihre Gesundheitsbenachrichtigungen. Wenn Dateien nicht hochgeladen werden können, generiert das Gateway eine Integritätsbenachrichtigung mit weiteren Details zum Problem.

Ihr Gateway-Sicherungsauftrag schlägt fehl oder es gibt Fehler beim Schreiben in Ihr Gateway

Wenn Ihr File Gateway-Sicherungsauftrag fehlschlägt oder während des Schreibens in Ihr File Gateway Fehler auftreten, gehen Sie folgendermaßen vor:

- Wenn das Symbol`CachePercentDirty`Die Metrik beträgt 90 Prozent oder höher. Ihr File Gateway kann keine neuen Schreibvorgänge auf den Datenträger akzeptieren, da auf dem Cache-Datenträger nicht genügend Speicherplatz verfügbar ist. Hier erfahren Sie, wie schnell Ihr Datei-Gateway auf Amazon FSx oder Amazon S3 hochlädt, rufen Sie die`CloudBytesUploaded`-Metrik Vergleichen Sie diese Metrik mit dem`WriteBytes`Metrik, die anzeigt, wie schnell der Client Dateien in Ihr Datei-Gateway schreibt. Wenn Ihr File Gateway schneller schreibt, als es in Amazon FSx oder Amazon S3 hochladen kann, fügen Sie weitere Cache-Datenträger hinzu, um mindestens die Größe des Sicherungsauftrags abzudecken. Oder erhöhen Sie die Upload-Bandbreite.
- Wenn ein Backup-Job fehlschlägt, aber der`CachePercentDirty`Die Metrik beträgt weniger als 80 Prozent, Ihr File Gateway trifft möglicherweise auf ein clientseitiges Sitzungs-Timeout. In SMB können Sie dieses Timeout mit dem PowerShell-Befehl `Set-SmbClientConfiguration -SessionTimeout 300` erhöhen. Wenn Sie diesen Befehl ausführen, wird das Timeout auf 300 Sekunden festgelegt.

  Stellen Sie in NFS sicher, dass der Client hart und nicht weich gemountet ist.

Fehlerbehebung bei Datenfreigabe Problemen

Informationen über die Aktionen finden Sie nachfolgend, Aktionen die Sie vornehmen können, wenn Sie unerwartete Probleme mit Ihrer Datenfreigabe haben.

Themen

- Änderungen, die direkt in einem S3-Bucket mit aktivierter Objektversionierung vorgenommen werden, können sich auf das auswirken, was Sie in Ihrer Dateifreigabe sehen
- Beim Schreiben in einen S3-Bucket mit aktivierter Objektversionierung kann das Amazon S3 File Gateway mehrere Versionen eines S3-Objekts erstellen
- Änderungen an einem S3-Bucket werden im Storage Gateway nicht berücksichtigt
- ACL-Berechtigungen funktionieren nicht wie erwartet
- Ihre Gateway-Leistung ging zurück, nachdem Sie einen rekursiven Vorgang ausgeführt haben

Ihre Dateifreigabe steckt im CREATING Status fest

Wenn Ihre Datenfreigabe erstellt wird, hat sie den Status CREATING. Der Status geht in den AVAILABLE Status über, nachdem die Dateifreigabe erstellt wird. Wenn Ihre Dateifreigabe im Status CREATING bleibt, führen Sie folgende Schritte aus:

1. Öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Stellen Sie sicher, dass die S3-Buckets, die Sie Dateifreigabe zugeordnet haben vorhanden ist. Wenn das Bucket nicht vorhanden ist, erstellen Sie es. Nachdem Sie den Bucket erstellt haben, geht der Dateifreigaben-Status in den AVAILABLE Status über. Weitere Informationen zum Erstellen eines S3-Buckets finden Sie unterBucket erstellenimAmazon Simple Storage Service — Benutzerhandbuchaus.
3. Stellen Sie sicher, dass der Name des Buckets mit den Regeln für die Benennung von Buckets in Amazon S3 übereinstimmt. Weitere Informationen finden Sie unterRegeln für die Bucket-BenennungimBenutzerhandbuch für Amazon Simple Storage Serviceaus.
4. Stellen Sie sicher, dass die IAM-Rolle, die Sie für den Zugriff auf den S3-Bucket verwendet haben, über die richtigen Berechtigungen verfügt, und prüfen Sie, ob das S3-Bucket als Ressource in der IAM-Richtlinie aufgelistet ist. Weitere Informationen finden Sie unter Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket.

Sie können keine Dateifreigabe erstellen

1. Wenn Sie keine Dateifreigabe erstellen können, da Ihre Dateifreigabe im Status CREATING bleibt, prüfen Sie, dass das S3-Bucket, das Sie Ihrer Dateifreigabe zugeordnet haben vorhanden ist. Weitere Informationen über wie dies getan wird finden Sie unter Ihre Dateifreigabe steckt im CREATING Status fest, oben.

2. Wenn der S3-Bucket vorhanden ist, stellen Sie sicher, dassAWS Security Token ServiceIn der Region aktiviert, in der Sie die Dateifreigabe erstellen. Wenn ein Sicherheits-Token nicht aktiviert ist, sollten Sie diesen aktivieren. Weitere Informationen zum Aktivieren eines TokensAWS Security Token Service, finden Sie unterAktivieren und DeaktivierenAWSSTS in einemAWSRegionimIAM User Guideaus.

SMB-Dateifreigaben erlauben nicht mehrere verschiedene Zugriffsmethoden

SMB-Dateifreigaben haben die folgenden Beschränkungen:

1. Wenn derselbe Client versucht, eine SMB-Dateifreigabe mit Active Directory- und eine mit Gastzugriff zu mounten, wird die folgende Fehlermeldung angezeigt: `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. Ein Windows-Benutzer kann nicht mit zwei SMB-Dateifreigaben mit Gastzugriff verbunden bleiben und die Verbindung wird möglicherweise getrennt, wenn eine neue Gastzugriff-Verbindung aufgebaut wird.
3. Ein Windows-Client kann nicht gleichzeitig eine SMB-Dateifreigabe mit Gastzugriff und eine mit Active Directory-Zugriff mounten, die vom selben Gateway exportiert wird.

Mehrere Dateifreigaben können nicht in den zugeordneten S3-Bucket schreiben

Wir empfehlen nicht den S3-Bucket so zu konfigurieren, dass mehrere Dateifreigaben die Erlaubnis zum Schreiben auf einen S3-Bucket haben. Dieser Ansatz kann zu unvorhersehbaren Ergebnissen führen.

Stattdessen empfehlen wir, dass Sie nur eine Dateifreigabe zulassen, die auf separate S3-Bucket schreibt. Sie erstellen Bucket-Richtlinien um die Rolle die mit Ihre Dateifreigabe verknüpft ist auf den Bucket zu schreiben. Weitere Informationen finden Sie unter Bewährte Methoden für die Datei.

Dateien können nicht in Ihren S3-Bucket hochgeladen werden

Wenn Sie keine Dateien in Ihr S3-Bucket hochladen können, führen Sie folgende Schritte aus:

1. Stellen Sie sicher, dass Sie dem Amazon S3 File Gateway den erforderlichen Zugriff zum Hochladen von Dateien in Ihren S3-Bucket gewähren. Weitere Informationen finden Sie unter Gewähren des Zugriffs auf einen Amazon S3 S3-Bucket.
2. Stellen Sie sicher, dass die Rolle, die den Bucket erstellt hat über Schreibberechtigungen auf dem S3 Bucket verfügt. Weitere Informationen finden Sie unter Bewährte Methoden für die Datei.
3. Wenn Ihr Datei-Gateway SSE-KMS zur Verschlüsselung verwendet, stellen Sie sicher, dass die mit der Dateifreigabe verknüpfte IAM-Rolle enthältkms:Encrypt,kms:Decrypt,km:Reverschlüsseln,kms:GenerateDataKey, undkms:DescribeKey-Berechtigungen Weitere Informationen finden Sie unterVerwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für Storage Gatewayaus.

Die Standardverschlüsselung kann nicht geändert werden, um SSE-KMS zum Verschlüsseln von Objekten zu verwenden, die in meinem S3-Bucket gespeichert sind

Wenn Sie die Standardverschlüsselung ändern und SSE-KMS vornehmen (serverseitige Verschlüsselung mitAWS KMS—verwaltete Schlüssel) Als Standardwert für Ihren S3-Bucket, werden Objekte, die ein Amazon S3 File Gateway im -Bucket speichert, nicht mit SSE-KMS verschlüsselt. Standardmäßig verwendet ein S3 File Gateway eine serverseitige Verschlüsselung, die mit Amazon S3 (SSE-S3) verwaltet wird, wenn es Daten in einen S3-Bucket schreibt. Durch die Änderung des Standards wird nicht automatisch Ihre Verschlüsselung geändert.

Um die Verschlüsselung zu ändern, sodass SSE-KMS mit Ihrem eigenen AWS KMS-Schlüssel verwendet wird, müssen Sie die SSE-KMS-Verschlüsselung aktivieren. Dazu geben Sie den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels an, wenn Sie Ihre Dateifreigabe erstellen. Sie können mit der API-Operation `UpdateNFSFileShare` oder `UpdateSMBFileShare` auch KMS-Einstellungen für Ihre Dateifreigabe aktualisieren. Diese Aktualisierung gilt für Objekte, die nach der Aktualisierung in den S3-Buckets gespeichert sind. Weitere Informationen finden Sie unter Datenverschlüsselung mitAWS KMS.

Änderungen, die direkt in einem S3-Bucket mit aktivierter Objektversionierung vorgenommen werden, können sich auf das auswirken, was Sie in Ihrer Dateifreigabe sehen

Wenn Ihr S3-Bucket über Objekte verfügt, die von einem anderen Client in diesen geschrieben wurden, ist die Ansicht Ihres S3-Buckets möglicherweise aufgrund des Objekt-Versioning des S3-

Buckets nicht aktuell. Aktualisieren Sie immer erst den Cache, ehe Sie sich die gewünschten Dateien genauer ansehen.

Objekt-Versioning ist eine optionale S3-Bucket-Funktion, die den Schutz der Daten unterstützt, indem mehrere Kopien des Objekts mit demselben Namen gespeichert werden. Jede Kopie hat z. B. einen separaten ID-Wert`file1.jpg`:`ID="xxx"`und`file1.jpg`: `ID="yyy"`aus. Die Anzahl der Objekte mit dem gleichen Namen und deren Lebensdauer wird durch die Amazon S3 S3-Richtlinien für den Lebenszyklus geregelt. Weitere Informationen zu diesen Amazon S3 S3-Konzepten finden Sie unterVerwenden von VersioningundVerwaltung des ObjektlebenszyklusimEntwicklerhandbuch für Amazon S3.

Wenn Sie ein versioniertes Objekt löschen, erhält dieses eine Löschmarkierung, bleibt aber erhalten. Nur ein S3-Bucket-Eigentümer kann ein Objekt mit aktiviertem Versioning dauerhaft löschen.

Bei den in Ihrem S3 File Gateway gezeigten Dateien handelt es sich um die neuesten Versionen von Objekten in einem S3-Bucket zum Zeitpunkt des Abrufens des Objekts oder zum Zeitpunkt der Cache-Aktualisierung. S3-Datei-Gateways ignorieren ältere Versionen oder Objekte, die für die Löschung markiert sind. Beim Lesen einer Datei werden Daten aus der neuesten Version gelesen. Wenn Sie eine Datei in Ihre Dateifreigabe schreiben, erstellt Ihr S3 File Gateway eine neue Version des benannten Objekts mit Ihren Änderungen. Diese Version wird dann zur neuesten Version.

Ihr S3 File Gateway liest weiter aus der früheren Version. Aktualisierungen, die Sie vornehmen, basieren auf der früheren Version, wenn eine neue Version außerhalb der Anwendung zum S3-Bucket hinzugefügt wird. Nutzen Sie zum Lesen der neuesten Version eines Objekts die API-Aktion RefreshCache oder führen Sie über die Konsole eine Aktualisierung durch, wie in Aktualisieren von Objekten in Ihrem Amazon S3 S3-Bucket beschrieben.

> **Important**
>
> Wir empfehlen nicht, dass Objekte oder Dateien von außerhalb der Dateifreigabe in Ihren S3 File Gateway S3 Bucket geschrieben werden.

Beim Schreiben in einen S3-Bucket mit aktivierter Objektversionierung kann das Amazon S3 File Gateway mehrere Versionen eines S3-Objekts erstellen

Wenn die Objektversionierung aktiviert ist, können Sie bei jedem Update von Ihrem NFS- oder SMB-Client auf eine Datei mehrere Versionen eines Objekts in Amazon S3 erstellt haben. Hier sind Szenarien, die dazu führen können, dass mehrere Versionen eines Objekts in Ihrem S3-Bucket erstellt werden:

- Wenn eine Datei im Amazon S3 File Gateway von einem NFS- oder SMB-Client geändert wird, nachdem sie auf Amazon S3 hochgeladen wurde, lädt das S3 File Gateway die neuen oder geänderten Daten hoch, anstatt die gesamte Datei hochzuladen. Die Dateiänderung führt dazu, dass eine neue Version des Amazon S3 S3-Objekts erstellt wird.
- Wenn eine Datei von einem NFS- oder SMB-Client in das S3 File Gateway geschrieben wird, lädt das S3 File Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von seinen Metadaten (Eigentümern, Zeitstempel usw.). Durch das Hochladen der Dateidaten wird ein Amazon S3 S3-Objekt erstellt, und das Hochladen der Metadaten für die Datei aktualisiert die Metadaten für das Amazon S3 S3-Objekt. Dieser Prozess erstellt eine andere Version des Objekts, was zu zwei Versionen eines Objekts führt.
- Wenn das S3 File Gateway größere Dateien hochlädt, muss es möglicherweise kleinere Teile der Datei hochladen, bevor der Client mit dem Schreiben in das Datei-Gateway fertig ist. Einige Gründe dafür sind die Freigabe von Cache-Speicherplatz oder eine hohe Schreibrate in eine Datei. Dies kann zu mehreren Versionen eines Objekts im S3-Bucket führen.

Sie sollten Ihren S3-Bucket überwachen, um festzustellen, wie viele Versionen eines Objekts vorhanden sind, bevor Sie Lebenszyklusrichtlinien einrichten, um Objekte in verschiedene Speicherklassen zu verschieben. Sie sollten den Lebenszyklusablauf für frühere Versionen konfigurieren, um die Anzahl der Versionen zu minimieren, die Sie für ein Objekt in Ihrem S3-Bucket haben. Die Verwendung der Replikation derselben Region (SRR) oder regionsübergreifender Replikation (CRR) zwischen S3-Buckets erhöht den verwendeten Speicher. Weitere Informationen zur Replikation finden Sie unterReplikationaus.

> **Important**
>
> Konfigurieren Sie die Replikation zwischen S3-Buckets erst, wenn Sie wissen, wie viel Speicher verwendet wird, wenn die Objektversionierung aktiviert ist.

Die Verwendung von versionierten S3-Buckets kann die Menge an gespeicherten Daten in Amazon S3 erheblich erhöhen, da jede Änderung an einer Datei dazu führt, dass eine neue Version des S3-Objekts erstellt wird. Standardmäßig speichert Amazon S3 weiterhin all diese Versionen, es sei denn, Sie erstellen eine Richtlinie, die dieses Verhalten außer Kraft setzt und begrenzen die Anzahl der beibehaltenen Versionen. Wenn Sie bei aktiviertem Objekt-Versioning einen ungewöhnlich hohen Speicherverbrauch feststellen, sollten Sie Ihre Speicherrichtlinien überprüfen. Eine Erhöhung der Anzahl der `HTTP 503-slow down`-Antworten auf Browser-Anforderungen kann ebenfalls auf Probleme mit dem Objekt-Versioning hindeuten.

Wenn Sie die Objektversionierung nach der Installation eines S3 File Gateways aktivieren, werden alle eindeutigen Objekte beibehalten (`ID="NULL"`) und Sie können sie alle im Dateisystem sehen. Neuen Versionen von Objekten wird eine eindeutige ID zugewiesen (ältere Versionen bleiben erhalten). Basierend auf dem Zeitstempels des Objekts ist nur das neueste versionierte Objekt im NFS-Dateisystem zu sehen.

Nachdem Sie das Objekt-Versioning aktiviert haben, kann Ihr S3-Bucket nicht mehr zurück in einen nicht versionierten Status versetzt werden. Sie können das Versioning jedoch aussetzen. Wenn Sie das Versioning aussetzen, wird einem neuen Objekt eine ID zugewiesen. Wenn dasselbe Objekt mit einem `ID="NULL"`-Wert vorhanden ist, wird die ältere Version überschrieben. Alle Versionen mit einer ID von nicht `NULL` werden beibehalten. Zeitstempel kennzeichnen das neue Objekt als das aktuelle. Dieses aktuelle Objekt wird dann im NFS-Dateisystem angezeigt.

Änderungen an einem S3-Bucket werden im Storage Gateway nicht berücksichtigt

Storage Gateway aktualisiert den Dateifreigabe-Cache automatisch, wenn Sie Dateien lokal mit der Dateifreigabe in den Cache schreiben. Storage Gateway aktualisiert den Cache jedoch nicht automatisch, wenn Sie eine Datei direkt auf Amazon S3 hochladen. Wenn Sie dies tun, müssen Sie`RefreshCache`-Operation, um die Änderungen an der Dateifreigabe anzuzeigen. Wenn Sie über mehr als eine Dateifreigabe verfügen, müssen Sie die`RefreshCache`-Operation für jede Dateifreigabe.

Sie können den Cache mit der Storage Gateway Gateway-Konsole und derAWS Command Line Interface(AWS CLI):

- Informationen zum Aktualisieren des Caches mit der Storage Gateway Gateway-Konsole finden Sie unter Aktualisieren von Objekten in Ihrem Amazon S3 S3-Bucket.
- So aktualisieren Sie den Cache mit demAWS CLI:
  1. Führen Sie den Befehl aus`aws storagegateway list-file-shares`
  2. Kopieren Sie die Amazon-Ressourcennummer (ARN) der Dateifreigabe mit dem Cache, den Sie aktualisieren möchten.
  3. Ausführen des `srefresh-cache`-Befehl mit Ihrem ARN als Wert für`--file-share-arn`:

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

So automatisieren Sie`RefreshCache`Betrieb, siehe[Wie kann ich den RefreshCache-Vorgang auf Storage Gateway automatisieren?]

ACL-Berechtigungen funktionieren nicht wie erwartet

Wenn Zugriffskontrolllisten(Access Control List, ACL)-Berechtigungen mit Ihrer SMB-Dateifreigabe nicht wie erwartet funktionieren, können Sie einen Test durchführen.

Testen Sie dazu zuerst die Berechtigungen für einen Microsoft Windows-Dateiserver oder für eine lokale Windows-Dateifreigabe. Vergleichen Sie anschließend das Verhalten mit dem der Dateifreigabe Ihres Gateways.

Ihre Gateway-Leistung ging zurück, nachdem Sie einen rekursiven Vorgang ausgeführt haben

In bestimmten Fällen ist es möglich, dass Sie eine rekursive Operation durchführen, wie z. B. das Umbenennen eines Verzeichnisses oder das Aktivieren der Vererbung für eine ACL, und diese dann für die übrige Struktur erzwingen. In diesem Fall wendet Ihr S3 File Gateway die Operation rekursiv auf alle Objekte in der Dateifreigabe an.

Nehmen wir beispielsweise an, Sie wenden Vererbung auf vorhandene Objekte in einem S3-Bucket an. Ihr S3-Datei-Gateway wendet Vererbung rekursiv auf alle Objekte im Bucket an. Solche Operationen können dazu führen, dass die Leistung Ihres Gateways abnimmt.

High Availability-Zustandsbenachrichtigungen

Wenn Sie Ihr Gateway auf der VMware vSphere High Availability(HA)-Plattform ausführen, erhalten Sie möglicherweise Zustandsbenachrichtigungen. Weitere Informationen zu Zustandsbenachrichtigungen finden Sie unter Behebung von Fehlern bei hoher Verfügbarkeit.

Behebung von Fehlern bei hoher Verfügbarkeit

Im Folgenden finden Sie Informationen zu Aktionen, die Sie ausführen müssen, wenn Probleme im Zusammenhang mit der Verfügbarkeit auftreten.

Themen

Zustands-Benachrichtigungen

Wenn Sie Ihr Gateway auf VMware vSphere HA ausführen, senden alle Gateways die folgenden Zustandsbenachrichtigungen an Ihre konfigurierte Amazon CloudWatch CloudWatch-Protokollgruppe. Diese Benachrichtigungen werden in einem Protokollstream mit dem Namen `AvailabilityMonitor` erfasst.

Themen

: Benachrichtigung Neustart

Sie können eine Neustart-Benachrichtigung erhalten, wenn die Gateway-VM neu gestartet wird. Sie können eine Gateway-VM mithilfe der VM Hypervisor-Managementkonsole oder der Storage Gateway Gateway-Konsole neu starten. Sie können den Neustart auch mithilfe der Gateway-Software während des Wartungszyklus des Gateways ausführen.

Maßnahme

Wenn die Zeit des Neustarts innerhalb von 10 Minuten nach der konfigurierten Wartungsstartzeit des Gateways liegt, handelt es sich wahrscheinlich um ein normales Ereignis und es deutet nicht auf ein Problem hin. Wenn der Neustart deutlich außerhalb des Wartungsfensters stattgefunden hat, überprüfen Sie, ob das Gateway manuell neu gestartet wurde.

: Benachrichtigung HardReBoot

Sie können eine `HardReboot`-Benachrichtigung erhalten, wenn die Gateway-VM unerwartet neu gestartet wird. Ein solcher Neustart kann auf Stromausfall, einen Hardwarefehler oder ein anderes Ereignis zurückzuführen sein. Bei VMware-Gateways kann ein Zurücksetzen durch vSphere High Availability Application Monitoring dieses Ereignis auslösen.

Maßnahme

Wenn Ihr Gateway in einer solchen Umgebung ausgeführt wird, überprüfen Sie, ob die Benachrichtigung `HealthCheckFailure` vorhanden ist, und konsultieren Sie das VMware-Ereignisprotokoll für die VM.

: Benachrichtigung HealthCheckFailure

Für ein Gateway auf VMware vSphere HA können Sie die Benachrichtigung `HealthCheckFailure` erhalten, wenn eine Zustandsprüfung fehlschlägt und ein Neustart der VM angefordert wird. Dieses Ereignis tritt auch während eines Tests zum Überwachen der Verfügbarkeit auf, der durch die Benachrichtigung `AvailabilityMonitorTest` angezeigt wird. In diesem Fall wird die Benachrichtigung `HealthCheckFailure` erwartet.

> **Note**
>
> Diese Benachrichtigung gilt nur für VMware-Gateways.

Maßnahme

Wenn dieses Ereignis wiederholt ohne die Benachrichtigung `AvailabilityMonitorTest` auftritt, überprüfen Sie die VM-Infrastruktur auf Probleme (Speicher, Arbeitsspeicher usw.). Wenn Sie zusätzliche Unterstützung benötigen, wenden Sie sich anSupportaus.

: Benachrichtigung AvailabilityMonitorTest

Für ein Gateway auf VMware vSphere HA können Sie ein`AvailabilityMonitorTest`Benachrichtigung wenn Sie[führe einen Test durch](#)der[Verfügbarkeit und Anwendungsüberwachung](#)-System in VMware.

Metriken

Die Metrik `AvailabilityNotifications` ist auf allen Gateways verfügbar. Diese Metrik ist eine Zählung der Anzahl an Zustandsbenachrichtigungen im Zusammenhang mit der Verfügbarkeit, die vom Gateway generiert werden. Verwenden Sie die Statistik `Sum`, um zu beobachten, ob Ereignisse im Zusammenhang mit der Verfügbarkeit im Gateway auftreten. Informationen zu den Ereignissen finden Sie in der konfigurierten CloudWatch-Protokollgruppe.

Bewährte Methoden für die Wiederherstellung Ihrer Daten

Obwohl ist es selten vorkommt, könnte in Ihrem Gateway ein Dauerfehler aufgetreten sein. Solche Fehler können in Ihrer virtuellen Maschine (VM), im Gateway selbst, dem lokalen Speicher oder an anderer Stelle auftreten. Wenn ein Fehler auftritt, empfehlen wir, dass Sie die Anweisungen im entsprechenden Abschnitt befolgen um Ihre Daten wiederherzustellen.

> **Important**
>
> Storage Gateway unterstützt keine Wiederherstellung einer Gateway-VM von einem Snapshot, die von Ihrem Hypervisor oder aus Ihrem Amazon-EC2-Computerabbild (AMI) erstellt wurde. Wenn Ihre Gateway VM, ein neues Gateway aktiviert und Ihre Daten auf diesem Gateway wiederhergestellt werden, dann folgen Sie folgenden Anweisungen.

Themen

- [Wiederherstellen von einem unerwarteten Shutdown der virtuellen Maschine](#)
- [Wiederherstellen Ihrer Daten von einer fehlerhaften Cache-Diskette](#)
- [Wiederherstellen Ihrer Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann](#)

Wiederherstellen von einem unerwarteten Shutdown der virtuellen Maschine

Wenn Ihr VM unerwartet heruntergefahren wird, z. B. während eines Stromausfalls, ist Ihr Gateway nicht mehr erreichbar. Wenn Strom- und Netzwerkverbindungen wiederhergestellt werden, wird Ihr Gateway erreichbar und beginnt normal zu funktionieren. Im Folgenden werden einige Schritte beschrieben, die Ihnen helfen können Ihre Daten wiederherzustellen:

- Wenn ein Ausfall dafür sorgt, dass Netzwerkverbindungs Problemen auftreten, dann können Sie diese Probleme beheben. Weitere Informationen zum Testen der Netzwerkverbindung finden Sie unter Testen der Netzwerkkonnektivität Ihres Gateways.
- Wenn Ihre Gateway fehlerhaft ist und Probleme mit Ihren Volumes oder Bändern auftreten und das im Zusammenhang mit einem unerwarteten Herunterfahren steht, dann können Sie Daten wiederherstellen. Weitere Informationen dazu, wie Sie Ihre Daten wiederherstellen, finden Sie in den folgenden Abschnitten, die auf Ihren Fall passen.

Wiederherstellen Ihrer Daten von einer fehlerhaften Cache-Diskette

Wenn in Ihrer Cache-Festplatte ein Fehler auftritt, empfehlen wir die folgenden Schritte zum Wiederherstellen Ihrer Daten je nach Situation, zu befolgen:

- Wenn der Fehler aufgetreten ist, weil eine Cache-Festplatte aus Ihrem Host entnommen wurde, fahren Sie das Gateway herunter, fügen Sie die Festplatte wieder ein und starten Sie das Gateway.
- Wenn der Cache-Datenträger beschädigt ist oder wenn nicht auf ihn zugegriffen werden kann, setzen Sie den Cache-Datenträger, konfigurieren Sie die Festplatte für den Cache-Speicher neu und starten Sie das Gateway neu.

Weitere Informationen hierzu finden Sie unter Wiederherstellen Ihrer Daten von einer fehlerhaften Cache-Diskette.

Wiederherstellen Ihrer Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann

Wenn auf Ihr Gateway oder Rechenzentrum aus irgendeinem Grund nicht zugegriffen werden kann, können Sie Ihre Daten in einem anderen Gateway in einem anderen Rechenzentrum oder in einem Gateway, das auf einer Amazon EC2 EC2-Instance gehostet ist, wiederherstellen. Wenn Sie keinen

Zugriff auf ein anderes Rechenzentrum haben, empfehlen wir, das Gateway auf einer Amazon EC2 EC2-Instance anzulegen. Die weiteren Schritte sind abhängig vom Gateway-Typ, von dem aus Sie die Daten wiederherstellen.

So stellen Sie Daten von einem Datei-Gateway in einem Rechenzentrum wieder her, auf das nicht zuge

Beim File-Gateway ordnen Sie dem Amazon S3 S3-Bucket eine neue Dateifreigabe zu, der die Daten enthält, die Sie wiederherstellen möchten.

1. Erstellen und aktivieren Sie ein neues Datei-Gateway auf einem Amazon EC2 EC2-Host. Weitere Informationen finden Sie unter Bereitstellen eines File Gateways auf einem Amazon EC2 EC2-Host.
2. Erstellen Sie eine neue Dateifreigabe auf dem von Ihnen erstellten EC2-Gateway. Weitere Informationen finden Sie unterErstellen Sie eine Dateifreigabeaus.
3. Mounten Sie die Dateifreigabe auf dem Client und ordnen Sie sie dem S3-Bucket zu, der die Daten enthält, die Sie wiederherstellen möchten. Weitere Informationen finden Sie unterMounten Sie und verwenden Sie Ihre Dateifreigabeaus.

Weitere Speicher-Gateway-Ressourcen

In diesem Abschnitt finden Sie Informationen überAWSsowie Software, Tools und Ressourcen von Drittanbietern, die Ihnen helfen können, Ihr Gateway einzurichten und zu verwalten, sowie auch Informationen zu Storage Gateway Gateway-Quoten.

Themen

Host-Setup

Themen

Konfigurieren von VMware für Storage Gateway

Stellen Sie beim Konfigurieren von VMware für Storage Gateway sicher, dass Sie die VM-Zeit mit der Host-Zeit synchronisieren, die VM für die Verwendung von paravirtualisierten Festplattencontrollern konfigurieren, wenn Sie Speicher bereitstellen, und Schutz vor Fehlern im Infrastruktur-Layer bereitstellen, das eine Gateway-VM unterstützt.

Themen

- Synchronisieren der VM-Zeit mit der Host-Zeit
- Verwenden von Storage Gateway mit VMware High Availability

Synchronisieren der VM-Zeit mit der Host-Zeit

Damit das Gateway erfolgreich aktiviert wird, müssen Sie sicherstellen, dass die VM-Zeit mit der Host-Zeit synchronisiert ist und dass die Host-Zeit richtig eingestellt ist. In diesem Abschnitt synchronisieren Sie zunächst die Zeit für die VM mit der Host-Zeit. Anschließend prüfen Sie die Host-Zeit. Stellen Sie dann bei Bedarf die Host-Zeit ein und konfigurieren Sie den Host so, dass die Zeit automatisch mit einem NTP-Server (Network Time Protocol) synchronisiert wird.

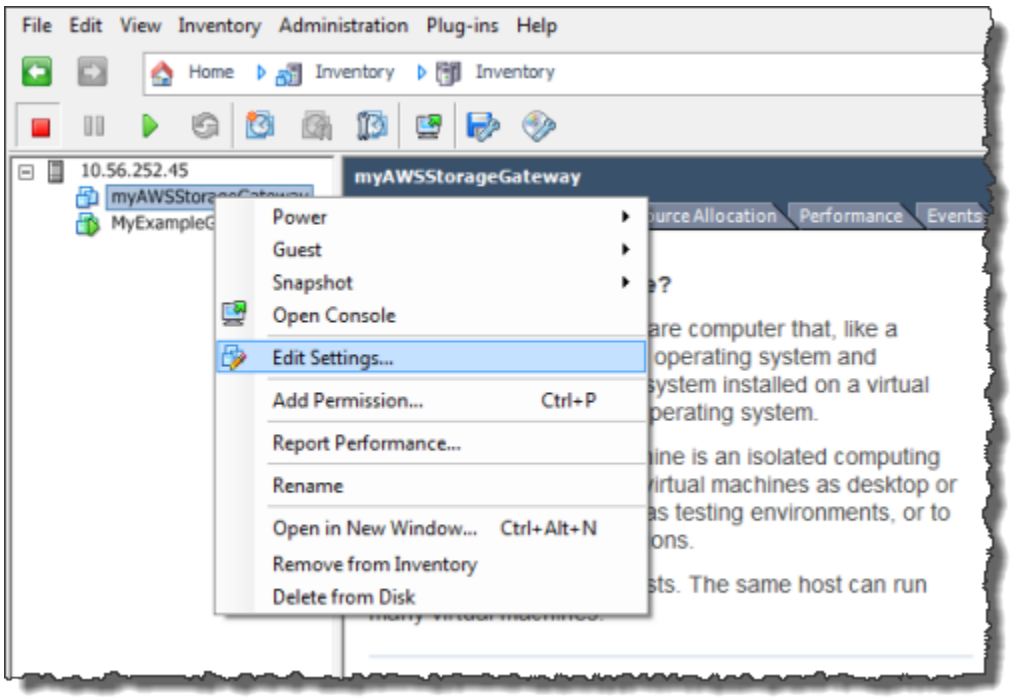
> **Important**
>
> Das Synchronisieren der VM-Zeit mit der Host-Zeit ist erforderlich, um das Gateway erfolgreich zu aktivieren.

So synchronisieren Sie die VM-Zeit mit der Host-Zeit

1. Konfigurieren Sie Ihre VM-Zeit.

    a. Öffnen Sie im vSphere-Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM und wählen Sie Edit Settings (Einstellungen bearbeiten).

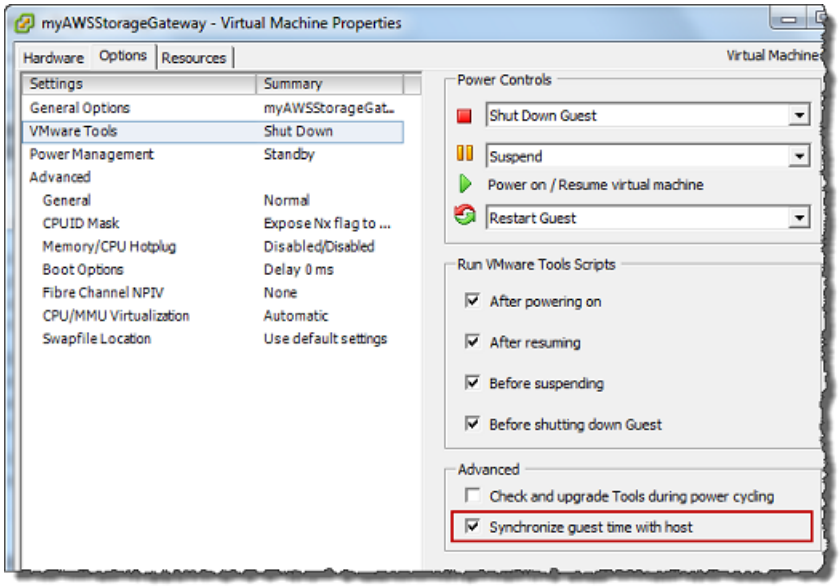
    Das Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) wird geöffnet.



b. Wählen Sie die Registerkarte Options (Optionen) und wählen Sie die Option VMware Tools (VMware-Tools) in der Optionenliste.

c. Aktivieren Sie die Option Synchronize guest time with host (Gastzeit mit Host synchronisieren) und wählen Sie dann OK.

   Die VM synchronisiert ihre Zeit mit dem Host.



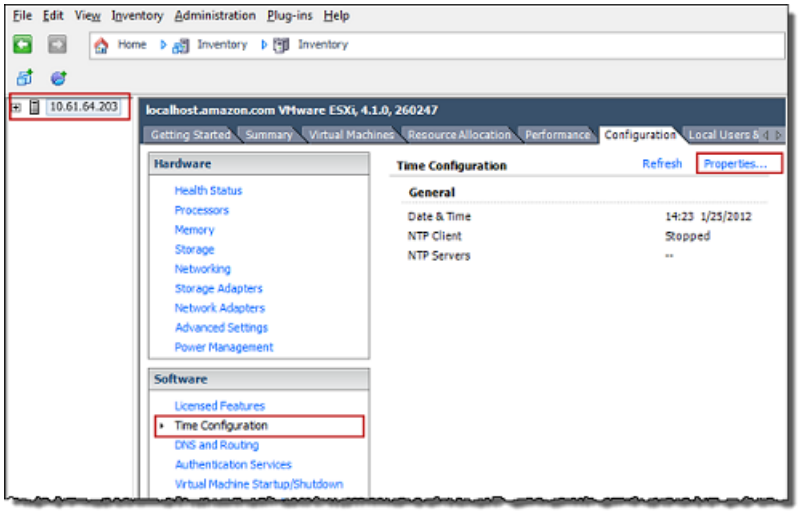
2. Konfigurieren Sie die Host-Zeit.

Es muss unbedingt sichergestellt werden, dass die Host-Uhr auf die korrekte Zeit eingestellt ist. Wenn Sie die Host-Uhr noch nicht konfiguriert haben, führen Sie die folgenden Schritte aus, um sie einzurichten und mit einem NTP-Server zu synchronisieren.

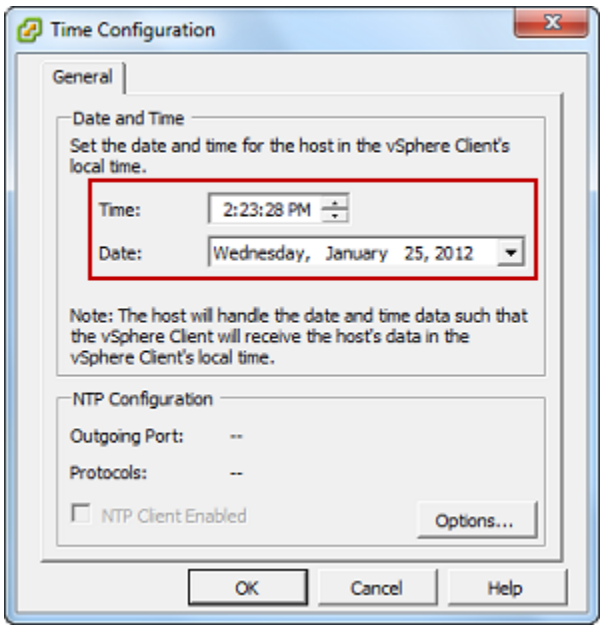
a. Wählen Sie im VMware vSphere-Client den vSphere Host-Knoten im linken Bereich und wählen Sie dann die Registerkarte Configuration (Konfiguration).

b. Wählen Sie die Option Time Configuration (Zeitkonfiguration) im Bereich Software und wählen Sie dann den Link Properties (Eigenschaften).

   Das Dialogfeld Time Configuration (Zeitkonfiguration) wird geöffnet.

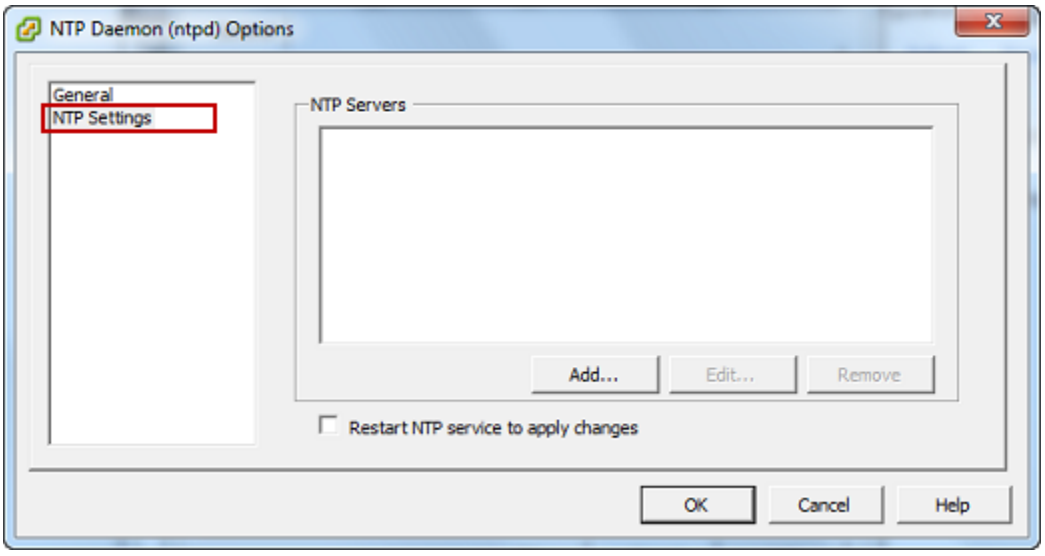


c. Legen Sie im Bereich Date and Time (Datum und Uhrzeit) das Datum und die Uhrzeit fest.



d. Konfigurieren Sie den Host so, dass seine Zeit automatisch mit einem NTP-Server synchronisiert wird.

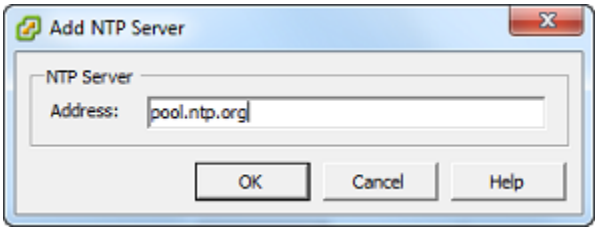
   i. Wählen Sie Options (Optionen) im Dialogfeld Time Configuration (Zeitkonfiguration) und wählen Sie dann im Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) die Option NTP Settings (NTP-Einstellungen) im linken Bereich.



   ii. Wählen Sie Add (Hinzufügen), um einen neuen NTP-Server hinzuzufügen.

   iii. Geben Sie im Dialogfeld Add NTP Server (NTP-Server hinzufügen) die IP-Adresse oder den vollqualifizierten Domänennamen eines NTP-Servers ein und wählen Sie dann OK.

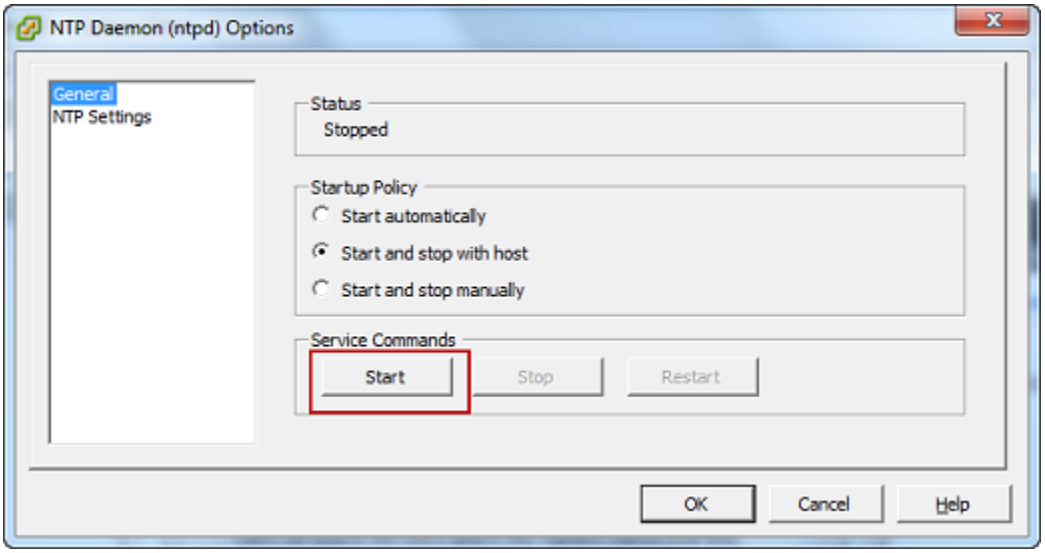
   Sie können `pool.ntp.org` verwenden, wie im folgenden Beispiel gezeigt.



iv. Wählen Sie im Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) die Option General (Allgemein) im linken Bereich.

v. Wählen Sie im Bereich Service Commands (Servicebefehle) die Option Start, um den Service zu starten.

Hinweis: Wenn Sie diese NTP-Serverreferenz ändern oder später einen anderen Server hinzufügen, müssen Sie den Service neu starten, um den neuen Server zu verwenden.



e. Wählen Sie OK, um das Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) zu schließen.

f. Wählen Sie OK, um das Dialogfeld Time Configuration (Zeitkonfiguration) zu schließen.

Verwenden von Storage Gateway mit VMware High Availability

VMware High Availability (HA) ist eine Komponente von vSphere, die Schutz vor Fehlern in der Infrastrukturebene, die eine Gateway-VM unterstützt, bieten kann. VMware HA tut dies durch die Verwendung von mehreren Hosts, die als Cluster konfiguriert sind, so dass, wenn ein Host mit einer Gateway-VM fehlschlägt, der Gateway-VM automatisch auf einem anderen Host im Cluster

neu gestartet werden kann. Weitere Informationen über VMware HA finden Sie unterVMware HA: Konzepte und bewährte Methodenauf der VMware-Website.

Um Storage Gateway mit VMware HA zu verwenden, empfehlen wir die folgenden Dinge:

- Bereitstellen des VMware ESX`.ova`herunterladbares Paket, das die Storage Gateway Gateway-VM auf nur auf einem Host in einem Cluster enthält.
- Bei der Bereitstellung des `.ova` Pakets, wählen Sie einen Datenspeicher, der sich nicht auf einem lokalen Host befindet. Verwenden Sie stattdessen einen Datenspeicher, der auf alle Hosts im Cluster zugreifen kann. Wenn Sie einen Datenspeicher auswählen, der lokal zu einem Host ist und der Host ausfällt, dann kann auf die Datenquelle möglicherweise von andere Hosts im Cluster nicht mehr zugegriffen werden und andere Hosts im Cluster und Failover zu einem anderen Host sind eventuell nicht erfolgreich.
- Mit Clustering, wenn Sie bei der Bereitstellung des `.ova` Pakets zum Cluster wählen Sie den Host, wenn Sie dazu aufgefordert werden. Alternativ können Sie direkt auf einem Host in einem Cluster bereitstellen.

Synchronisieren der Gateway-VM-Zeit

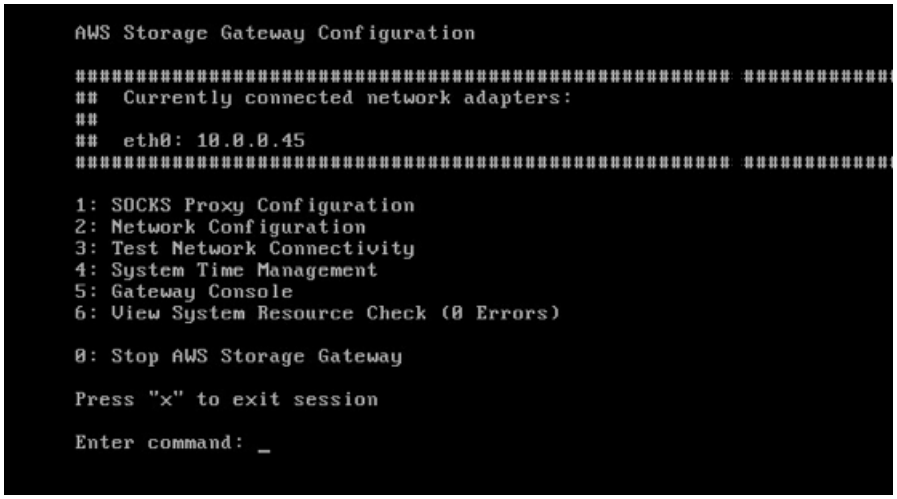
Bei einem Gateway, das auf einem VMware ESXi bereitgestellt wird, reicht es aus, die Hypervisor-Host-Zeit einzustellen und die VM-Zeit mit dem Host zu synchronisieren, um eine Abweichung zu verhindern. Weitere Informationen finden Sie unter Synchronisieren der VM-Zeit mit der Host-Zeit. Bei einem Gateway, das auf Microsoft Hyper-V bereitgestellt wird, sollten Sie die Zeit Ihrer VM regelmäßig anhand des folgenden Verfahrens prüfen.

So zeigen Sie die Zeit einer Hypervisor-Gateway-VM an und synchronisieren Sie mit der Zeit eines Network Time Protocol(NTP)-Servers

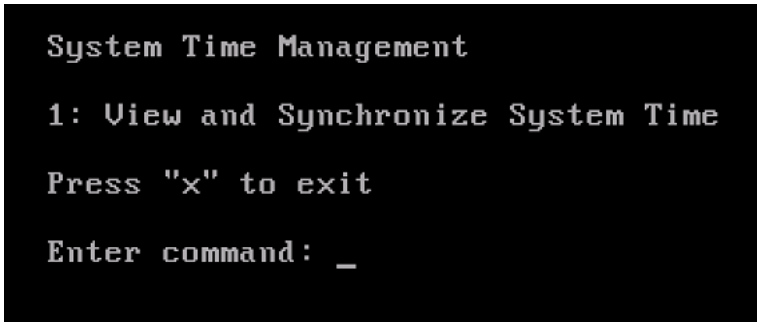
1. Melden Sie sich bei der lokalen Konsole des Gateways an:

   - Weitere Informationen zum Anmelden bei der lokalen VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zur Anmeldung bei der lokalen Konsole für die Linux Kernel-basierte virtuelle Maschine (KVM) finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.

2. Auf derStorage GatewayHauptmenü, geben Sie**4**zumSystemzeitmanagementaus.



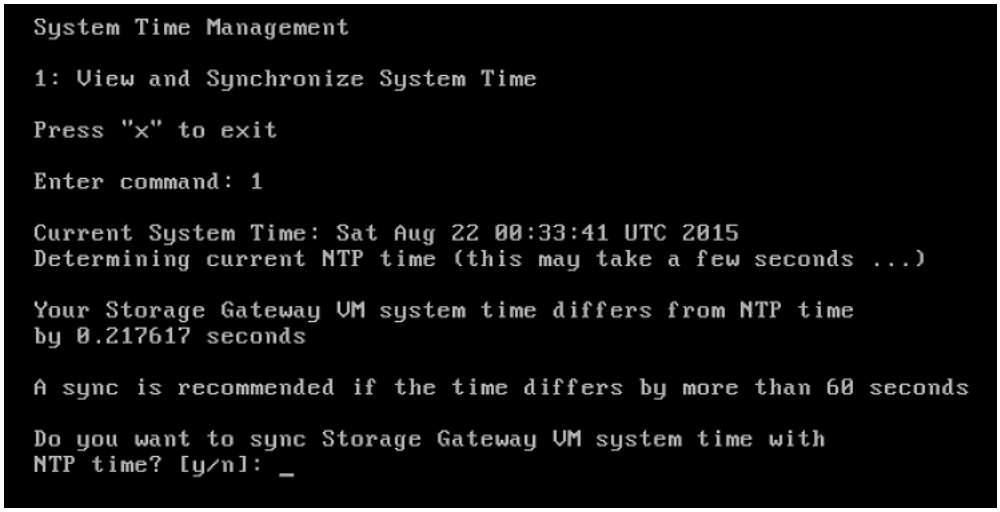
3. Geben Sie im Menü System Time Management (Systemzeit-Management) die Option **1** für View and Synchronize System Time (Systemzeit anzeigen und synchronisieren) ein.



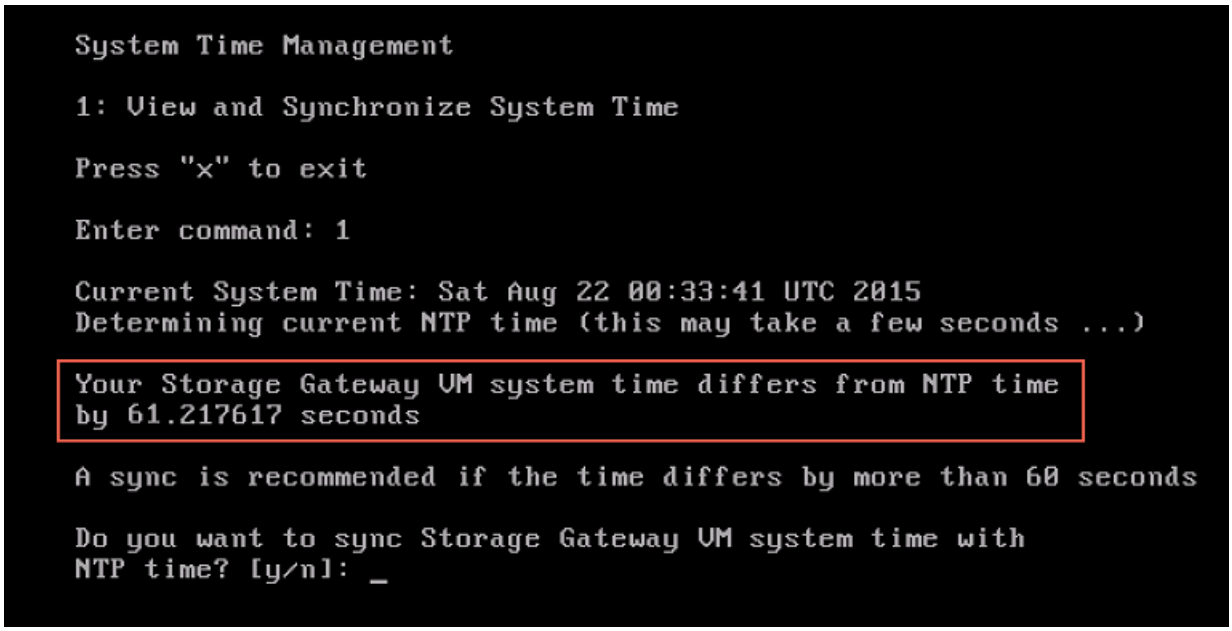
4. Wenn das Ergebnis anzeigt, dass Sie die Zeit Ihrer VM mit der Zeit des NTP synchronisieren sollten, geben Sie **y** ein. Geben Sie andernfalls **n** ein.

   Wenn Sie **y** eingeben, um zu synchronisieren, kann die Synchronisierung einige Zeit in Anspruch nehmen.

   Der folgende Screenshot zeigt eine VM, die keine Zeitsynchronisierung erfordert.



Der folgende Screenshot zeigt eine VM, die eine Zeitsynchronisierung erfordert.



Bereitstellen eines File Gateways auf einem Amazon EC2 EC2-Host

Sie können ein Datei-Gateway auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance bereitstellen und aktivieren. Das Amazon Machine Image (AMI) des File Gateways ist als Community-AMI verfügbar.

So stellen Sie ein Gateway auf einer Amazon EC2 EC2-Instance bereit

1. Wählen Sie auf der Seite Select host platform (Hostplattform auswählen) die Option Amazon EC2 aus.
2. Wählen Sie Launch instance (Instance starten) aus, um ein Storage Gateway-EC2-AMI zu starten. Sie werden zur Amazon EC2 EC2-Konsole weitergeleitet, wo Sie einen Instance-Typ auswählen können.
3. Auf derSchritt 2: Wählen eines Instance-TypsWählen Sie die Hardware-Konfiguration Ihrer Instance aus. Storage Gateway wird auf Instance-Typen unterstützt, die bestimmte Mindestanforderungen erfüllen. Wir empfehlen, mit dem Instance-Typ m4.xlarge zu beginnen, der die Mindestanforderungen erfüllt, damit das Gateway korrekt funktioniert. Weitere Informationen finden Sie unter Hardwareanforderungen für lokale VMs.

   Sie können die Größe der Instance nach dem Start bei Bedarf ändern. Weitere Informationen finden Sie unterGrößenanpassung Ihrer InstanzimAmazon EC2-Benutzerhandbuch für Linux-Instancesaus.

   > **Note**
   >
   > Bestimmte Instance-Typen, insbesondere i3 EC2, verwenden NVMe-SSD-Datenträger. Dies kann zu Problemen führen, wenn Sie das File-Gateway starten oder beenden. Beispielsweise können Sie Daten aus dem Cache verlieren. Überwachen Sie die`CachePercentDirty`Amazon CloudWatch CloudWatch-Metrik. Starten/Stoppen Sie Ihr System nur, wenn dieser Parameter lautet`0`aus. Weitere Informationen zur Überwachung von Metriken für Ihr Gateway finden Sie unterStorage Gateway Gateway-Metriken undin der CloudWatch-Dokumentation. Weitere Informationen zu den Anforderungen von Amazon EC2 Instance-Typen finden Sie unterthe section called “Anforderungen für Amazon EC2 EC2-Instance-Typen”aus.
4. Wählen Sie Weiter. Konfigurieren von Instance-Detailsaus.
5. Auf derSchritt 3: Konfigurieren von Instance-DetailsKlicken Sie auf, wählen Sie einen Wert fürAuto-assign Public IPaus. Wenn Ihre Instance über das öffentliche Internet verfügbar sein soll, müssen Sie Auto-assign Public IP (Öffentliche IP automatisch zuweisen) auf Enable (Aktivieren) festlegen. Wenn Ihre Instance nicht über das Internet verfügbar sein soll, müssen Sie Auto-assign Public IP (Öffentliche IP automatisch zuweisen) auf Disable (Deaktivieren) festlegen.
6. FürIAM-Rolle, wähle dasAWS Identity and Access Management(IAM) -Rolle, die Sie für Ihr Gateway verwenden möchten.

7. Wählen Sie Weiter. Hinzufügen von Speicheraus.
8. Auf derSchritt 4: Hinzufügen von Speicher-Seite, wählen SieNeues Volume hinzufügenum der Datei-Gateway-Instance Speicher hinzuzufügen. Sie benötigen mindestens ein Amazon EBS-Volume, um für Cache-Speicher zu konfigurieren.

   Empfohlene Festplattengröße: Cache (Minimum) 150 GiB und Cache (Maximum) 64 TiB
9. Auf derSchritt 5: Tags hinzufügen-Seite können Sie Ihrer Instance ein optionales Tag hinzufügen. Klicken Sie dann auf Next (Weiter): Konfigurieren der Sicherheitsgruppeaus.
10. Auf derSchritt 6: Konfigurieren der SicherheitsgruppeFügen Sie Firewall-Regeln für spezifischen Datenverkehr hinzu, um die Instance zu erreichen. Sie können eine neue Sicherheitsgruppe erstellen oder eine vorhandene Sicherheitsgruppe auswählen.

    > **Important**
    >
    > Neben Storage Gateway Gateway-Aktivierung und Secure Shell (SSH) -Zugriffsports benötigen NFS-Clients Zugriff auf weitere Ports. Weitere Informationen hierzu finden Sie unter Netzwerk- und Firewall-Anforderungen.
11. Wählen Sie Review and Launch (Prüfen und starten) aus, um die Konfiguration zu prüfen.
12. Auf derSchritt 7: Überprüfen des Instance-Starts-Seite, wählen Siestartenaus.
13. Wählen Sie im Dialogfeld Select an existing key pair or create a new key pair (Vorhandenes Schlüsselpaar auswählen oder neues Schlüsselpaar erstellen) die Option Choose an existing key pair (Vorhandenes Schlüsselpaar auswählen) und das während der Einrichtung von Ihnen erstellte Schlüsselpaar aus. Wenn Sie bereit sind, aktivieren Sie das Bestätigungs-Kontrollkästchen und wählen dann Launch Instances (Instances starten) aus.

    Eine Bestätigungsseite informiert Sie darüber, dass Ihre Instance gestartet wird.
14. Wählen Sie View Instances aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren. Auf dem Bildschirm Instances können Sie den Status der Instance anzeigen. Es dauert einige Zeit, bis die Instance startet. Wenn Sie eine Instance starten, ist der anfängliche Status pending (ausstehend). Nachdem die Instance gestartet wurde, ist der Status running (wird ausgeführt). Sie erhält einen öffentlichen DNS-Namen.
15. Wählen Sie Ihre Instance aus, notieren Sie sich die öffentliche IP-Adresse imBeschreibungTag, und kehren Sie zumVerbinden mitAWSin der Storage Gateway Gateway-Konsole, um Ihre Gateway-Setup fortzusetzen.

Sie können die AMI-ID bestimmen, die zum Starten eines Datei-Gateways verwendet werden soll, indem Sie die Storage Gateway Gateway-Konsole oder dieAWS Systems ManagerParameterspeicher aktiviert.

So ermitteln Sie die AMI-ID:

1. Melden Sie sich bei derAWS Management Consoleund öffnen Sie die Storage Gateway Gateway-Konsole unterhttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie Create gateway (Gateway erstellen), File gateway (Datei-Gateway) und dann Next (Weiter).
3. Wählen Sie auf der Seite Choose host platform (Hostplattform wählen) die Option Amazon EC2 aus.
4. Klicken Sie aufStarten der Instanceum ein Storage Gateway EC2-AMI zu starten. Sie werden zur Community-AMI-Seite von EC2 weitergeleitet, auf der Sie die AMI-ID für Ihre sehen könnenAWSRegion in der URL.

   Oder Sie können den Parameterspeicher von Systems Manager abfragen. Sie können dasAWS CLIoder Storage Gateway Gateway-API zum Abfragen des öffentlichen Parameters von Systems Manager unter dem Namespace`/aws/service/storagegateway/ami/FILE_S3/latest`aus. Mit dem folgenden CLI-Befehl wird beispielsweise die ID des aktuellen AMI im aktuellenAWSRegion :

   ```
   aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
   FILE_S3/latest
   ```

   Dieser CLI-Befehl gibt etwa die folgende Ausgabe zurück:

   ```
   {
       "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"
       }
   }
   ```

Abrufen eines Aktivierungsschlüssels für das Gateway

Um einen Aktivierungsschlüssel für das Gateway abzurufen, richten Sie eine Web-Anforderung an die Gateway-VM. Diese gibt eine Umleitung zurück, die den Aktivierungsschlüssel enthält. Dieser Aktivierungsschlüssel wird als einer der Parameter an die API-Aktion `ActivateGateway` übergeben, um die Konfiguration des Gateways anzugeben. Weitere Informationen finden Sie unterActivateGatewayimStorage Gateway Gateway-APIaus.

Die Anforderung, die Sie an die Gateway-VM richten, enthältAWSRegion, in der die Aktivierung stattfindet. Die von der Umleitung in der Antwort zurückgegebene URL enthält einen Abfragezeichenfolgenparameter namens `activationkey`. Dieser Abfragezeichenfolge-Parameter ist Ihr Aktivierungsschlüssel. Das Format der Abfragezeichenfolge: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*.

Themen

- AWS CLI
- Linux (bash/zsh)
- Microsoft Windows PowerShell

AWS CLI

Wenn Sie es noch nicht getan haben, müssen Sie AWS CLI installieren und konfigurieren. Befolgen Sie hierzu die Anweisungen im AWS Command Line Interface Benutzerhandbuch:

- Installieren vonAWS Command Line Interface
- Konfigurieren vonAWS Command Line Interface

Das folgende Beispiel zeigt, wie Sie dasAWS CLIUm die HTTP-Antwort abzurufen, analysieren Sie die HTTP-Header und rufen Sie den Aktivierungsschlüssel ab.

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

Linux (bash/zsh)

Das folgende Beispiel zeigt, wie Sie mit Linux (bash/zsh) die HTTP-Antwort abfangen, HTTP-Header analysieren und den Aktivierungsschlüssel abrufen.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

Das folgende Beispiel zeigt, wie Sie mit Microsoft Windows PowerShell die HTTP-Antwort abrufen, die HTTP-Header analysieren und den Aktivierungsschlüssel abrufen.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

benutzenAWS Direct Connectmit Storage Gateway

AWS Direct Connectverknüpft Ihr internes Netzwerk mit der Amazon Web Services Cloud. Durch Verwendung vonAWS Direct ConnectMit Storage Gateway können Sie eine Verbindung für den Bedarf bei Workload mit hohem Durchsatz erstellen und eine dedizierte Netzwerkverbindung zwischen dem Gateway vor Ort undAWSaus.

Storage Gateway verwendet öffentliche Endpunkte. Mit einemAWS Direct Connect-Verbindung eingerichtet, können Sie eine öffentliche virtuelle Schnittstelle erstellen, um Datenverkehr an die Storage Gateway Gateway-Endpunkte weiterzuleiten. Die öffentliche virtuelle Schnittstelle umgeht Internetdienstanbieter in Ihrem Netzwerkpfad. Der öffentliche Endpunkt des Storage Gateway Gateway-Dienstes kann sich im selben befindenAWSRegion alsAWS Direct ConnectOrt, oder es kann in einem anderen seinAWSRegion :

Die folgende Abbildung zeigt ein Beispiel fürAWS Direct Connectarbeitet mit Storage Gateway.

In der folgenden Vorgehensweise wird davon ausgegangen, dass Sie bereits ein funktionsfähiges Gateway erstellt haben.

Um zu verwendenAWS Direct Connectmit Storage Gateway

1. Erstellen und etablieren Sie eineAWS Direct ConnectVerbindung zwischen Ihrem lokalen Rechenzentrum und Ihrem Storage Gateway Gateway-Endpunkt. Weitere Informationen zum Herstellen einer Verbindung finden Sie unterErste Schritte mitAWS Direct ConnectimAWS Direct Connect-Benutzerhandbuch.
2. Connect Sie Ihre lokale Storage Gateway Gateway-Appliance mitAWS Direct ConnectRouter.
3. Erstellen Sie eine öffentliche virtuelle Schnittstelle und konfigurieren Sie Ihren lokalen Router entsprechend. Weitere Informationen finden Sie unterErstellen einer virtuellen SchnittstelleimAWS Direct Connect-Benutzerhandbuch.

Weitere Informationen überAWS Direct Connectfinden Sie unterWas ist ?AWS Direct Connect?imAWS Direct Connect-Benutzerhandbuchaus.

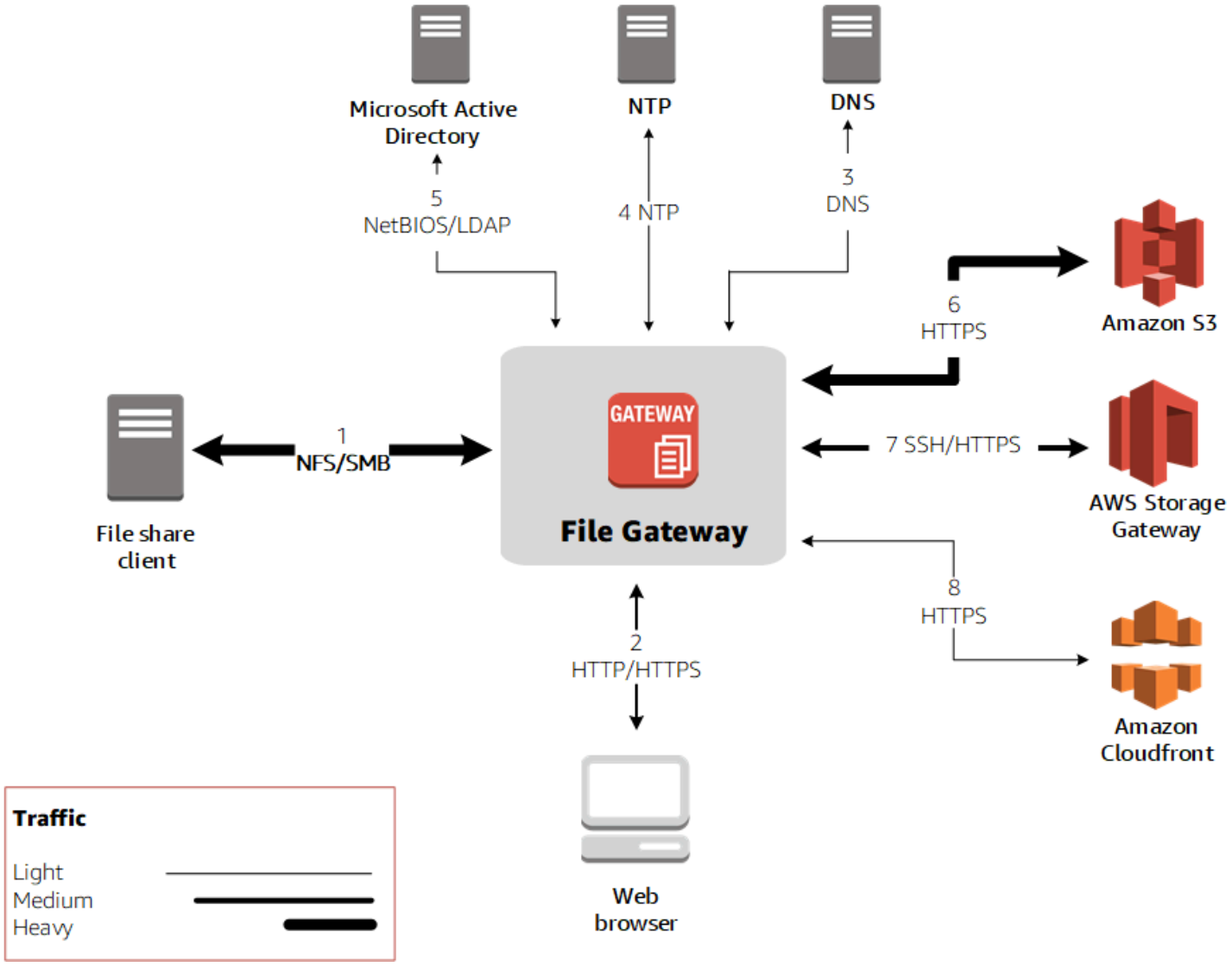
Port-Anforderungen

Für Storage Gateway sind die nachfolgend aufgeführten Ports erforderlich. Einige Ports werden von allen Gateway-Typen verwendet und sind für alle Gateway-Typen erforderlich. Andere Ports

werden für bestimmte Gateway-Typen benötigt. In diesem Abschnitt finden Sie eine Abbildung der erforderlichen Ports und eine Liste der von jedem Gateway-Typ benötigten Ports.

File Gateways

Die folgende Abbildung zeigt die Ports, die für die Operation von Datei-Gateways offen sein müssen.



Die folgenden Ports werden von allen Gateway-Typen verwendet und sind für alle Gateway-Typen erforderlich.

Aus	Bis	Protocol (Protokoll)	Port	Verwendung	
Storage Gateway	Amazon Web Services	Transmission Control Protocol (TCP)	443 (HTTPS)	Für die Kommunikation von einer Storage Gateway Gateway-VM mit einemAWSService-Endpunkt. Informationen über Service-Endpunkte finden Sie unter Gewähren von Zugriff über Firewalls und Router für AWS Storage Gateway.	
Ihr Webbrowser	Storage Gateway	TCP	80 (HTTP)	Rufen Sie durch lokale Systeme den Storage Gateway Gateway-Aktivierungsschlüssel ab. Port 80 wird nur	

Aus	Bis	Protocol (Protokoll)	Port	Verwendung	
				während der Aktivierung einer Storage Gateway Gateway-Appliance verwendet. Für eine Storage Gateway Gateway-VM ist es nicht erforderlich, dass Port 80 öffentlich zugänglich ist. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie das Gateway von der Storage Gateway Management Console aus aktivieren, muss der	

Aus	Bis	Protocol (Protokoll)	Port	Verwendung	
				Host, von dem aus Sie die Verbindung mit der Konsole herstellen, Zugriff auf Port 80 Ihres Gateways haben.	
Storage Gateway	Domain Name Service (DNS)-Server	User Datagram Protocol (UDP)/UDP	53 (DNS)	Für die Kommunikation zwischen einer Storage Gateway Gateway-VM und dem DNS-Server	

Aus	Bis	Protocol (Protokoll)	Port	Verwendung	
Storage Gateway	Amazon Web Services	TCP	22 (Support-Kanal)	Ermöglicht Amazon Web Services Support den Zugriff auf das Gateway, um Ihnen bei der Lösung von Gateway-Problemen zu helfen. Dieser Port muss für den normalen Betrieb des Gateways nicht offen sein, für die Fehlerbehebung ist dies jedoch erforderlich.	

Aus	Bis	Protocol (Protokoll)	Port	Verwendung	
Storage Gateway	Network Time Protocol (NTP)-Server	UDP	123 (NTP)	Verwendet von lokalen Systemen zur Synchronisierung der VM-Zeit mit der Host-Zeit. Eine Storage Gateway Gateway-VM ist so konfiguriert, dass die folgenden NTP-Server verwendet werden: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org	

Aus	Bis	Protocol (Protokoll)	Port	Verwendung	
Storage Gateway-Hardware-Appliance	Hypertext Transfer Protocol (HTTP)-Proxy	TCP	8080 (HTTP)	Für die Aktivierung kurz erforderlich.	

Die folgende Tabelle führt die erforderlichen Ports auf, die für ein File Gateway unter Verwendung des Network File System (NFS)- oder Server Message Block (SMB)-Protokolls geöffnet sein müssen. Diese Portregeln sind Teil der Sicherheitsgruppendefinition.

Re	Netzwerkelement	Dateifreigabetyp	Protocol (Protokoll)	Port	Einge	Ausge	Erforde ich?	Hinweise
1	Dateifreigabe-Client	NFS	TCP/UDP-Daten	111	✓	✓	✓	Dateifreigabe für die Datenübertragung (nur NFS)
			TCP/UDP NFS	2049	✓	✓	✓	Dateifreigabe für die Datenübertragung (nur NFS)
			TCP/UDP NFSv3	2004	✓	✓	✓	Dateifreigabe für die Datenübertragung (nur NFS)
		SMB	TCP/UDP SMBv2	139	✓	✓	✓	Der Service für die Datenübertragungssitzung der Dateifreigabe (nur SMB); ersetzt Ports 137 bis 139 für Microsoft Windows NT und höher

Re	Netzwerkelement	Dateifreigabetyp	Protocol (Protokoll)	Port	Einge	Ausge	Erforde ich?	Hinweise
			TCP/UDP SMBv3	445	✓	✓	✓	Der Service für die Datenübertragungssitzung der Dateifreigabe (nur SMB); ersetzt Ports 137 bis 139 für Microsoft Windows NT und höher
2	Webbrowser	NFS und SMB	TCP HTTP	80	✓	✓	✓	Amazon Web Services Management Console (nur Aktivierung)
			TCP HTTPS	443	✓	✓	✓	Amazon Web Services Management Console (alle anderen Operationen)
3	DNS	NFS und SMB	TCP/UDP DNS	53	✓	✓	✓	IP-Namensauflösung
4	NTP	NFS und SMB	UDP NTP	123	✓	✓	✓	Zeitsynchronisierungsservice
5	Microsoft Active Directory	SMB	UDP NetBIOS	137	✓	✓	✓	Name Service (nicht für NFS)
			UDP NetBIOS	138	✓	✓	✓	Datagram Service

Re	Netzwerkelement	Dateifreigabetyp	Protocol (Protokoll)	Port	Einge	Ausge	Erforde ich?	Hinweise
			TCP LDAP	389	✓	✓		Directory System Agent (DSA); Client-Verbindung
			TCP LDAPS	636	✓	✓		LDAPS — Lightweight Directory Access Protocol (LDAP) über Secure Socket Layer (SSL)
6	Amazon S3	NFS und SMB	HTTPS-Daten	443	✓	✓	✓	Speicherdatenübertragung
7	Storage Gateway	NFS und SMB	TCP SSH	22	✓	✓	✓	Support-Kanal
			TCP HTTPS	443	✓	✓	✓	Managementkontrolle
8	Amazon CloudFront	NFS und SMB	TCP HTTPS	443	✓	✓	✓	Zur Aktivierung

Herstellen einer Verbindung mit einem Gateway

Nachdem Sie einen Host ausgewählt und eine Gateway-VM bereitgestellt haben, verbinden und aktivieren Sie das Gateway. Hierzu benötigen Sie die IP-Adresse der Gateway-VM. Rufen Sie die IP-Adresse von der lokalen Konsole des Gateways ab. Sie melden sich bei der lokalen Konsole an und rufen die IP-Adresse im oberen Bereich der Konsole ab.

Für lokal bereitgestellte Gateways können Sie auch die IP-Adresse vom Hypervisor abrufen. Für Amazon EC2 Gateways können Sie auch die IP-Adresse der Amazon EC2 Instance in der Amazon EC2 -Management-Konsole abrufen. Informationen zum Abrufen der IP-Adresse des Gateways finden unter:

- VMware-Host: Zugreifen auf die lokale Konsole mit VMware ESXi
- Hyper-V-Host: Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V
- Linux Kernel-basierte virtuelle Maschine (KVM)-Host: Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
- EC2-Host: Abrufen einer IP-Adresse von einem Amazon EC2 EC2-Host

Wenn Sie die IP-Adresse gefunden haben, notieren Sie sie. Kehren Sie dann zur Storage Gateway Gateway-Konsole zurück und geben Sie die IP-Adresse in der Konsole ein.

Abrufen einer IP-Adresse von einem Amazon EC2 EC2-Host

Um die IP-Adresse der Amazon EC2 EC2-Instance abzurufen, auf der das Gateway bereitgestellt wird, melden Sie sich bei der EC2-Instance auf der lokalen Konsole an. Rufen Sie dann die IP-Adresse am oberen Rand der Konsolenseite ab. Anweisungen finden Sie unter .

Sie können auch die IP-Adresse aus der Amazon EC2 -Management-Konsole abrufen. Wir empfehlen die Verwendung einer öffentlichen IP-Adresse für die Aktivierung. Verwenden Sie Verfahren 1, um die öffentliche IP-Adresse abzurufen. Wenn Sie die Elastic IP-Adresse verwenden möchten, gehen Sie wie unter Vorgehensweise 2 beschrieben vor.

Prozedur 1: So stellen Sie eine Verbindung mit dem Gateway über die öffentliche IP-Adresse her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances (Instances) und dann die EC2-Instance aus, auf der Ihr Gateway bereitgestellt wurde.
3. Wählen Sie unten die Registerkarte Description (Beschreibung) aus und notieren Sie die öffentliche IP-Adresse. Mit dieser IP-Adresse stellen Sie eine Verbindung zum Gateway her. Kehren Sie zur Storage Gateway Gateway-Konsole zurück und geben Sie die IP-Adresse ein.

Wenn Sie die Elastic IP-Adresse für die Aktivierung verwenden möchten, gehen Sie wie folgt vor.

Prozedur 2: So stellen Sie eine Verbindung mit dem Gateway über die Elastic IP-Adresse her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances (Instances) und dann die EC2-Instance aus, auf der Ihr Gateway bereitgestellt wurde.

3. Wählen Sie unten die Registerkarte Description (Beschreibung) aus und notieren Sie den Wert für Elastic IP (Elastische IP). Mit der Elastic IP-Adresse stellen Sie eine Verbindung zum Gateway her. Kehren Sie zur Storage Gateway Gateway-Konsole zurück und geben Sie die Elastic IP-Adresse ein.
4. Nachdem Ihr Gateway aktiviert wurde, wählen Sie das Gateway aus, das Sie gerade aktiviert haben, und dann die Registerkarte VTL devices (VTL-Geräte) im unteren Bereich aus.
5. Rufen Sie die Namen aller VTL-Geräte ab.
6. Führen Sie für jedes Ziel den folgenden Befehl aus, um das Ziel zu konfigurieren.

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```
7. Führen Sie für jedes Ziel den folgenden Befehl aus, um sich anzumelden.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   Ihr Gateway ist jetzt mit der Elastic IP-Adresse der EC2 Instance verbunden.

Grundlegendes zu Storage Gateway Gateway-Ressourcen und

In Storage Gateway ist die primäre RessourceTorZu den anderen Ressourcentypen gehören jedoch:Volumen,virtuelles Band,iSCSI-Ziel, undvtl Gerätaus. Diese werden als Subressourcen bezeichnet und existieren nur, wenn sie mit einem Gateway verknüpft sind.

Diesen Ressourcen und Unterressourcen sind eindeutige Amazon-Ressourcennamen (ARN) zugeordnet, wie in der folgenden Tabelle zu sehen ist.

Ressourcentyp	ARN-Format
Gateway-ARN	`arn:aws:storagegateway:` *region*`:`*account-id* `:gateway/` *gateway-id*
Dateifreigaben-ARN	`arn:aws:storagegateway:` *region*`:`*account-id* `:share/`*share-id*
Volume-ARN	`arn:aws:storagegateway:` *region*`:`*account-id* `:gateway/` *gateway-id* `/volume/`*volume-id*

Ressource ntyp	ARN-Format
Band-ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:tape/`*`tapebarcode`*
Ziel-ARN (iSCSI-Ziel)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*
VTL-Geräte-ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/device/`*`vtldevice`*

Storage Gateway unterstützt auch die Verwendung von EC2 Instances sowie EBS-Volumes und -Snapshots. Diese Ressourcen sind Amazon EC2 EC2-Ressourcen, die in Storage Gateway verwendet werden.

Arbeiten mit Ressourcen-IDs

Wenn Sie eine Ressource erstellen, weist Storage Gateway der Ressource eine eindeutige Ressourcen-ID zu. Diese Ressourcen-ID ist Teil des Ressourcen-ARN. Eine Ressourcen-ID besteht aus einer Ressourcenkennung, gefolgt von einem Bindestrich und einer eindeutigen Kombination aus acht Buchstaben und Zahlen. Eine Gateway-ID beispielsweise hat die Form `sgw-12A3456B`, wobei `sgw` die Ressourcenkennung für Gateways ist. Ein Volume-ID hat die Form `vol-3344CCDD`, wobei `vol` die Ressourcenkennung für Volumes ist.

Bei virtuellen Bändern können Sie der Barcode-ID ein Präfix von bis zu vier Zeichen voranstellen, um Ihre Bänder zu organisieren.

Storage Gateway Gateway-Ressourcen-IDs sind in Großbuchstaben. Wenn Sie allerdings diese Ressourcen-IDs mit der Amazon EC2 -API verwenden, erwartet Amazon EC2 Ressourcen-IDs in Kleinbuchstaben. Sie müssen Ihre Ressourcen-ID in Kleinbuchstaben ändern, um Sie mit der EC2-API verwenden zu können. Bei einem Storage Gateway beispielsweise könnte die ID für ein Volume `vol-1122AABB` lauten. Wenn Sie diese ID mit der EC2-API verwenden, müssen Sie sie zu `vol-1122aabb` ändern. Andernfalls verhält sich die EC2-API möglicherweise nicht wie erwartet.

> **Important**
>
> IDs für Storage Gateway Gateway-Volumes und Amazon EBS-Snapshots, die aus Gateway-Volumes erstellt wurden, werden zu einem längeren Ab Dezember 2016 werden alle neuen

Volumes und Snapshots mit einer 17-stelligen Zeichenfolge erstellt. Ab April 2016 können Sie diese längeren IDs verwenden, um Ihre Systeme mit dem neuen Format zu testen. Weitere Informationen finden Sie unter Längere EC2- und EBS-Ressourcen-IDS.
Beispielsweise sieht ein Volume-ARN mit dem längeren Volume-ID-Format wie folgt aus: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
Eine Snapshot-ID mit dem längeren ID-Format sieht so aus: `snap-78e226633445566ee`.
Weitere Informationen finden Sie unterAnkündigung: Heads-Up — Längere Storage Gateway Gateway-Volume und Snapshots werden 2016 bereitgestelltaus.

Markieren von Storage Gateway-

In Storage Gateway können Sie Tags verwenden, um Ihre Ressourcen zu verwalten. Mit Tags können Sie den Ressourcen Metadaten hinzufügen und sie so kategorisieren, das sie einfacher zu verwalten sind. Jedes Tag besteht aus einem Schlüssel-Wert-Paar, das Sie definieren. Sie können Tags zu Gateways, Volumes und virtuellen Bändern hinzufügen. Sie können diese Ressourcen auf der Grundlage der hinzugefügten Tags filtern und danach suchen.

Beispielsweise können Sie Tags verwenden, um zu erkennen, von welcher Abteilung -Ressourcen in Ihrer Organisation verwendet werden. Sie können Gateways und Volumes kennzeichnen, die von der Buchhaltungsabteilung verwendet werden, z. B.: (`key=department` und `value=accounting`). Anschließend können Sie nach diesen Tags filtern und alle Gateways und Volumes erkennen, die von der Buchhaltungsabteilung verwendet werden. Anhand dieser Informationen können Sie die Kosten bestimmen. Weitere Informationen finden Sie unter Verwenden von Kostenzuweisungs-Tags und Arbeiten mit dem Tag-Editor.

Wenn Sie ein virtuelles Band archivieren, das gekennzeichnet ist, behält das Band die Tags auch im Archiv. Wenn Sie dann ein Band aus dem Archiv auf ein anderes Gateway abrufen, bleiben die Tags auch im neuen Gateway erhalten.

Für das Datei-Gateway können Sie mithilfe von Tags den Zugriff auf Ressourcen bestimmen. Weitere Informationen über die entsprechende Vorgehensweise finden Sie unter Verwenden von Tags zur Steuerung des Zugriffs auf Ihr Gateway und Ihre -Ressourcen.

Tags haben keine semantische Bedeutung, sondern werden als Zeichenfolgen interpretiert.

Für Tags gelten die folgenden Einschränkungen:

- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Die maximale Anzahl von Tags pro Ressource beträgt 50.
- Tags dürfen nicht mit `aws:` beginnen. Dieses Präfix ist reserviert fürAWSVerwendung von.
- Gültige Zeichen der Schlüsseleigenschaft sind UTF-8-Buchstaben und Zahlen, Leerzeichen und die Sonderzeichen + - = . _ : / und @.

Arbeiten mit Tags

Sie können mit Tags arbeiten, indem Sie die Storage Gateway Gateway-Konsole, die Storage Gateway Gateway-API oder die-Speicher-Gateway-Befehlszeilenschnittstelle (CLI)aus. Das folgende Verfahren zeigt, wie Sie ein Tag in der Konsole hinzufügen, bearbeiten und löschen.

So fügen Sie ein Tag hinzu

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie im Navigationsbereich die Ressource, die Sie kennzeichnen möchten.

   Wenn Sie z. B. ein Gateway mit Tags versehen möchten, wählen Sie Gateways und wählen Sie dann das Gateway, das Sie kennzeichnen möchten, aus der Liste der Gateways aus.
3. Wählen Sie Tagsund dann Add/edit tags (Tags hinzufügen/bearbeiten).
4. Wählen Sie im Dialogfeld Add/edit tags (Tags hinzufügen/bearbeiten) die Option Create tag (Tag erstellen).
5. Geben Sie einen Schlüssel für Key (Schlüssel) und einen Wert für Value (Wert) ein. Beispielsweise können Sie **`Department`** für den Schlüssel und **`Accounting`** für den Wert eingeben.

   > **Note**
   >
   > Sie können das Feld Value (Wert) auch leer lassen.

6. Wählen Sie Create Tag (Tag erstellen), um weitere Tags hinzuzufügen. Sie können einer Ressource mehrere Tags hinzufügen.
7. Wenn Sie alle Tags hinzugefügt haben, wählen Sie Save (Speichern).

So bearbeiten Sie ein Tag

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie die Ressource aus, deren Tag Sie bearbeiten möchten.
3. Wählen Sie Tags, um das Dialogfeld Add/edit tags (Tags hinzufügen/bearbeiten) zu öffnen.
4. Wählen Sie das Bleistiftsymbol neben dem Tag aus, das Sie bearbeiten möchten, und bearbeiten Sie dann das Tag.
5. Wenn Sie das Tag bearbeitet haben, wählen Sie Save (Speichern).

So löschen Sie ein Tag

1. Öffnen Sie die Storage Gateway Gateway-Konsolehttps://console.aws.amazon.com/storagegateway/homeaus.
2. Wählen Sie die Ressource aus, deren Tag Sie löschen möchten.
3. Wählen Sie Tags und dann Add/edit tags (Tags hinzufügen/bearbeiten), um das Dialogfeld Add/edit tags (Tags hinzufügen/bearbeiten) zu öffnen.
4. Wählen Sie das Symbol X neben dem Tag, das Sie löschen möchten, und wählen Sie dann Save (Speichern).

Weitere Informationen finden Sie auch unter

Verwenden von Tags zur Steuerung des Zugriffs auf Ihr Gateway und Ihre -Ressourcen

Arbeiten mit Open-Source-Komponenten fürAWS Storage Gateway

In diesem Abschnitt finden Sie Informationen zu Tools und Lizenzen von Drittanbietern, die für die Bereitstellung von Storage Gateway Gateway-Funktionen angewiesen sind.

Themen

- Open-Source-Komponenten für Storage Gateway
- Open-Source-Komponenten für Amazon S3 File Gateway

Open-Source-Komponenten für Storage Gateway

Mehrere Tools und Lizenzen von Drittanbietern werden verwendet, um Funktionen für Volume Gateway, Band-Gateway und Amazon S3 File Gateway bereitzustellen.

Verwenden Sie die folgenden Links, um Quellcode für bestimmte Open-Source-Softwarekomponenten herunterzuladen, die in enthalten sindAWS Storage GatewaySoftware:

- Für auf VMware ESXi bereitgestellte Gatewayssources.tar
- Für auf Microsoft Hyper-V bereitgestellte Gatewayssources_hyperv.tar
- Für Gateways, die auf einer Linux Kernel-basierten virtuellen Maschine (KVM) bereitgestellt werden:sources_KVM.tar

Dieses Produkt enthält Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL-Toolkit (http://www.openssl.org/) enthalten. Die entsprechenden Lizenzen für alle abhängigen Drittanbieter-Tools finden Sie unterDrittanbieterlizenzenaus.

Open-Source-Komponenten für Amazon S3 File Gateway

Mehrere Tools und Lizenzen von Drittanbietern werden verwendet, um die Funktionen von Amazon S3 File Gateway (S3 File Gateway) bereitzustellen.

Verwenden Sie die folgenden Links, um den Quellcode einiger der in der S3 File Gateway-Software enthaltenen Open-Source-Softwarekomponenten herunterzuladen:

- Für Amazon S3 File Gateway:sgw-Datei-s3-Open-Source-.tgz

Dieses Produkt enthält Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL-Toolkit (http://www.openssl.org/) enthalten. Die entsprechenden Lizenzen für alle abhängigen Drittanbieter-Tools finden Sie unterDrittanbieterlizenzenaus.

Kontingente

Kontingente für Dateifreigaben

In der folgenden Tabelle sind Kontingente für Dateifreigaben aufgeführt.

Description	File Gateway
Maximale Anzahl von Dateifreigaben pro Amazon S3 -Bucket. (Zwischen Dateifreigaben und S3-Buckets besteht jeweils eine 1-zu-1-Zu weisung.)	1
Maximale Anzahl von Dateifreigaben pro Gateway	10
Maximalgröße pro Einzeldatei (gleich Maximalgröße eines Einzelobjekts in Amazon S3) **Note** Wenn Sie eine Datei schreiben, die größer als 5 TB ist, wird die Fehlermel dung angezeigt, dass die Datei zu groß ist. Dann werden nur die ersten 5 TB der Datei hochgeladen.	5 TB
Maximale Pfadlänge **Note** Clients dürfen keinen Pfad erstellen , der diese Länge überschreitet. Dies würde zu einem Fehler führen. Diese Limits gelten für beide von File Gateways unterstützten Protokolle, NFS und SMB.	1024 Bytes

Empfohlene lokale Festplattengrößen für Ihr Gateway

In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt.

Gateway-Typ	Cache (Minimum)	Cache (Maximum)	Andere erforderliche lokale Festplatten
S3-Datei-Gateway	150 GiB	64 TiB	—

> **Note**
>
> Sie können ein oder mehrere lokale Laufwerke für Ihren Cache bis zur maximalen Kapazität konfigurieren.
> Beim Hinzufügen von Cache zu einem bestehenden Gateway ist es wichtig, neue Datenträger in Ihrem Host zu erstellen (Hypervisor- oder Amazon EC2 EC2-Instance). Ändern Sie nicht die Größe von vorhandenen Datenträgern, wenn die Datenträger vorher als Cache zugewiesen wurden.

Verwenden von Speicherklassen

Storage Gateway unterstützt die Speicherklassen Amazon S3 Standard, Amazon S3 Standard-Infrequent-Access, Amazon S3 One Zone-Infrequent-Access, Amazon S3 Intelligent-Tiering und S3 Glacier-Speicherklassen. Weitere Informationen über Speicherklassen finden Sie unterAmazon S3-SpeicherklassenimAmazon Simple Storage Service — Benutzerhandbuchaus.

Themen

- Verwenden von Speicherklassen mit einem Datei-Gateway
- Verwenden der GLACIER-Speicherklasse mit File Gateway

Verwenden von Speicherklassen mit einem Datei-Gateway

Wenn Sie eine Dateifreigabe erstellen oder aktualisieren, können Sie eine Speicherklasse für Ihre Objekte auswählen. Sie können die Speicherklasse Amazon S3 Standard oder eine der

Speicherklassen S3 Standard-IA, S3 One Zone-IA oder S3 Intelligent-Tiering auswählen. In diesen Speicherklassen gespeicherte Objekte können mithilfe einer Lebenszyklusrichtlinie an GLACIER übertragen werden

Amazon S3 S3-Speicherklassen	Überlegungen
Standard	Wählen Sie Standard aus, um Ihre häufig aufgerufenen Dateien redundant in mehreren Availability Zones zu speichern, die geografis ch voneinander getrennt sind. Dies ist die Standard-Speicherklasse. Weitere Informati onen finden Sie unter Amazon S3 — Preise.
S3 Intelligent-Tiering	Wählen Sie Intelligent-Tiering, um die Speicherkosten zu optimieren, indem Sie Daten automatisch in die kostengünstigste Speicherz ugriffsstufe verschieben. Objekte, die in der Speicherklasse Intelligent-Tiering gespeichert sind, können zusätzliche Gebühren für das Überschreiben, Löschen, Anfordern oder Übertragen von Objekten zwischen Speicherklassen innerhalb von 30 Tagen verursachen. Es gibt eine Mindestla gerdauer von 30 Tagen, und für Objekte, die vor 30 Tagen gelöscht werden, fallen eine anteilige Gebühr an, die der Lagergebühr für die verbleibenden Tage entspricht. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Objekte, die kleiner als 128 KB sind, können in der Speicherklasse Intelligent-Tiering nicht automatisch abgestuft werden. Diese Objekte werden zu den Raten der häufigen Zugangstu fe berechnet, und es fallen Gebühren für frühe Löschungen an.

Amazon S3 S3-Speicherklassen	Überlegungen
	S3 Intelligent-Tiering unterstützt jetzt eine Ebene für den Archivzugriff und eine Stufe für Deep Archive Access. S3 Intelligent-Tierin g verschiebt automatisch Objekte, auf die 90 Tage lang nicht zugegriffen wurde, in die Ebene Archive Access und dann nach 180 Tagen ohne Zugriff in die Ebene Deep Archive Access. Immer wenn ein Objekt in einer der Archivzugriffsebenen wiederhergestellt wird, wechselt das Objekt innerhalb weniger Stunden auf die Stufe „Häufiger Zugriff“ und kann abgerufen werden. Dies führt zu Timeout-Fehlern für Benutzer oder Anwendungen, die versuchen, über eine Dateifreigabe auf Dateien zuzugreifen, wenn das Objekt nur in einer der beiden Archivebenen vorhanden ist. Verwenden Sie die Archivstufen nicht mit S3 Intelligent-Tiering, wenn Ihre Anwendungen über die Dateifreigaben auf Dateien zugreifen, die vom Datei-Gateway dargestellt werden. Wenn Dateioperationen, die Metadaten aktualisieren (wie Eigentümer, Zeitstempel, Berechtigungen und ACLs), für vom Datei-Gat eway verwaltete Dateien ausgeführt werden, wird das vorhandene Objekt gelöscht und eine neue Version des Objekts in dieser Amazon S3 S3-Speicherklasse erstellt. Sie sollten überprüfen, wie sich Dateioperationen auf die Objekterstellung auswirken, bevor Sie diese Speicherklasse in der Produktion verwenden, da vorzeitige Löschgebühren anfallen. Weitere Informationen finden Sie unter Amazon S3 — Preise.

Amazon S3 S3-Speicherklassen	Überlegungen
S3 Standard-IA	Wählen Sie Standard-IA aus, um Ihre selten aufgerufenen Dateien redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind. Objekte, die in der Speicherklasse Standard-IA gespeichert sind, können zusätzliche Gebühren für das Überschreiben, Löschen, Anfordern , Abrufen oder Übertragen von Objekten zwischen Speicherklassen innerhalb von 30 Tagen verursachen. Es gibt eine Mindestla gerdauer von 30 Tagen. Für Objekte, die vor 30 Tagen gelöscht wurden, fällt eine anteilige Gebühr an, die der Lagergebühr für die verbleibenden Tage entspricht. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Objekte, die kleiner als 128 KB sind, werden 128 KB berechnet und es fallen Gebühren für vorzeitige Löschung an. Wenn Dateioperationen, die Metadaten aktualisieren (wie Eigentümer, Zeitstempel, Berechtigungen und ACLs), für vom Datei-Gat eway verwaltete Dateien ausgeführt werden, wird das vorhandene Objekt gelöscht und eine neue Version des Objekts in dieser Amazon S3 S3-Speicherklasse erstellt. Sie sollten überprüfen, wie sich Dateioperationen auf die Objekterstellung auswirken, bevor Sie diese Speicherklasse in der Produktion verwenden, da vorzeitige Löschgebühren anfallen. Weitere Informationen finden Sie unter Amazon S3 — Preise.

Amazon S3 S3-Speicherklassen	Überlegungen
S3 One Zone-IA	Wählen Sie One Zone-IA aus, um Ihre selten aufgerufenen Dateien in einer einzigen Availability Zone zu speichern. Objekte, die in der Speicherklasse One Zone-IA gespeichert sind, können zusätzliche Gebühren für das Überschreiben, Löschen, Anfordern, Abrufen oder Übertragen von Objekten zwischen Speicherklassen innerhalb von 30 Tagen verursachen. Es gibt eine Mindestlagerdauer von 30 Tagen, und für Objekte, die vor 30 Tagen gelöscht werden, fallen eine anteilige Gebühr an, die der Lagergebühr für die verbleibenden Tage entspricht. Bedenken Sie, wie oft diese Objekte geändert werden, wie lange Sie diese Objekte behalten möchten und wie oft Sie darauf zugreifen müssen. Objekte, die kleiner als 128 KB sind, werden 128 KB berechnet und es fallen Gebühren für vorzeitige Löschung an. Wenn Dateioperationen, die Metadaten aktualisieren (wie Eigentümer, Zeitstempel, Berechtigungen und ACLs), für vom Datei-Gateway verwaltete Dateien ausgeführt werden, wird das vorhandene Objekt gelöscht und eine neue Version des Objekts in dieser Amazon S3 S3-Speicherklasse erstellt. Sie sollten überprüfen, wie sich Dateioperationen auf die Objekterstellung auswirken, bevor Sie diese Speicherklasse in der Produktion verwenden, da vorzeitige Löschgebühren anfallen. Weitere Informationen finden Sie unter Amazon S3 — Preise.

Auch wenn Sie Objekte direkt von einer Dateifreigabe in die Speicherklasse S3-Standard-IA, S3-One Zone-IA oder S3 Intelligent-Tiering schreiben können, empfehlen wir die Verwendung einer Lebenszyklusrichtlinie zum Übertragen Ihrer Objekte, anstatt direkt in die Dateifreigabe zu schreiben. Dies gilt insbesondere, wenn Sie davon ausgegangen sind, dass die Objekt innerhalb von 30 Tagen nach der Archivierung. Weitere Informationen zur Lebenszyklus-Richtlinie finden Sie unterVerwaltung des Objektlebenszyklusaus.

Verwenden der GLACIER-Speicherklasse mit File Gateway

Wenn Sie eine Datei über Amazon S3-Lebenszyklusrichtlinien auf S3 Glacier übertragen und die Datei über den Cache sichtbar für Ihre Dateifreigabe-Clients ist, erhalten Sie E/A-Fehler beim Aktualisieren der Datei. Wir empfehlen, CloudWatch Events einzurichten, um benachrichtigt zu werden, wenn diese E/A-Fehler auftreten, und die Benachrichtigung zum Ergreifen von Maßnahmen zu verwenden. Beispielsweise können Sie das archivierte Objekt in Amazon S3 wiederherstellen. Nachdem das Objekt in S3 wiederhergestellt wurde, können Ihre Dateifreigabe-Clients über die Dateifreigabe darauf zugreifen und es aktualisieren.

Weitere Informationen zum Wiederherstellen archivierter Objekte finden Sie unterWiederherstellen archivierter ObjekteimAmazon Simple Storage Service — Benutzerhandbuchaus.

API-Referenz für Storage Gateway

Neben der Verwendung der Konsole können Sie Ihre Gateways mit der AWS Storage Gateway-API programmgesteuert konfigurieren und verwalten. In diesem Abschnitt werden die AWS Storage Gateway-Operationen, das Anfordern des Signierens für die Authentifizierung und die Fehlerbehandlung beschrieben. Weitere Informationen zu den für Storage Gateway verfügbaren Regionen und Endpunkten finden Sie unterAWS Storage GatewayEndpunkte und KontingenteimAWS– Allgemeine Referenzaus.

> **Note**
>
> Sie können auchAWSSDKs bei der Entwicklung von Anwendungen mit Storage Gateway DieAWSSDKs für Java, .NET und PHP umschließen die zugrunde liegende Storage Gateway Gateway-API und vereinfachen so Ihre Programmierungsaufgaben. Weitere Informationen zum Herunterladen der SDK-Bibliotheken finden Sie unter Beispiel-Code-Bibliotheken.

Themen

AWS Storage GatewayErforderliche Abfrage-Header

In diesem Abschnitt werden die erforderlichen Header beschrieben, an die Sie mit jeder POST-Abfrage senden müssenAWS Storage Gatewayaus. In HTTP-Headern geben Sie wichtige Informationen über die Abfrage an, z. B, die Operation, die aufgerufen werden soll, das Datum der Abfrage und Informationen zur Ihrer Autorisierung als Sender der Abfrage. In Headern muss Groß- und Kleinschreibung beachtet werden; die Reihenfolge der Header ist nicht wichtig.

Im folgenden Beispiel werden Header dargestellt, die in der ActivateGateway-Operation verwendet werden.

```
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
```

Die folgenden Kopfzeilen müssen mit in den POST-Abfragen an enthalten seinAWS Storage Gatewayaus. Die folgenden Kopfzeilen, die mit „x-amz“ beginnen, sindAWS-spezifische Köpfe. Alle anderen aufgeführten Header sind allgemeine Header für HTTP-Transaktionen.

Header	Description
`Authorization`	Der Autorisierungs-Header enthält mehrere Informationen über die Abfrage, dieAWS Storage Gatewayum festzustellen, ob die Abfrage eine gültige Aktion für den Auftraggeber ist. Das Format dieses Headers lautet wie folgt (Zeilenumbrüche dienen besserer Lesbarkeit): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` In der vorherigen Syntax geben Sie YourAccessKey, Jahr, Monat und Tag (JJJJMMTT), die Region und die CalculatedSignature an. Das Format des Autorisierungs-Headers hängt von den Anforderungen desAWSV4 Signierprozess. Detaillierte Informationen zum Signieren finden Sie unter dem Thema Signieren von Anforderungen.
`Content-Type`	Verwenden von`application/x-amz-json-1.1` als Inhaltstyp für alle Abfragen anAWS Storage Gatewayaus. `Content-Type: application/x-amz-json-1.1`

Header	Description
`Host`	Geben Sie mit dem Host-Header dieAWS Storage GatewayEndpunkt, an den Sie Ihre Anfrage senden. Beispiel,`storagegateway.us-east-2.amazonaws.com` ist der Endpunkt für die Region USA Ost (Ohio). Weitere Informationen zu den verfügbaren Endpunkten fürAWS Storage Gateway, finden Sie unterAWS Storage GatewayEndpunkte und KontingenteimAWS– Allgemeine Referenzaus. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Sie müssen den Zeitstempel entweder im HTTP-Header `Date` oder im AWS-Header `x-amz-date` angeben. (Einige HTTP-Client-Bibliotheken lassen den Header `Date` nicht zu.) Wenn ein`x-amz-date` Header ist vorhanden, derAWS Storage GatewayIgnore`Date`Header während der Anforderungsauthentifizierung. Das Format `x-amz-date` muss ISO8601 Basic dem Format JJJJMMTT'T'HHMMSS'Z' entsprechen. Wenn sowohl der `Date`- als auch der `x-amz-date` -Header verwendet werden, muss das Format des Datum-Headers nicht ISO8601 entsprechen. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	In diesem Header werden die Version der API und die angefragte Operation angegeben. Die Werte des Ziel-Headers werden durch Verknüpfung der API-Version mit dem API-Namen gebildet und haben folgendes Format. `x-amz-target: StorageGateway_ APIversion .operationName` Der Wert operationName (z. B. "ActivateGateway") ist in der API-Liste, API-Referenz für Storage Gateway, zu finden.

Signieren von Anforderungen

Das Storage Gateway verlangt von Ihnen, jede gesendete Anforderung durch eine Signatur zu authentifizieren. Zum Signieren einer Anforderung berechnen Sie eine digitale Signatur mit einer kryptografischen Hash-Funktion. Ein kryptografischer Hash ist eine Funktion, die auf Grundlage der Eingabe einen einzigartigen Hash-Wert zurückgibt. Die Eingabe in die Hash-Funktion besteht aus dem Text Ihrer Anforderung und Ihrem geheimen Zugriffsschlüssel. Die Hash-Funktion gibt einen Hash-Wert zurück, den Sie in die Anforderung als Ihre Signatur einfügen. Die Signatur ist Teil des Headers `Authorization` in der Anforderung.

Nach dem Erhalt Ihrer Anforderung berechnet Storage Gateway die Signatur mit derselben Hash-Funktion und den von Ihnen zum Signieren der Anforderung eingegebenen Daten neu. Wenn die so berechnete Signatur der Signatur in der Anforderung entspricht, verarbeitet Storage Gateway die Abfrage. Andernfalls wird die Anforderung abgelehnt.

Storage Gateway unterstützt die -AuthentifizierungAWSSignaturversion 4aus. Der Prozess zum Berechnen einer Signatur lässt sich in drei Aufgaben untergliedern:

- Aufgabe 1: Erstellen einer kanonischen Anforderung

  Ordnen Sie Ihre HTTP-Anforderung in einem kanonischen Format neu an. Die Verwendung eines kanonischen Formats ist erforderlich, weil Storage Gateway das gleiche kanonische Format verwendet, wenn eine Signatur erneut berechnet wird, um sie mit der von Ihnen gesendeten Signatur zu vergleichen.
- Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge

  Erstellen Sie eine Zeichenfolge, die Sie als einen der Eingabewerte für die kryptografische Hash-Funktion nutzen. Die als zu signierende Zeichenfolge bezeichnete Zeichenfolge ist eine Kombination aus dem Namen des Hash-Algorithmus, dem Anforderungsdatum, einer Zeichenfolge mit dem Umfang der Anmeldeinformationen und der kanonischen Anforderung aus der vorherigen Aufgabe. Die Zeichenfolge mit dem Umfang der Anmeldeinformationen selbst ist eine Kombination aus Datum, Region und Serviceinformationen.
- Aufgabe 3: Erstellen einer Signatur

  Erstellen Sie eine Signatur für Ihre Anforderung. Verwenden Sie dazu eine kryptografische Hash-Funktion, die zwei Eingabezeichenfolgen akzeptiert: die zu signierende Zeichenfolge und einen abgeleiteten Schlüssel. Der abgeleitete Schlüssel wird unter Nutzung des geheimen Zugriffsschlüssels und der Zeichenfolge mit dem Umfang der Anmeldeinformationen berechnet, um

eine Reihe von Hash-Nachrichtenauthentifizierungscodes (Hashed Message Authentication Code, HMAC) zu erstellen.

Signatur-Berechnungsbeispiel

Das folgende Beispiel führt Sie durch die Details der Erstellung einer Signatur für ListGateways. Das Beispiel kann als Referenz verwendet werden, um Ihre Signaturberechnungsmethode zu überprüfen. Andere Referenzberechnungen finden Sie in der Signature Version 4 Test Suite des Amazon Web Services-Glossars.

In diesem Beispiel wird Folgendes angenommen:

- Der Zeitstempel für die Anforderung ist „Mon, 10 Sep 2012 00:00:00“ GMT.
- Der Endpunkt ist die Region USA Ost (Ohio).

Die allgemeine Anforderungssyntax (einschließlich JSON-Text) ist:

```
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
{}
```

Die kanonische Form der für Aufgabe 1: Erstellen einer kanonischen Anforderung berechneten Anforderung ist:

```
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
```

Die letzte Zeile der kanonischen Anforderungen ist der Hash des Anforderungstextes. Beachten Sie auch die leere dritte Zeile in der kanonischen Anforderung. Der Grund dafür ist, dass es keine Abfrageparameter für diese API (oder beliebige Storage Gateway Gateway-APIs) gibt.

Die zu signierende Zeichenfolge für Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge ist:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

Die erste Zeile der zu signierenden Zeichenfolge ist der Algorithmus, die zweite Zeile der Zeitstempel, die dritte Zeile der Umfang der Anmeldeinformationen und die letzte Zeile ein Hash der kanonischen Anforderung aus Aufgabe 1.

Für Aufgabe 3: Erstellen einer Signatur kann der abgeleitete Schlüssel wie folgt dargestellt werden:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Wenn der geheime Zugriffsschlüssel wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY verwendet wird, lautet die berechnete Signatur:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Der letzte Schritt besteht im Erstellen des `Authorization`-Headers. Für den Demo-Zugriffsschlüssel AKIAIOSFODNN7EXAMPLE lautet der Header (mit hinzugefügten Zeilenumbrüchen zur leichteren Lesbarkeit):

```
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
```

Fehlermeldungen

Themen

- Ausnahmen
- Operationsfehlercodes
- Fehlermeldungen

In diesem Abschnitt finden Sie Referenzinformationen über die AWS Storage Gateway-Fehler. Diese Fehler werden durch eine Fehlerausnahme und einen Fehlercode für die Operation dargestellt. Die Fehlerausnahme `InvalidSignatureException` wird z. B. von einer API-Antwort zurückgegeben, wenn ein Problem mit der Anforderungssignatur aufgetreten ist. Der Operationsfehlercode `ActivationKeyInvalid` wird jedoch nur für die ActivateGateway-API zurückgegeben.

Abhängig von der Art des Fehlers kann Storage Gateway nur eine Ausnahme oder eine Ausnahme und einen Fehlercode für die Operation zurückgegeben. Beispiele für Fehlermeldungen finden Sie unter Fehlermeldungen.

Ausnahmen

Die folgende Tabelle listet AWS Storage Gateway API-Ausnahmen auf. Wenn eine AWS Storage Gateway-Operation eine Fehlerantwort zurückgibt, enthält der Antworttext eine dieser Ausnahmen. Die Codes `InternalServerError` und `InvalidGatewayRequestException` geben eine Operationsfehlercodes-Nachricht zurück, in der der entsprechende Operationsfehlercode angegeben ist.

Exception	Fehlermeldung	HTTP-Statuscode
`IncompleteSignatureException`	Die angegebene Signatur ist unvollständig.	400 Ungültige Anfrage
`InternalFailure`	Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.	500 Internal Server Error
`InternalServerError`	Eine der Operationsfehlercode-Nachrichten Operationsfehlercodes.	500 Internal Server Error
`InvalidAction`	Die angeforderte Aktion oder Operation ist ungültig.	400 Ungültige Anfrage

Exception	Fehlermeldung	HTTP-Statuscode
`InvalidClientTokenId`	Das X.509-Zertifikat oderAWSDie angegebene Zugriffsschlüssel-ID ist nicht in unseren Datensätzen vorhanden.	403 Verboten
`InvalidGatewayRequestException`	Eine der Operationsfehlercode-Nachrichten in Operationsfehlercodes.	400 Ungültige Anfrage
`InvalidSignatureException`	Die berechnete Anforderungssignatur entspricht nicht der angegebenen Signatur. Prüfen SieAWSZugriffsschlüssel und Signaturmethode	400 Ungültige Anfrage
`MissingAction`	In der Anforderung fehlt ein Aktions- oder Operationsparameter.	400 Ungültige Anfrage
`MissingAuthenticationToken`	Die Anforderung muss eine gültigen (registrierte)AWSGreifen Sie auf die Schlüssel-ID oder das X.509-Zertifikat zu.	403 Verboten
`RequestExpired`	Die Anforderung liegt nach dem Ablaufdatum oder dem Anforderungsdatum (jeweils in 15-Minuten-Schritten) oder das Anforderungsdatum liegt mehr als 15 Minuten in der Zukunft.	400 Ungültige Anfrage
`SerializationException`	Fehler bei der Serialisierung. Stellen Sie sicher, dass Ihre JSON-Nutzdaten wohlgeformt sind.	400 Ungültige Anfrage
`ServiceUnavailable`	Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.	503 Service Unavailable (503 Service nicht verfügbar)

Exception	Fehlermeldung	HTTP-Statuscode
`SubscriptionRequiredException`	DieAWSDie -Zugriffsschlüssel-ID benötigt ein Abonnement für den Service.	400 Ungültige Anfrage
`ThrottlingException`	Rate überschritten.	400 Ungültige Anfrage
`UnknownOperationException`	Eine unbekannte Operation wurde angegeben. Gültige Operationen werden in Operationen im Storage Gateway aufgeführt.	400 Ungültige Anfrage
`UnrecognizedClientException`	Das Sicherheits-Token der Anfrage ist ungültig.	400 Ungültige Anfrage
`ValidationException`	Der Wert des Parameters ist ungültig oder außerhalb des Bereichs.	400 Ungültige Anfrage

Operationsfehlercodes

Die folgende Tabelle zeigt die Zuweisung zwischen AWS Storage Gateway-Operationsfehlercodes und APIs, die die Codes zurückgeben. Alle Operationsfehlercodes werden mit einer von zwei allgemeinen Ausnahmen – `InternalServerError` und `InvalidGatewayRequestException` – zurückgegeben, die in Ausnahmen beschrieben werden.

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`ActivationKeyExpired`	Der angegebene Aktivierungsschlüssel ist abgelaufen.	ActivateGateway
`ActivationKeyInvalid`	Der angegebene Aktivierungsschlüssel ist ungültig.	ActivateGateway

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`ActivationKeyNotFound`	Der angegebene Aktivierungsschlüssel wurde nicht gefunden.	ActivateGateway
`BandwidthThrottleScheduleNotFound`	Die angegebene Bandbreitendrosselung wurde nicht gefunden.	DeleteBandwidthRateLimit
`CannotExportSnapshot`	Der angegebene Snapshot kann nicht exportiert werden.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	Der angegebene Initiator wurde nicht gefunden.	DeleteChapCredentials
`DiskAlreadyAllocated`	Der angegebene Datenträger ist bereits zugeordnet.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	Der angegebene Datenträger ist nicht vorhanden.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskSizeNotGigAligned`	Der angegebene Datenträger ist nicht für Gigabyte ausgerichtet.	CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`DiskSizeGreaterThanVolumeMaxSize`	Der angegebene Datenträger ist größer als die maximale Volume-Größe.	CreateStorediSCSIVolume
`DiskSizeLessThanVolumeSize`	Der angegebene Datenträger ist kleiner als die Volume-Größe.	CreateStorediSCSIVolume
`DuplicateCertificateInfo`	Die angegebenen Zertifikatinformationen sind bereits vorhanden.	ActivateGateway
FileSystemAssociationEndPointConfigurationConflict	Die vorhandene Endpunkt-Konfiguration der Dateisystemzuordnung steht in Konflikt mit der angegebenen	AssociateFileSystem
FileSystemAssociationEndPointiPaddressalReadyInUse	Die angegebene Endpunkt-IP-Adresse wird bereits verwendet.	AssociateFileSystem
FileSystemAssociationEndPointiPaddressMissing	Die IP-Adresse des Endpoints der Dateisystemzuordnung fehlt.	AssociateFileSystem
FileSystemAssociationNotFound	Die angegebene Dateisystemzuordnung wurde nicht gefunden.	updateFileSystemAssociation DisAssociateFileSystem describeFileSystemAssociations

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
FileSystemNotFound	Das angegebene Dateisystem wurde nicht gefunden.	AssociateFileSystem

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`GatewayInternalError`	Es ist ein interner Gateway-Fehler aufgetreten.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`GatewayNotConnected`	Das angegebene Gateway ist nicht verbunden.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`GatewayNotFound`	Das angegebene Gateway wurde nicht gefunden.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`GatewayProxyNetworkConnectionBusy`	Die angegebene Proxy-Netzwerkverbindung des Gateways ist ausgelastet.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`InternalError`	Es ist ein interner Fehler aufgetreten.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`InvalidParameters`	Die angegebene Anforderung enthält ungültige Parameter.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`LocalStorageLimitExceeded`	Der lokale Speicher wurde überschritten.	AddCache AddUploadBuffer AddWorkingStorage
`LunInvalid`	Die angegebene LUN ist ungültig.	CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`MaximumVolumeCount Exceeded`	Die maximale Volume-Anzahl wurde überschri tten.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	Die Gateway-N etzwerkkonfiguration wurde geändert.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`NotSupported`	Die angegebene Operation wird nicht unterstützt.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	Das angegebene Gateway ist nicht mehr auf dem neuesten Stand.	ActivateGateway
`SnapshotInProgressException`	Der angegeben e Snapshot wird bearbeitet.	DeleteVolume
`SnapshotIdInvalid`	Der angegebene Snapshot ist ungültig.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`StagingAreaFull`	Der Staging-Bereich ist voll.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetAlreadyExists`	Das angegebene Ziel ist bereits vorhanden.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	Das angegebene Ziel ist ungültig.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	Das angegebene Ziel wurde nicht gefunden.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`UnsupportedOperationForGatewayType`	Die angegebene Operation ist für den Typ des Gateways nicht gültig.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Das angegebene Volume ist bereits vorhanden.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	Das angegebene Volume ist ungültig.	DeleteVolume
`VolumeInUse`	Das angegebene Volume wird bereits verwendet.	DeleteVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`VolumeNotFound`	Das angegebene Volume wurde nicht gefunden.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	Das angegeben e Volume ist nicht einsatzbereit.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Fehlermeldungen

Bei einem Fehler enthalten die Informationen im Antwort-Header:

- Content-Type: application/x-amz-json-1.1
- Einen passenden `4xx`- oder `5xx`-HTTP-Statuscode

Der Textkörper einer Fehlermeldung enthält Informationen zu dem aufgetretenen Fehler. Das folgende Beispiel zeigt eine Fehlerantwort mit der Ausgabesyntax von Antwortelementen für alle Fehlermeldungen.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

In der folgenden Tabellen werden die Felder der JSON-Fehlerantwort in dieser Syntax erläutert.

__type

Eine der Ausnahmen aus Ausnahmen.

Type: Zeichenfolge

error

Enthält API-spezifische Fehlerdetails. Unter den allgemeinen Fehler (z. B. nicht spezifische Fehler für eine API) werden diese Fehlerinformationen nicht angezeigt.

Type: Sammlung

errorCode

Einer der Operationsfehlercodes .

Type: Zeichenfolge

errorDetails

Dieses Feld wird nicht in der aktuellen Version der API verwendet.

Type: Zeichenfolge

message

Eine der Operationsfehlercode-Nachrichten .

Type: Zeichenfolge

Beispielantwort auf einen Fehler

Der folgende JSON-Text wird zurückgegeben, wenn Sie die API DescribeStorediSCSIVolumes verwenden und eine Anforderung für den Gateway-ARN eingeben, die nicht vorhanden ist.

```
{
  "__type": "InvalidGatewayRequestException",
```

```
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
}
```

Der folgende JSON-Text wird zurückgegeben, wenn Storage Gateway eine Signatur berechnet, die nicht der mit einer Anforderung gesendeten Signatur entspricht.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Operationen im Storage Gateway

Eine Liste der Storage Gateway Gateway-Operationen finden Sie unterAktionenimAWS Storage Gateway-API-Referenzaus.

Dokumentverlauf fürAWSStorage Gateway

- API-Version: 2013-06-30
- Letzte Aktualisierung der Dokumentation: 12. Oktober 2021

In der folgenden Tabelle sind wichtige Änderungen in den einzelnen Versionen des beschriebenAWSStorage Gateway Gateway-Benutzerhandbuchnach April 2018. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

update-history-change	Aktualisierung der Verlaufsbeschreibung	Aktualisierung des Verlaufsdatums
Aktualisierte Gateway-Erstellung	Das Verfahren zum Erstellen eines neuen Gateways wurde aktualisiert, um die Änderung der Storage Gateway Gateway-Konsole zu berücksichtigen. Weitere Informationen finden Sie unterErstellen und aktivieren Sie ein Amazon S3 File Gatewayaus.	12. Oktober 2021
Support für zwangsschließende Dateien auf SMB-Dateifreigaben	Sie können jetzt die Einstellungen für lokale Gruppen verwenden, um Gateway-Admin-Berechtigungen zuzuweisen. Gateway-Administratoren können das Microsoft Management Console-Snap-In für freigegebene Ordner verwenden, um Dateien zu schließen, die für SMB-Dateifreigaben geöffnet und gesperrt sind. Weitere	12. Oktober 2021

	Informationen finden Sie unterKonfigurieren Sie lokale Gruppen für Ihr Gatewayaus.	
Unterstützung von Überwachungsprotokollen für NFS-Dateifreigaben	Sie können jetzt NFS-Dateifreigaben konfigurieren, um Auditprotokolle zu generieren, die Details zum Benutzerzugriff auf Dateien und Ordner innerhalb einer Dateifreigabe enthalten. Sie können diese Protokolle verwenden, um Benutzeraktivitäten zu überwachen und Maßnahmen zu ergreifen, wenn unangemessene Aktivitätsmuster identifiziert werden. Weitere Informationen finden Sie unterVerstehen von Datei-Gateway-Auditaus.	12. Oktober 2021
Aliasunterstützung für Zugriffspunkte	File-Gateway-Dateifreigaben können jetzt über Access Point-Aliase im Bucket-Stil eine Verbindung zu Amazon S3 S3-Speicher herstellen. Weitere Informationen finden Sie unterErstellen Sie eine Dateifreigabeaus.	12. Oktober 2021

Unterstützung von VPC-Endpunkten und Access Points	File-Gateway-Dateifreigaben können jetzt über Access Points oder Interface-Endpoints in Ihrer VPC powered by mit S3-Buckets verbunden werdenAWS PrivateLinkaus. Weitere Informationen finden Sie unterErstellen Sie eine Dateifreigabeaus.	7. Juli 2021
Unterstützung für Opportunistische Sperren	File-Gateway-Dateifreigaben können jetzt opportunistische Sperren verwenden, um ihre Dateipufferungsstrategie zu optimieren, was in den meisten Fällen die Leistung verbessert, insbesondere im Hinblick auf Windows-Kontextmenüs. Weitere Informationen finden Sie unterErstellen Sie eine SMB-Dateifreigabeaus.	7. Juli 2021
FedRAMP-Compliance	Storage Gateway ist jetzt FedRAMP-konform. Weitere Informationen finden Sie unterStorage Gatewayaus.	24. November 2020
Zeitplanbasierte Bandbreitendrosselung	Storage Gateway unterstützt jetzt die planbasierte Bandbreitendrosselung für Band- und Volume-Gateways. Weitere Informationen finden Sie unterPlanen der Bandbreitendrosselung mit der Storage Gateway Gateway-Konsoleaus.	9. November 2020

Benachrichtigung zum Hochladen von Dateien für File	Das Datei-Gateway bietet jetzt eine Benachrichtigung zum Hochladen von Dateien, die Sie benachrichtigt, wenn eine Datei vom Datei-Gateway vollständig auf Amazon S3 hochgeladen wurde. Weitere Informationen finden Sie unterBenachrichtigung zum Hochladen von Dateienaus.	9. November 2020
Zugriffsbasierte Aufzählung für File-Gateway	File Gateway bietet jetzt zugriffsbasierte Aufzählun g, die die Aufzählung von Dateien und Ordnern auf einer SMB-Dateifreigabe basierend auf den ACLs der Freigabe filtert. Weitere Informationen finden Sie unterErstellen einer SMB-Dateifreigabeaus.	9. November 2020
File Gateways	File Gateway bietet jetzt einen dokumentierten Prozess zum Ersetzen eines vorhanden en Datei-Gateways durch ein neues Datei-Gateway. Weitere Informationen finden Sie unterErsetzen eines Datei-Gateways durch ein neues Datei-Gatewayaus.	30. Oktober 2020
File Gateway Cold Cache Leseleistung 4-fache Erhöhung	Storage Gateway hat die Leseleistung des kalten Caches um das Vierfache Weitere Informationen finden Sie unterLeistungsleitlinien für File Gatewaysaus.	31. August 2020

Bestellen Sie die Hardware-Appliance über die Konsole	Sie können die Hardware-Appliance jetzt über dieAWSStorage Gateway Gateway-Konsole Weitere Informationen finden Sie unterVerwenden der Storage Gateway Hardware Appliance aus.	12. August 2020
Support von Endpunkten für den Federal Information Processing Standard (FIPS) in neuAWS-Regionen	Sie können jetzt ein Gateway mit FIPS-Endpunkten in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Nordkalifornien), USA West (Oregon) und Kanada (Central) aktiviere n. Weitere Informationen finden Sie unterAWSStorage Gateway Gateway-Endpunkte und KontingenteimAWS–Allgemeine Referenzaus.	31. Juli 2020

Support für mehrere Dateifreigaben, die an einen einzelnen Amazon S3 S3-Bucket angehängt sind	Das Datei-Gateway unterstützt jetzt das Erstellen mehrerer Dateifreigaben für einen einzelnen S3-Bucket und das Synchronisieren des lokalen Caches des Datei-Gateways mit einem Bucket basierend auf der Häufigkeit des Verzeichniszugriffs. Sie können die Anzahl der Buckets einschränken, die für die Verwaltung der Dateifreigaben erforderlich sind, die Sie auf Ihrem Datei-Gateway erstellen. Sie können mehrere S3-Präfixe für einen S3-Bucket definieren und ein einzelnes S3-Präfix einer einzelnen Gateway-Dateifreigabe zuordnen. Sie können auch Namen für Gateway-Dateifreigaben definieren, um unabhängig vom Bucket-Namen zu sein, damit sie an die Namenskonvention für lokale Dateifreigaben passen. Weitere Informationen finden Sie unterErstellen einer NFS-DateifreigabeoderErstellen einer SMB-Dateifreigabeaus.	7. Juli 2020

Lokaler Cache-Speicher des Datei-Gateways 4x	Storage Gateway unterstützt jetzt einen lokalen Cache von bis zu 64 TB für das Datei-Gateway und verbessert die Leistung für lokale Anwendungen, indem der Zugriff mit geringer Latenz auf größere Arbeitsdatensets ermöglicht wird. Weitere Informationen finden Sie unter Empfohlene lokale Festplattengrößen für Ihr Gateway im Storage Gateway Gateway-Benutzerhandbuch aus.	7. Juli 2020
Anzeigen von Amazon CloudWatch CloudWatch-Alarmen in der Storage Gateway Gateway-Konsole	Sie können jetzt CloudWatch-Alarme in der Storage Gateway Gateway-Konsole anzeigen. Weitere Informationen finden Sie unter Verstehen von CloudWatch-Alarmen aus.	29. Mai 2020

Unterstützung von Endpunkten für den Federal Information Processing Standard (FIPS).	Sie können nun ein Gateway mit FIPS-Endpunkten in den AWS GovCloud (US)-Regionen aktivieren. Informationen zum Auswählen eines FIPS-Endpunkts für ein File Gateway finden Sie unter Auswählen eines Service-Endpunkts. Informationen zum Auswählen eines FIPS-Endpunkts für ein Volume-Gateway finden Sie unter Auswählen eines Service-Endpunkts. Informationen zum Auswählen eines FIPS-Endpunkts für ein Tape Gateway finden Sie unter Auswählen eines Service-Endpunkts.	22. Mai 2020
NeuAWS-Regionen	Storage Gateway ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar. Weitere Informationen finden Sie unterAWSStorage Gateway Gateway-Endpunkte und KontingenteimAWS–Allgemeine Referenzaus.	7. Mai 2020

Unterstützung für die S3 Intelligent-Tiering-Speicherklasse	Storage Gateway unterstützt jetzt die S3 Intelligent-Tiering-Speicherklasse. Die S3 Intelligent-Tiering-Speicherklasse optimiert die Speicherkosten, indem Daten automatisch auf die kostengünstigste Zugriffsebene übertragen werden, ohne dass sich dies auf die Leistungsfähigkeit oder den Betriebsaufwand auswirkt. Weitere Informationen finden Sie unterSpeicherklasse, die häufig und weniger häufig verwendete Objekte optimiertimAmazon Simple Storage Service — Benutzerhandbuchaus.	30. April 2020
NeuAWSRegion	Storage Gateway ist jetzt in der Region verfügbar AWSRegion GovCloud (USA-Ost) Weitere Informationen finden Sie unterAWSStorage Gateway Endpunkte und KontingenteimAWS–Allgemeine Referenzaus.	12. März 2020

Unterstützung für Linux KVM-Hypervisor (Kernel-basierte virtuelle Maschine)	Storage Gateway stellt nun die Bereitstellung eines lokalen Gateways auf der KVM-Virtualisierungsplattform bereit. Gateways, die auf KVM bereitgestellt werden, verfügen über die gleiche Funktionalität und Funktionen wie die vorhandenen lokalen Gateways. Weitere Informationen finden Sie unterUnterstützte Hypervisoren und Host-AnforderungenimStorage Gateway Gateway-Benutzerhandbuchaus.	4. Februar 2020
Support für VMware vSphere High Availability	Storage Gateway stellt jetzt Support für hohe Verfügbarkeit auf VMware bereit, um Speicher-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen zu schützen. Weitere Informationen finden Sie unterVerwenden von VMware vSphere High Availability mit Storage GatewayimStorage Gateway Gateway-Benutzerhandbuchaus. Diese Version enthält auch Leistungsverbesserungen. Weitere Informationen finden Sie unterLeistungimStorage Gateway Gateway-Benutzerhandbuchaus.	20. November 2019

NeuAWS-Regionfür Tape Gateway	Tape-Gateway ist jetzt in der Region Südamerika (São Paulo) verfügbar. Weitere Informationen finden Sie unterAWSStorage Gateway Endpunkte und Kontingenteimaws– Allgemeine Referenzaus.	24. September 2019
Support für Amazon CloudWatch Logs	Sie können jetzt Datei-Gateways mit Amazon CloudWatch CloudWatch-Protokollgruppen konfigurieren, um über Fehler und den Zustand Ihres Gateways und seiner Ressourcen benachrichtigt zu werden. Weitere Informationen finden Sie unterBenachrichtigungen zu Gateway-Zustand und -Fehlern mit Amazon CloudWatch CloudWatch-Protokollgruppenim Storage Gateway Gateway-Benutzerhandbuch.	4. September 2019
NeuAWS-Region	Storage Gateway ist jetzt in der Region Asien-Pazifik (Hongkong) verfügbar. Weitere Informationen finden Sie unterAWSStorage Gateway Endpunkte und Kontingenteimaws– Allgemeine Referenzaus.	14. August 2019

NeuAWS-Region	Storage Gateway ist jetzt in der Region Mittlerer Osten (Bahrain) verfügbar. Weitere Informationen finden Sie unterAWSStorage Gateway Endpunkte und Kontingenteim AWS– Allgemeine Referenzaus.	29. Juli 2019
Unterstützung für das Aktivieren eines Gateways in einer Virtual Private Cloud (VPC)	Sie können jetzt ein Gateway in einer VPC aktivieren. Sie können eine private Verbindung zwischen Ihrer lokalen Software-Appliance und der Cloud-basierten Speicherinfrastruktur herstellen. Weitere Informationen finden Sie unter Aktivieren eines Gateways in einer Virtual Private Cloud.	20. Juni 2019
Unterstützung der SMB-Dateifreigabe für Microsoft Windows-ACLs	Für File Gateways können Sie jetzt Microsoft Windows-Zugriffskontrolllisten (ACLs) verwenden, um den Zugriff auf Server Message Block (SMB)-Dateifreigaben zu steuern. Weitere Informationen finden Sie unter Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe .	8. Mai 2019

Unterstützung von File Gateway für Tag-basierte Autorisierung	File Gateway unterstützt nun Tag-basierte Autorisierung. Sie können den Zugriff auf File Gateway-Ressourcen basierend auf den Tags in diesen Ressourcen bestimmen. Sie können auch den Zugriff basierend auf den Tags bestimmen, die in einer IAM-Anforderungsbedingung übergeben werden. Weitere Informationen finden Sie unter Bestimmung des Zugriffs auf File Gateway-Ressourcen.	4. März 2019
Verfügbarkeit von Storage Gateway Hardware Appliance in Europa	Die Storage Gateway Gateway-Hardware Appliance ist jetzt in Europa verfügbar. Weitere Informationen finden Sie unterAWSStorage Gateway Hardware Appliance -RegionenimAWS– Allgemeine Referenzaus. Darüber hinaus können Sie jetzt den nutzbaren Speicher auf der Storage Gateway-Hardware Appliance von 5 TB auf 12 TB erhöhen und die installierte Kupfer-Netzwerkkarte mit einer 10-Gigabit-Glasfaser-Netzwerkkarte ersetzen. Weitere Informationen finden Sie unter Einrichten Ihrer Hardware-Appliance.	25. Februar 2019

Support für Storage Gateway Hardware Appliance	Die Storage Gateway Hardware Appliance enthält auf einem Drittanbieterserver vorinstallierte Storage Gateway Gateway-Software. Sie können die Appliance in der AWS Management Console verwalten. Die Appliance kann Datei-, Band- und Volume-Gateways hosten. Weitere Informationen finden Sie unterVerwenden der Storage Gateway Hardware Applianceaus.	18. September 2018
Support für Server Message Block (SMB)-Protokolle	File Gateways bieten jetzt Unterstützung für Server Message Block (SMB)-Protokolle bei Dateifreigaben. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	20. Juni 2018

Frühere Updates

In der folgenden Tabelle sind wichtige Änderungen in den einzelnen Versionen des beschriebenAWSStorage Gateway Gateway-Benutzerhandbuchvor Mai 2018.

Änderung	Beschreibung	Änderungsdatum
Support für S3-One-Zone-IA Storage Class	Für Datei-Gateways können Sie jetzt die S3 One Zone-IA als Standard-Speicherklasse für Ihre Dateifreigaben wählen. Mit dieser Speicherklasse können Sie Ihre Objektdaten in einer einzelnen Availability Zone in Amazon S3 speichern. Weitere Informationen finden Sie unter Erstellen Sie eine Dateifreigabe.	4. April 2018

Änderung	Beschreibung	Änderungsdatum
Neu - AWS-Region	Tape Gateway ist jetzt in der Region Asien-Pazifik (Singapur) verfügbar. Weitere Informationen hierzu finden Sie unter Unterstützte AWS-Regionen.	3. April 2018
Support für Benachrichtigungen zur Cache-Aktualisierung, Zahlungen durch den Anforderer und vorgefertigte ACLs für Amazon S3 S3-Buckets	Mit File Gateways können Sie nun eine Benachrichtigung erhalten, wenn ein Gateway die Aktualisierung des Caches für Ihren Amazon S3 S3-Bucket abgeschlossen hat. Weitere Informationen finden Sie unterRefreshCache.htmlimStorage Gateway Gateway-APIaus. Für Datei-Gateways können Sie nun angeben, dass der Anforderer oder Leser anstelle des Bucket-Eigentümers für den Zugriff zahlt. Mit File Gateways können Sie nun aktivieren, um dem Eigentümer des S3-Buckets, der der der der der der der NFS-Dateifreigabe zugeordnet ist, volle Kontrolle zu gewähren. Weitere Informationen finden Sie unter Erstellen Sie eine Dateifreigabe.	1. März 2018
Neu - AWS-Region	Storage Gateway ist jetzt in der Region Europa (Paris) verfügbar. Weitere Informationen hierzu finden Sie unter Unterstützte AWS-Regionen.	18. Dezember 2017

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Datei-Upload-Benachrichtigung und zur Bestimmung des MIME-Typs	Mithilfe von File Gateways können Sie jetzt Benachrichtigungen erhalten, sobald alle Dateien, die auf Ihre NFS-Dateifreigabe geschrieben werden, zu Amazon S3 hochgeladen wurden. Weitere Informationen finden Sie unterNotifyWhenUploadedimStorage Gateway Gateway-APIaus. Mit File Gateways können Sie jetzt den MIME-Typ für hochgeladene Objekte basierend auf Dateierweiterungen bestimmen. Weitere Informationen finden Sie unter Erstellen Sie eine Dateifreigabe.	21. November 2017
Unterstützung für die Version 6.5 des Hypervisors VMware ESXi	AWSStorage Gateway unterstützt jetzt VMware ESXi Hypervisor 6.5. Diese Version wird zusätzlich zu den Versionen 4.1, 5.0, 5.1, 5.5 und 6.0 unterstützt. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	13. September 2017
Unterstützung für den Hypervisor Microsoft Hyper-V in der File Gateway-Konfiguration	Es ist nun möglich, ein File Gateway auf dem Hypervisor Microsoft Hyper-V bereitzustellen. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	22. Juni 2017
Neu - AWS-Region	Storage Gateway ist jetzt in der Region Asien-Pazifik (Mumbai) verfügbar. Weitere Informationen hierzu finden Sie unter Unterstützte AWS-Regionen.	02. Mai 2017

Änderung	Beschreibung	Änderungsdatum
Updates bei den Einstellungen für Dateifreigaben Unterstützung für die Cache-Aktualisierung in Dateifreigaben	Die Einstellungen für Dateifreigaben in der File Gateway-Konfiguration wurden um Mounting-Optionen erweitert. Nun stehen für Dateifreigaben eine Squash-Option und eine schreibgeschützte Option zur Verfügung. Weitere Informationen finden Sie unter Erstellen Sie eine Dateifreigabe. In der File Gateway-Konfiguration lassen sich nun alle Objekte im Amazon S3 S3-Bucket finden, die hinzugefügt oder entfernt wurden, seit das Gateway letztmalig die Inhalte des Buckets aufgelistet und die Ergebnisse zwischengespeichert hat. Weitere Informationen finden Sie unter RefreshCache in der API-Referenz.	28. März 2017
Unterstützung für File Gateways in Amazon EC2	AWSStorage Gateway stellt nun die Bereitstellung von File Gateways in Amazon EC2 bereit. Sie können in Amazon EC2 ein Datei-Gateway starten, indem Sie das Storage Gateway Amazon Machine Image (AMI) starten, das nun als Community-AMI verfügbar ist. Weitere Informationen zur Erstellung von File Gateways und ihrer Bereitstellung in EC2-Instances finden Sie unter Erstellen und aktivieren Sie ein Amazon S3 File Gateway. Weitere Informationen zum Starten eines File Gateway-AMIs finden Sie unter Bereitstellen eines File Gateways auf einem Amazon EC2 EC2-Host. Darüber hinaus unterstützt File Gateway jetzt die Konfiguration eines HTTP-Proxys. Weitere Informati onen finden Sie unter Routing Ihres auf EC2 bereitges tellten Gateway über einen HTTP-Proxy.	08. Februar 2017

Änderung	Beschreibung	Änderungsdatum
Neu - AWS-Region	Storage Gateway ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen hierzu finden Sie unter Unterstützte AWS-Regionen.	13. Dezember 2016
Neu - AWS-Region	Storage Gateway ist jetzt in der Region Kanada (Zentral) verfügbar. Weitere Informationen hierzu finden Sie unter Unterstützte AWS-Regionen.	08. Dezember 2016
Unterstützung für File-Gateway	Neben Volume-Gateways und Band-Gateway stellt Storage Gateway nun File Gateway bereit. File Gateway kombiniert einen Service und eine virtuelle Software-Appliance. So können Sie Objekte in Amazon S3 mit Dateiprotokollen nach Branchenstandard wie beispielsweise NFS (Network File System) speichern und abrufen. Das Gateway stellt Objekte in Amazon S3 als Dateien auf einem NFS-Mounting Point bereit.	29. November 2016

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.