Amazon S3 File Gateway-Benutzerhandbuch

AWSStorage Gateway

API-Version 2013-06-30

AWSStorage Gateway: Amazon S3 File Gateway-Benutzerhandbuch

Table of Contents

Was ist Amazon S3 File Gateway

Amazon S3 File Gateway — Amazon S3 File Gateway unterstützt eine Dateischnittstelle zu Amazon Simple Storage Service (Amazon S3) und kombiniert einen Service und eine virtuelle Software-Appliance. Mit dieser Kombination können Sie Objekte in Amazon S3 mithilfe branchenüblicher Dateiprotokolle wie Network File System (NFS) und Server Message Block (SMB) speichern und abrufen. Sie stellen das Gateway in Ihrer lokalen Umgebung als virtuelle Maschine (VM) bereit VMware ESXi, die auf Microsoft Hyper-V oder Linux Kernel-based Virtual Machine (KVM) läuft, oder als Hardware-Appliance, die Sie bei Ihrem bevorzugten Händler bestellen. Sie können die Storage Gateway Gateway-VM auch in VMware Cloud on AWS oder als AMI in Amazon bereitstellen EC2. Das Gateway bietet Zugriff auf Objekte in S3 als Dateien oder Dateifreigabe-Einhängepunkte. Mit einem S3 File Gateway können Sie Folgendes tun:

- 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 von jeder AWS Cloud-Anwendung oder jedem Cloud-Dienst aus direkt in Amazon S3 auf Ihre Daten zugreifen.
- Sie können Ihre S3-Daten mithilfe von Lebenszyklusrichtlinien, regionsübergreifender Replikation und Versionierung verwalten. Sie können sich ein S3 File Gateway als Dateisystem-Mount auf Amazon S3 vorstellen.

Ein S3 File Gateway vereinfacht die Dateispeicherung in Amazon S3, lässt sich über branchenübliche Dateisystemprotokolle in bestehende Anwendungen integrieren und bietet eine kostengünstige 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 zu AWS, schützt Anwendungen vor Netzwerküberlastung, optimiert und streamt Daten parallel und verwaltet den Bandbreitenverbrauch.

S3 File Gateway lässt sich in andere AWS Dienste integrieren, zum Beispiel:

- Gemeinsames Zugriffsmanagement mit AWS Identity and Access Management (IAM)
- Verschlüsselung mit AWS Key Management Service ()AWS KMS
- Überwachung mit Amazon CloudWatch (CloudWatch)
- Prüfung mit AWS CloudTrail (CloudTrail)
- Operationen mit AWS-Managementkonsole 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:

- enthält Anweisungen zum Erstellen und Verwenden eines S3 File Gateways. Es zeigt Ihnen, wie Sie eine Dateifreigabe erstellen, Ihr Laufwerk einem Amazon S3-Bucket zuordnen und Dateien und Ordner auf Amazon S3 hochladen.

- beschreibt, wie Verwaltungsaufgaben für alle Gateway-Typen und Ressourcen ausgeführt werden.

In dieser Anleitung finden Sie in erster Linie Informationen zum Arbeiten mit den Gateway-Operationen mithilfe der AWS-Managementkonsole. Wenn Sie diese Operationen programmgesteuert ausführen möchten, finden Sie weitere Informationen in der AWS Storage Gateway API-Referenz.

So funktioniert Amazon S3 File Gateway

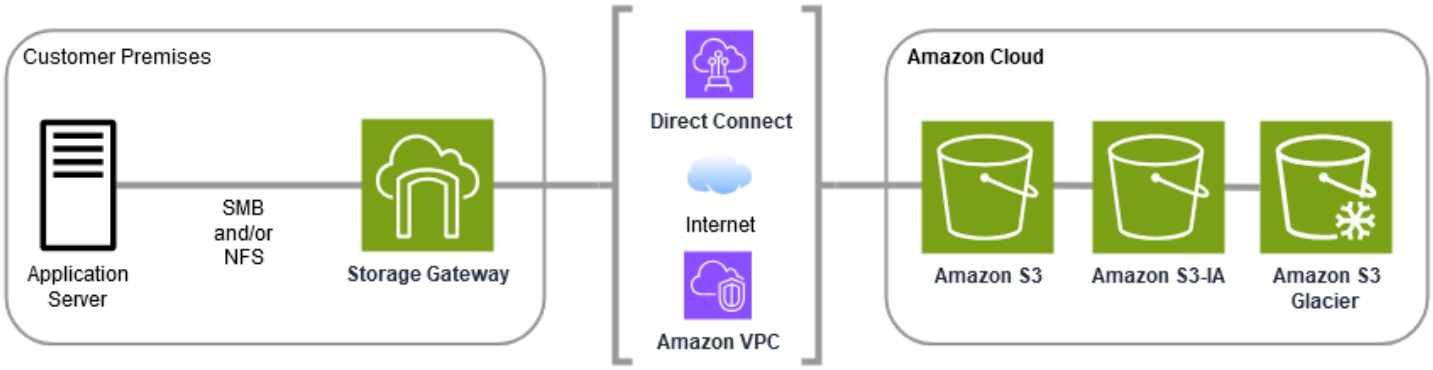
Um ein S3 File Gateway zu verwenden, laden Sie zunächst ein VM-Image für das Gateway herunter. Anschließend aktivieren Sie das Gateway über die AWS-Managementkonsole oder über die Storage Gateway Gateway-API. Sie können auch ein S3 File Gateway mit einem EC2 Amazon-Image erstellen.

Nachdem das S3 File Gateway aktiviert wurde, erstellen und konfigurieren Sie Ihre Dateifreigabe und verknüpfen diese Freigabe mit Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket. Dadurch können Clients, die entweder das Network File System (NFS) oder das Server Message Block (SMB) -Protokoll verwenden, auf die gemeinsame Nutzung zugreifen. In eine Dateifreigabe geschriebene Dateien werden in Amazon S3 zu Objekten, wobei der Pfad der Schlüssel ist. Es gibt eine one-to-one Zuordnung zwischen Dateien und Objekten, und das Gateway aktualisiert die Objekte in Amazon S3 asynchron, wenn Sie die Dateien ändern. Bestehende Objekte im Amazon S3 S3-Bucket werden als Dateien im Dateisystem angezeigt, und der Schlüssel wird zum Pfad. Objekte werden mit serverseitigen Amazon S3 S3-Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt. Die gesamte Datenübertragung erfolgt über HTTPS.

Beim Senden von HTTPS-Daten-Upload-Anfragen an Amazon S3 füllt File Gateway den MD5 Content-Header mit der MD5 Prüfsumme der hochgeladenen Daten. Die Verwendung dieses Headers veranlasst Amazon S3, im Falle einer Nichtübereinstimmung zwischen der von Amazon S3 berechneten MD5 Prüfsumme und dem vom File Gateway empfangenen Wert einen Fehler zurückzugeben. Wenn ein solcher Fehler zurückgegeben wird, sendet das File Gateway die Anfrage erneut.

Der Dienst optimiert die Datenübertragung zwischen dem Gateway und AWS verwendet mehrteilige parallel Uploads oder Downloads im Bytebereich, um die verfügbare Bandbreite besser zu nutzen. Der lokale Cache wird beibehalten, um den Zugriff auf die zuletzt abgerufenen Daten mit geringer Latenz zu ermöglichen und die Gebühren für den Datenausgang zu senken. CloudWatch Metriken bieten Einblicke in die Ressourcennutzung auf der VM und den Datentransfer von AWS und zu. CloudTrail verfolgt alle API-Aufrufe.

Mit dem S3 File Gateway-Speicher können Sie Aufgaben wie das Einlesen von Cloud-Workloads in Amazon S3, das Durchführen von Backups und Archivieren, Tiering und die Migration von Speicherdaten in die Cloud erledigen. AWS Das folgende Diagramm bietet einen Überblick über die Bereitstellung von Dateispeichern für Storage Gateway.



S3 File Gateway konvertiert Dateien in S3-Objekte, wenn Dateien auf Amazon S3 hochgeladen werden. Die Wechselwirkung zwischen Dateioperationen, die gegen Dateifreigaben auf S3 File Gateway ausgeführt werden, und S3-Objekten erfordert, dass bestimmte Operationen bei der Konvertierung zwischen Dateien und Objekten sorgfältig geprüft werden.

Bei häufigen Dateioperationen werden Dateimetadaten geändert, was zum Löschen des aktuellen S3-Objekts und zur Erstellung eines neuen S3-Objekts führt. Die folgende Tabelle zeigt Beispiele für Dateioperationen und deren Auswirkungen auf S3-Objekte.

Betrieb von Dateien	Auswirkung auf das S3-Objekt	Auswirkung auf die Speicherklasse
Datei umbenennen	Ersetzt ein vorhandenes S3-Objekt und erstellt für jede Datei ein neues S3-Objekt	Es können Gebühren für vorzeitiges Löschen und Abrufen anfallen
Ordner umbenennen	Ersetzt alle vorhandenen S3-Objekte und erstellt neue S3-Objekte für jeden Ordner und jede Datei in der Ordnerstruktur	Es können Gebühren für vorzeitiges Löschen und Abrufen anfallen
Berechtigungen ändern file/folder	Ersetzt ein vorhandenes S3-Objekt und erstellt ein neues S3-Objekt für jede Datei oder jeden Ordner	Gebühren für vorzeitiges Löschen und Abrufen können anfallen
Inhaberschaft ändern file/folder	Ersetzt ein vorhandenes S3-Objekt und erstellt ein neues S3-Objekt für jede Datei oder jeden Ordner	Gebühren für vorzeitiges Löschen und Abrufen können anfallen
An eine Datei anhängen	Ersetzt ein vorhandenes S3-Objekt und erstellt für jede Datei ein neues S3-Objekt	Es können Gebühren für vorzeitiges Löschen und Abrufen anfallen

Wenn eine Datei von einem NFS- oder SMB-Client auf das S3 File Gateway geschrieben wird, lädt das File Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von ihren Metadaten (Besitzverhältnisse, Zeitstempel usw.). Durch das Hochladen der Dateidaten wird ein S3-Objekt erstellt, und beim Hochladen der Metadaten für die Datei werden die Metadaten für das S3-Objekt aktualisiert. Durch diesen Vorgang wird eine weitere Version des Objekts erstellt, was zu zwei Versionen eines Objekts führt. Wenn die S3-Versionierung 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 auf das S3 File Gateway fertig ist. Zu den Gründen hierfür gehören die Freigabe von Cache-Speicherplatz oder eine hohe Schreibgeschwindigkeit auf 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 existieren, 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 von Same-Region-Replication (SRR) oder Cross-Region-Replication (CRR) zwischen S3-Buckets erhöht den Speicherverbrauch.

Erste Schritte mitAWS Storage Gateway

Dieser Abschnitt enthält Anweisungen für die ersten Schritte mitAWS. Sie benötigen ein AWS Konto, bevor Sie mit der Nutzung beginnen könnenAWS Storage Gateway. Sie können ein vorhandenes AWS Konto verwenden oder sich für ein neues Konto registrieren. Sie benötigen außerdem einen IAM-Benutzer in Ihrem AWS Konto, der zu einer Gruppe mit den erforderlichen Administratorberechtigungen gehört, um Storage Gateway Gateway-Aufgaben auszuführen. Benutzer mit den entsprechenden Rechten können auf die Storage Gateway-Konsole und die Storage Gateway-API zugreifen, um Gateway-Bereitstellungs-, Konfiguration- und Wartungsaufgaben durchzuführen. Wenn Sie zum ersten Mal Benutzer sind, empfehlen wir Ihnen, die Abschnitte Unterstützte AWS Regionen und File Gateway-Setup-Anforderungen zu lesen, bevor Sie mit Storage Gateway arbeiten.

Dieser Abschnitt enthält die folgenden Themen, die zusätzliche Informationen zu den ersten Schritten enthalten: AWS Storage Gateway

Topics

- ZugriffAWS Storage Gateway- Erfahre, wie du dich registrierst AWS und ein AWS Konto erstellst.
- ZugriffAWS Storage Gateway- Erfahren Sie, wie Sie einen IAM-Benutzer mit Administratorrechten für Ihr AWS Konto erstellen.
- ZugriffAWS Storage Gateway- Erfahren Sie, wie Sie AWS Storage Gateway über die Storage Gateway Gateway-Konsole oder programmgesteuert mithilfe der AWS SDKs darauf zugreifen.
- AWS-Regionendie Storage Gateway unterstützen- Erfahren Sie, AWS in welchen Regionen Sie Ihre Daten speichern können, wenn Sie Ihr Gateway in Storage Gateway aktivieren.

Melden Sie sich für einAWS-Konto

Um loszulegenAWS, benötigen Sie eineAWS-Konto. Informationen zum Erstellen eines AWS-Konto finden Sie unter Erste Schritte mit einem AWS-Konto im AWS -KontenverwaltungReferenzhandbuch.

ZugriffAWS Storage Gateway

Sie können die AWS Storage GatewayKonsole verwenden, um verschiedene Gateway-Konfiguration und Wartungsaufgaben durchzuführen, darunter das Aktivieren oder Entfernen von Storage Gateway Gateway-Hardware-Appliances aus Ihrer Bereitstellung, das Erstellen, Verwalten und Löschen der

verschiedenen Gateway-Typen, das Erstellen, , Verwalten und Löschen von Dateisystemen zum sowie die Überwachung des Zustands und Status verschiedener Elemente des Storage Gateway Gateway-Dienstes. Aus Gründen der Einfachheit und Benutzerfreundlichkeit konzentriert sich dieses Handbuch auf die Ausführung von Aufgaben über die Weboberfläche der Storage Gateway Gateway-Konsole. Sie können über Ihren Webbrowser auf die Storage Gateway Gateway-Konsole zugreifen unter:https://console.aws.amazon.com/storagegateway/home/.

Wenn Sie einen programmatischen Ansatz bevorzugen, können Sie die AWS Storage Gateway Anwendungsprogrammierschnittstelle (API) oder die Befehlszeilenschnittstelle (CLI) verwenden, um die Ressourcen in Ihrer Storage Gateway Gateway-Bereitstellung einzurichten und zu verwalten. Weitere Informationen zu Aktionen, Datentypen und der erforderlichen Syntax für die Storage Gateway API finden Sie in der Storage Gateway API-Referenz. Weitere Informationen zur Storage Gateway Gateway-CLI finden Sie in der AWSCLI Command Reference.

Sie können die AWS SDKs auch verwenden, um Anwendungen zu entwickeln, die mit Storage Gateway interagieren. Die AWS SDKs for Java, .NET und PHP umfassen die zugrunde liegende Storage-Gateway-API und vereinfachen Ihre Programmieraufgaben. Informationen zum Herunterladen der SDK-Bibliotheken finden Sie im AWSDeveloper Center.

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

AWS-Regionendie Storage Gateway unterstützen

An AWS-Region ist ein physischer Standort auf der Welt, an dem es AWS mehrere Availability Zones gibt. Availability Zones bestehen aus einem oder mehreren diskreten AWS Rechenzentren, die jeweils über redundante Stromversorgung, Netzwerke und Konnektivität verfügen und in separaten Einrichtungen untergebracht sind. Das bedeutet, AWS-Region dass jede Region physisch isoliert und unabhängig von den anderen Regionen ist. Regionen bieten Fehlertoleranz, Stabilität und Ausfallsicherheit und können auch die Latenz verkürzen. Die Ressourcen, die Sie in einer Region erstellen, sind in keiner anderen Region vorhanden, es sei denn, Sie verwenden ausdrücklich eine von einem AWS Dienst angebotene Replikationsfunktion. Beispielsweise unterstützen Amazon S3 und Amazon EC2 die regionsübergreifende Replikation. Einige Dienste, z. B.AWS Identity and Access Management, verfügen nicht über regionale Ressourcen. Sie können AWS Ressourcen an Standorten einsetzen, die Ihren Geschäftsanforderungen entsprechen. Möglicherweise möchten Sie Amazon EC2 EC2-Instances starten, um Ihre AWS Storage Gateway Appliances AWS-Region in Europa zu hosten, um Ihren europäischen Benutzern näher zu sein oder um gesetzliche Anforderungen zu erfüllen. Ihr AWS-Konto bestimmt, welche der Regionen, die von einem bestimmten Service unterstützt werden, für Sie verfügbar sind.

- Storage Gateway — Unterstützte AWS Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage GatewayEndpunkte und Kontingente in der. Allgemeine AWS-Referenz
- Storage Gateway Gateway-Hardware-Appliance — Informationen zu unterstützten Regionen, die Sie mit der Hardware-Appliance verwenden können, finden Sie unter AWS Storage GatewayHardware-Appliance-Regionen in der Allgemeine AWS-Referenz.

Setup-Anforderungen für File Gateway

Sofern nicht anders angegeben, gelten die folgenden Anforderungen für alle File Gateway-Typen inAWS Storage Gateway. 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

Voraussetzungen

Bevor Sie Ihr Amazon S3 File Gateway (S3 File Gateway) einrichten, müssen Sie die folgenden Voraussetzungen erfüllen:

- Konfigurieren Sie Microsoft Active Directory (AD) und erstellen Sie ein Active Directory-Dienstkonto mit den erforderlichen Berechtigungen. Weitere Informationen finden Sie unter Berechtigungsanforderungen für Active Directory-Dienstkonten Berechtigungsanforderungen für .
- Stellen Sie sicher, dass zwischen dem Gateway und ausreichend Netzwerkbandbreite vorhanden istAWS. Für das erfolgreiche Herunterladen, Aktivieren und Aktualisieren des Gateways sind mindestens 100 Mbit/s erforderlich.
- Konfigurieren Sie die Verbindung, die Sie für den Netzwerkverkehr zwischen AWS und der lokalen Umgebung verwenden möchten, in der Sie Ihr Gateway bereitstellen. Sie können eine Verbindung über das öffentliche Internet, ein privates Netzwerk, ein VPN oder Direct Connect herstellen. Wenn Sie möchten, dass Ihr Gateway AWS über eine private Verbindung mit einer Amazon Virtual Private Cloud kommuniziert, richten Sie die Amazon VPC ein, bevor Sie Ihr Gateway einrichten.
- Stellen Sie sicher, dass Ihr Gateway den Namen Ihres Active Directory-Domain-Controllers auflösen kann. Sie können DHCP in Ihrer Active Directory-Domäne für die Auflösung verwenden

oder einen DNS-Server manuell über das Einstellungsmenü für die Netzwerkkonfiguration in der lokalen Gateway-Konsole angeben.

Hardware- und Speicheranforderungen

Die folgenden Abschnitte enthalten Informationen zu den mindestens erforderlichen Hardware- und Speicherkonfigurationen für Ihr Gateway und zur Mindestmenge an Festplattenspeicher, die für den erforderlichen Speicher zugewiesen werden muss.

Informationen zu bewährten Methoden für die Leistung von File Gateway finden Sie unterGrundlegende Hinweise zur Leistung für S3 File Gateway FSx .

Hardwareanforderungen für lokale VMs

Stellen Sie bei der lokalen Bereitstellung Ihres Gateways sicher, dass die zugrunde liegende Hardware, auf der Sie die virtuelle Gateway-Maschine (VM) bereitstellen, die folgenden Mindestressourcen bereitstellen kann:

- Vier virtuelle Prozessoren sind der VM zugewiesen
- 16 GiB reservierter RAM für File Gateways
- 80 GiB Festplattenspeicher für die Installation von VM-Image- und Systemdaten

Weitere Informationen finden Sie unter Maximieren des S3 File Gateway-Durchsatzes. Weitere Informationen zu den Auswirkungen der Hardware auf die Leistung der Gateway-VM finden Sie unter Kontingente für Dateifreigaben.

Anforderungen für Amazon-EC2-Instance-Typen

Wenn Sie Ihr Gateway auf Amazon Elastic Compute Cloud (Amazon EC2) bereitstellen, muss die Instance-Größe mindestens **`xlarge`**so groß sein, dass Ihr Gateway funktioniert. Für die rechenoptimierte Instance-Familie muss die Größe jedoch mindestens betragen. **`2xlarge`**

> **Note**
>
> Das Storage Gateway AMI ist nur mit x86-basierten Instances kompatibel, die Intel- oder AMD-Prozessoren verwenden. ARM-based Instances, die Graviton-Prozessoren verwenden, werden nicht unterstützt.

Verwenden Sie einen der folgenden für Ihr Gateway empfohlenen Instance-Typen.

Für File Gateway-Typen empfohlen

- General-purpose Instanzfamilie — Instanztyp m5, m6 oder m7. Wählen Sie die Xlarge-Instance-Größe oder höher, um die Prozessor- und RAM-Anforderungen von Storage Gateway zu erfüllen.
- Compute-optimized Instance-Familie — Instance-Typen c5, c6 oder c7. Wählen Sie die 2xlarge-Instance-Größe oder höher, um die Prozessor- und RAM-Anforderungen von Storage Gateway zu erfüllen.
- Memory-optimized Instance-Familie — Instance-Typen r5, r6 oder r7 Wählen Sie die Xlarge-Instance-Größe oder höher, um die Prozessor- und RAM-Anforderungen von Storage Gateway zu erfüllen.
- Storage-optimized Instance-Familie — Instance-Typen i3, i4 oder i7 Wählen Sie die Xlarge-Instance-Größe oder höher, um die Prozessor- und RAM-Anforderungen von Storage Gateway zu erfüllen.

> **Note**
>
> Wenn Sie Ihr Gateway in Amazon EC2 starten und der von Ihnen gewählte Instance-Typ kurzlebigen Speicher unterstützt, werden die Festplatten automatisch aufgelistet. Weitere Informationen zum Amazon EC2 EC2-Instance-Speicher finden Sie unter Instance-Speicher im Amazon EC2 EC2-Benutzerhandbuch.
> Anwendungsschreibvorgänge werden synchron im Cache gespeichert und dann asynchron in einen dauerhaften Speicher in Amazon S3 hochgeladen. Wenn der kurzlebige Speicher verloren geht, weil eine Instance beendet wird, bevor der Upload abgeschlossen ist, können die Daten, die sich noch im Cache befinden und noch nicht in Amazon Simple Storage Service (Amazon S3) geschrieben wurden, verloren gehen. Bevor Sie die Instance beenden, die das Gateway hostet, stellen Sie sicher, dass die Metrik `CachePercentDirty` CloudWatch `0` Weitere Informationen zum flüchtigen Speicher finden Sie unter Verwendung von kurzlebigem Speicher mit EC2-Gateways. Informationen zur Überwachung von Metriken für Ihr Storage Gateway finden Sie unterÜberwachung Ihres S3 File Gateway FSx .
> Wenn Sie mehr als 5 Millionen Objekte in Ihrem S3-Bucket haben und ein gp2-EBS-Volume verwenden, ist für eine akzeptable Leistung Ihres Gateways beim Start ein EBS-Root-Volume von mindestens 350 GiB erforderlich. Newly-created Amazon EC2 File Gateway-Instances verwenden standardmäßig gp3-Root-Volumes, für die diese

Anforderung nicht gilt. Informationen zur Erhöhung der Volume-Größe finden Sie unter Ändern eines EBS-Volumes mithilfe elastischer Volumes (Konsole).

Speicheranforderungen

Neben 80 GiB Festplattenspeicher für die VM benötigen Sie auch zusätzliche Festplatten für Ihr Gateway.

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

Note

Sie können ein oder mehrere lokale Laufwerke für Ihren Cache konfigurieren, bis die maximale Kapazität erreicht ist.
Wenn Sie einem vorhandenen Gateway Cache hinzufügen, ist es wichtig, neue Festplatten auf Ihrem Host (Hypervisor oder Amazon EC2 EC2-Instance) zu erstellen. Ändern Sie nicht die Größe vorhandener Festplatten, wenn die Festplatten 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 hoch- und heruntergeladen wird. Für das erfolgreiche Herunterladen, Aktivieren und Aktualisieren des Gateways sind mindestens 100 Mbit/s erforderlich. Ihre Datenübertragungsmuster bestimmen die Bandbreite, die zur Unterstützung Ihrer Workload 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 Ihr Gateway auf Amazon EC2 bereitstellen oder andere Bereitstellungsarten (einschließlich lokal) mit Netzwerksicherheitsrichtlinien verwenden, die AWS IP-Adressbereiche einschränken. In diesen Fällen kann es bei Ihrem Gateway zu Problemen mit der Dienstkonnektivität kommen, wenn sich die AWS IP-Bereichswerte ändern. Die Werte für den AWS IP-Adressbereich, die Sie verwenden müssen, gehören zur Amazon-Servicesubmenge für die AWS Region, in der Sie Ihr Gateway aktivieren. Informationen zu den aktuellen IP-Bereichswerten finden Sie unter AWS IP-Adressbereiche im Allgemeine AWS-Referenz.

Themen

Port-Anforderungen

Für S3 File Gateway müssen für eine erfolgreiche Bereitstellung und einen erfolgreichen Betrieb bestimmte Ports durch Ihre Netzwerksicherheit zugelassen werden. Einige Ports sind für alle Gateways erforderlich, während andere nur für bestimmte Konfigurationen erforderlich sind, z. B. beim Herstellen einer Verbindung zu NFS- oder SMB-Clients, VPC-Endpunkten oder Microsoft Active Directory.

Für S3 File Gateway müssen Sie Microsoft Active Directory nur verwenden, wenn Sie Domänenbenutzern den Zugriff auf eine SMB-Dateifreigabe (Server Message Block) ermöglichen möchten. Sie können Ihr File Gateway mit jeder gültigen Microsoft Windows-Domäne verbinden (durch DNS auflösbar).

Sie können die auch verwendenDirectory Service, um eine AWS Managed Microsoft ADin der Amazon Web Services Cloud zu erstellen. Für die meisten AWS Managed Microsoft AD Bereitstellungen müssen Sie den Dynamic Host Configuration Protocol (DHCP) -Dienst für Ihre VPC

konfigurieren. Informationen zum Erstellen eines DHCP-Optionssatzes finden Sie unter Erstellen eines DHCP-Optionssatzes im Administratorhandbuch. AWS Directory Service

In der folgenden Tabelle sind die erforderlichen Ports aufgeführt und die bedingten Anforderungen werden in der Spalte „Hinweise“ beschrieben.

Portanforderungen für S3 File Gateway Gateway

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Webbrowser	Ihr Webbrowser	Storage-Gateway-VM	TCP HTTP	80	✓	✓	✓	Wird von lokalen Systemen verwendet, um den Storage Gateway Gateway-Aktivierungsschlüssel zu erhalten. Port 80 wird nur während der Aktivierung einer Storage-Gateway-Ap

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								pliance verwendet. Für eine Storage-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 Ihr Gateway

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								von der Storage Gateway Management Console aus aktivieren, muss der Host, von dem aus Sie eine Verbindung zur Konsole herstellen, Zugriff auf den Port 80 Ihres Gateways haben.

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Webbrowser	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓	AWSManagement-Konsole (alle anderen Operationen)
DNS	Storage-Gateway-VM	Domain Name Service (DNS)-Server	TCP- und UDP-DNS	53	✓	✓	✓	Wird für die Kommunikation zwischen einer Storage Gateway Gateway-VM und dem DNS-Server für die IP-Namensauflösung verwendet.

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
NTP	Storage-Gateway-VM	Network Time Protocol (NTP)-Server	TCP & UDP NTP	123	✓	✓	✓	Wird von lokalen Systemen verwendet, um die VM-Zeit mit der Host-Zeit zu synchronisieren. Eine Storage-Gateway-VM ist so konfiguriert, dass die folgenden NTP-Server verwendet werden: • 0.amazon.pool.ntp.org

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								• 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org **Note** Nicht erforderlich für Gateways, die auf Amazon EC2 gehostet werden.

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Storage Gateway	Storage-Gateway-VM	SupportEndpunkt	TCP SSH	22	✓	✓	✓	Ermöglicht Support den Zugriff auf Ihr Gateway, um Ihnen bei der Behebung von Gateway-Problemen zu helfen. Dieser Port muss für den normalen Betrieb des Gateways nicht offen sein, für die Fehlerbehebung ist dies

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								jedoch erforderlich. Eine Liste der Support-Endpunkte finden Sie unter SupportEndpunkte.
Storage Gateway	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓	Managementkontrolle
Amazon CloudFront	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓	Zur Aktivierung

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓*	Managementkontrolle *Nur erforderlich, wenn VPC-Endpoints verwendet werden
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	1026		✓	✓*	Endpunkt der Kontrollebene *Nur erforderlich, wenn VPC-Endpoints verwendet werden

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	1027		✓	✓*	Anon Control Plane (zur Aktivierung) *Nur erforderlich, wenn VPC-Endpoints verwendet werden
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	1028		✓	✓*	Proxy-Endpunkt *Nur erforderlich, wenn VPC-Endpoints verwendet werden

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	1031		✓	✓*	Datenebene *Nur erforderlich, wenn VPC-Endpoints verwendet werden
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	2222		✓	✓*	SSH-Supportkanal für vPCe *Nur für das Öffnen des Support-Kanals bei Verwendung von VPC-Endpunkten erforderlich

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓*	Managementkontrolle *Nur erforderlich, wenn VPC-Endpoints verwendet werden

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Dateifreigabe-Client	SMB-Client	Storage-Gateway-VM	TCP oder UDP SMBv3	445	✓	✓	✓*	Sitzungsdienst für die gemeinsame Nutzung von Daten. Ersetzt die Ports 137—139 für Microsoft Windows NT und höher. *Nur für SMB erforderlich.
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	UDP NetBIOS	137	✓	✓	✓*	Benennen Sie den Dienst *Nur für SMBv1 erforderlich.

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	UDP NetBIOS	138	✓	✓	✓*	Datagram Service *Nur für SMBv1 erforderlich.
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	TCP- und UDP-LDAP	389	✓	✓	✓*	Client-Verbindung zum Directory System Agent (DSA) *Nur für SMB erforderlich.
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	TCP- und UDP-Kerberos	88	✓	✓	✓*	Kerberos *Nur für SMB erforderlich.

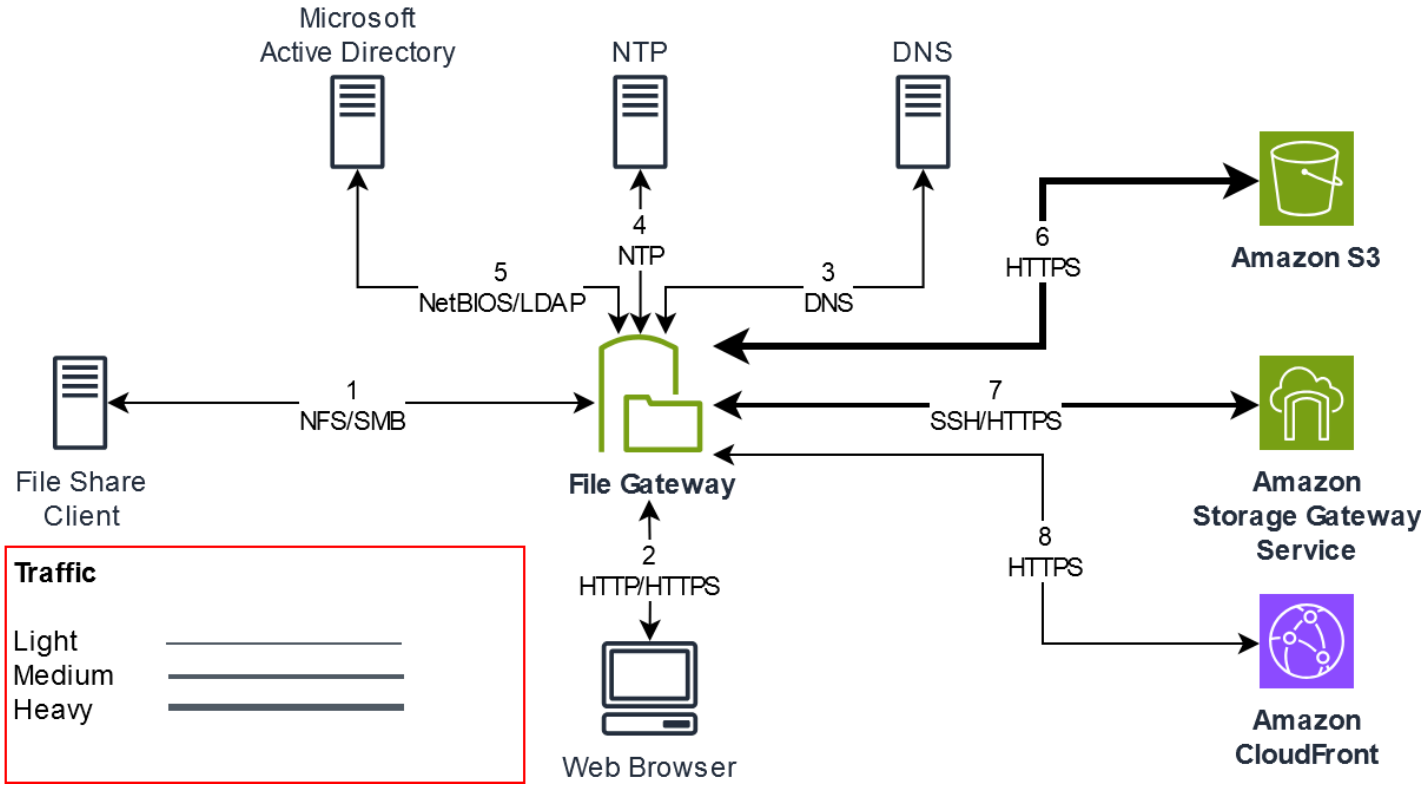
Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	Mapper für verteilte Environment/End TCP-Rechenpunkte () DCE/EMAP	135	✓	✓	✓*	RPC *Nur für SMB erforderlich.
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	Mapper für verteilte Environment/End TCP-Rechenpunkte () DCE/EMAP	49152-655 35	✓	✓	✓*	RPC Wenn Ihr AD-Domänencontroller dedizierte RPC-Ports verwendet, öffnen Sie stattdessen diese. *Nur für SMB erforderlich.

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Dateifreigabe-Client	NFS-Client	Storage-Gateway-VM	TCP- oder UDP-Daten NFSv3	111	✓	✓	✓*	Dateifreigabe-Datenübertragung (nur für NFS v3) *Nur für NFS erforderlich.
Dateifreigabe-Client	NFS-Client	Storage-Gateway-VM	TCP- oder UDP-NFS	2049	✓	✓	✓*	Fileshari ng, Datenüber tragung *Nur für NFS v3 und v4 erforderlich.
Dateifreigabe-Client	NFS-Client	Storage-Gateway-VM	TCP oder UDP NFSv3	20048	✓	✓	✓*	Fileshari ng, Datenüber tragung *Nur für NFSv3 erforderlich

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Dateifreigabe-Client	SMB-Client	Storage-Gateway-VM	TCP oder UDP SMBv2	139	✓	✓	✓*	Sitzungsdienst für die gemeinsame Nutzung von Daten *Nur für SMB erforderlich

Netzwerkelement	From	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Amazon S3	Storage-Gateway-VM	Amazon S3 S3-Serviceendpunkte	TCP HTTPS	443	✓	✓	✓	Für die Kommunikation von der Storage Gateway Gateway-VM zum AWS Service-Endpunkt. Informationen zu Dienstendpunkten finden Sie unter Zulassen des AWS Storage Gateway Gateway-Zugriffs über Firewalls und Router.

Die folgende Abbildung zeigt den Netzwerkdatenverkehr für eine einfache S3 File Gateway-Bereitstellung.



Netzwerk- und Firewall-Anforderungen für das Storage-Gateway-Hardwaregerät

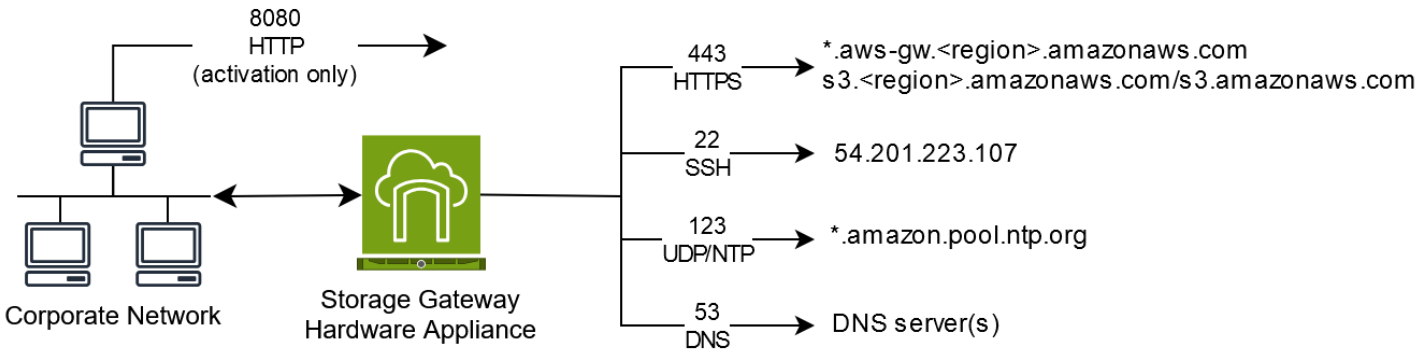
Jedes Storage-Gateway-Hardwaregerät benötigt die folgenden Netzwerkdienste:

- Internetzugriff: eine ständig aktive Internetverbindung über eine Netzwerkschnittstelle auf dem Server.
- DNS-Services: DNS-Services für die Kommunikation zwischen Hardware-Appliance und dem DNS-Server.
- Zeitsynchronisierung: ein automatisch konfigurierter Amazon NTP-Zeitservice muss verfügbar sein.
- IP-Adresse: eine zugewiesene DHCP- oder statische IPv4-Adresse. Sie können keine IPv6-Adressen zuweisen.

Auf der Rückseite des Dell PowerEdge R640-Servers befinden sich fünf physische Netzwerkanschlüsse. 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	Usage
SSH	22	Ausgehend	Hardware-Appliance	`54.201.223.107`	Support-Kanal
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

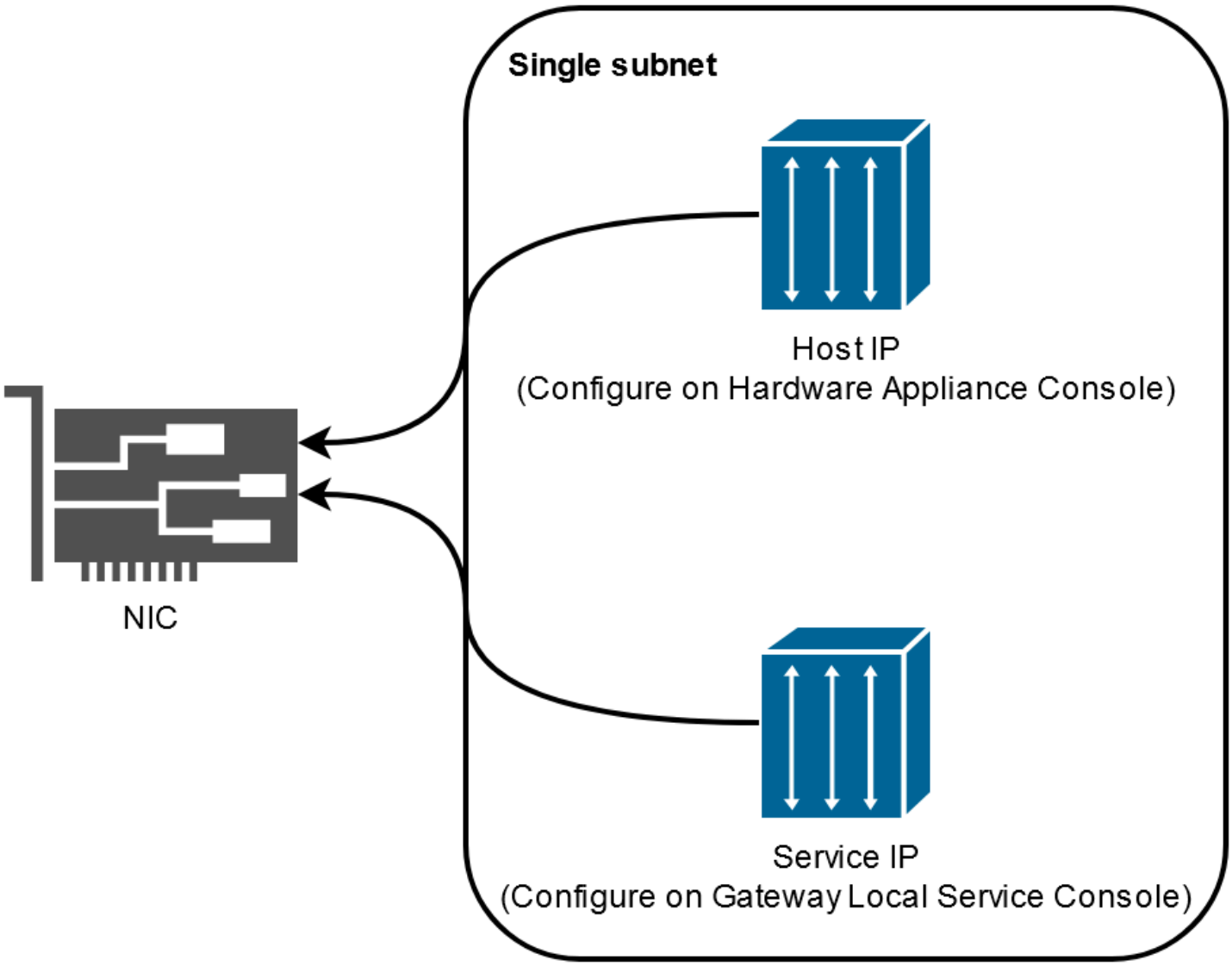
Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Usage
HTTP	8080	Eingehend	AWS	Hardware-Appliance	Aktivierung (nur kurz)

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 Konfiguration der Netzwerkparameter der Hardware-Appliance.

> **Note**
>
> Eine Abbildung, die die Rückseite des Servers mit seinen Anschlüssen zeigt, finden Sie unterPhysische Installation Ihrer Hardware-Appliance.

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 zur Aktivierung und Konfiguration einer Hardware-Appliance finden Sie unterVerwenden der AWS Storage Gateway Gateway-Hardware-Appliance.

ZulassenAWS Storage GatewayZugriff über Firewalls und Router

Ihr Gateway benötigt Zugriff auf die folgenden Storage Gateway-Dienstendpunkte, mit AWS denen es kommunizieren kann. Wählen Sie bei der Gateway-Einrichtung den Endpunkttyp für Ihr Gateway basierend auf Ihrer Netzwerkumgebung aus. Falls Sie den Netzwerkdatenverkehr mithilfe einer Firewall oder eines Routers filtern oder einschränken, müssen Sie die Firewall und den Router so konfigurieren, dass diese Service-Endpunkte für die ausgehende Kommunikation mit AWS verwendet werden dürfen.

> **Note**
>
> Wenn Sie private VPC-Endpunkte für Ihr Storage Gateway konfigurieren, die für die Verbindung und Datenübertragung von und zu verwendet werdenAWS, benötigt Ihr Gateway keinen Zugriff auf das öffentliche Internet. Weitere Informationen finden Sie unter Aktivieren eines Gateways in einer virtuellen privaten Cloud.

> **Important**
>
> Ersetzen Sie *region* in den folgenden Endpunktbeispielen die richtige AWS-Region Zeichenfolge für Ihr Gateway, z. B. `us-west-2` *amzn-s3-demo-bucket*Ersetzen Sie es durch den tatsächlichen Namen des Amazon S3 S3-Buckets in Ihrer Bereitstellung. Sie können anstelle von auch ein Sternchen (`*`) verwenden, *amzn-s3-demo-bucket* um einen Platzhaltereintrag in Ihren Firewall-Regeln zu erstellen, der es ermöglicht, den Service-Endpunkt für alle Bucket-Namen aufzulisten. Wenn Ihre Gateways AWS-Regionen in den Vereinigte Staaten oder Kanada eingesetzt werden und FIPS-konforme Endpunktverbindungen (Federal Information Processing Standard) erfordern, ersetzen Sie *s3* diese durch. `s3-fips`

Endpunkttypen

Standard-Endpunkte

Diese Endpunkte unterstützen IPv4-Verkehr zwischen Ihrer Gateway-Appliance und. AWS

Der folgende Service-Endpunkt wird von allen Gateways für Head-Bucket-Operationen benötigt.

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

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

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

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`).

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

Dual-stack Endpunkte

Diese Endpunkte unterstützen IPv4- und IPv6-Verkehr zwischen Ihrer Gateway-Appliance und. AWS

Der folgende Dual-Stack-Serviceendpunkt wird von allen Gateways für Head-Bucket-Operationen benötigt.

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

Die folgenden Dual-Stack-Dienstendpunkte werden von allen Gateways für den Betrieb von Steuerpfaden (Aktivierung, Steuerungsebene, Proxy) und Datenpfadoperationen (Datenebene) benötigt.

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

Der folgende Gateway-Dual-Stack-Serviceendpunkt ist für API-Aufrufe erforderlich.

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

Das folgende Beispiel ist ein Gateway-Dual-Stack-Serviceendpunkt in der Region USA West (Oregon) (`us-west-2`).

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

Amazon S3 S3-Serviceendpunkte

Amazon S3 File Gateway benötigt die folgenden drei Arten von Endpunkten, um eine Verbindung zum Amazon S3 S3-Service herzustellen:

Amazon S3 S3-Serviceendpunkt

> **Note**
>
> Nur für diesen Endpunkt, ersetzen Sie ihn nicht `s3` durch `s3-fips` für FIPS-compliant Bereitstellungen.

```
s3.amazonaws.com
```

Regionale Amazon S3 S3-Endpunkte

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

Das folgende Beispiel zeigt einen regionalen Amazon S3 S3-Endpunkt in der Region USA Ost (Ohio) (`us-east-2`).

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

Das folgende Beispiel zeigt regionale Standard- und Dual-Stack-Endpunkte von FIPS-compliant Amazon S3 in der Region USA West (Nordkalifornien) (`us-west-1`).

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

Die folgenden Beispiele zeigen die regionalen Standard- und Dual-Stack-Endpunkte von Amazon S3, die von AWS GovCloud (US) Regionen verwendet werden:

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

```
s3.dualstack.us-gov-east-1.amazonaws.com (AWSGovCloud (US-East) Region (Dual-stack))
s3.dualstack.us-gov-west-1.amazonaws.com (AWSGovCloud (US-West) Region (Dual-stack))
```

> **Note**
>
> Wenn Ihr Gateway nicht ermitteln kann, AWS-Region wo sich Ihr Amazon S3 S3-Bucket befindet, ist dieser Service-Endpunkt standardmäßig auf `s3.us-east-1.amazonaws.com` eingestellt. Wir empfehlen Ihnen, den Zugriff auf die Region USA Ost (Nord-Virginia) (`us-east-1`) zusätzlich zu der Region, in der Ihr Gateway aktiviert ist und AWS-Regionen wo sich Ihr Amazon S3 S3-Bucket befindet, zuzulassen.

Amazon S3 S3-Bucket-Endpunkte

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

Die folgenden Beispiele zeigen Standard- und Dual-Stack-Amazon S3-Bucket-Endpunkte für einen Bucket, der *amzn-s3-demo-bucket* in der Region USA Ost (Ohio) benannt ist (`us-east-2`).

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

Die folgenden Beispiele zeigen Standard- und FIPS-compliant Dual-Stack-Amazon S3-Bucket-Endpunkte für einen Bucket mit *amzn-s3-demo-bucket1* dem Namen AWS GovCloud (US-East) Region ()`us-gov-east-1`.

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

Zusätzlich zu den Service-Endpunkten Storage Gateway und Amazon S3 benötigen Storage Gateway Gateway-VMs auch Netzwerkzugriff auf die folgenden NTP-Server:

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

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

Weitere Informationen zu unterstützten Endpunkten AWS-Regionen und Service-Endpunkten finden Sie unter Storage Gateway in der Allgemeine AWS-Referenz.

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

In AWS Storage Gateway steuert 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.

  Wenn Sie Instances erlauben müssen, sich von außerhalb der Sicherheitsgruppe mit dem Gateway zu verbinden, empfehlen wir, dass Sie Verbindungen nur über Port 80 (zur Aktivierung) zulassen.
- Wenn Sie Ihr Gateway über einen Amazon-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 den Zugriff auf Port 22 nur, wenn Sie Support ihn zur Fehlerbehebung verwenden. Weitere Informationen finden Sie unter Sie Support möchten bei der Fehlerbehebung für Ihr Amazon EC2 EC2-Gateway helfen.

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

Unterstützte Hypervisoren und Host-Anforderungen

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

> **Note**
>
> Der UEFI-Startmodus mit deaktiviertem Secure Boot (loader_secure=no) ist für File Gateway 2.x, Volume Gateway 3.x und Tape Gateway 3.x erforderlich. Eine XML-Datei wird mit jedem Qcow-Download als Schnellkonfiguration mitgeliefert.

Storage Gateway unterstützt die folgenden Hypervisor-Versionen und Hosts:

- VMware ESXi Hypervisor (Version 7.0 oder 8.0) — Für dieses Setup benötigen Sie außerdem einen VMware vSphere-Client, um eine Verbindung zum Host herzustellen.
- Microsoft Hyper-V Hypervisor (2019, 2022 oder 2025) — Für dieses Setup benötigen Sie einen Microsoft Hyper-V Manager auf einem Microsoft Windows-Client-Computer, um eine Verbindung zum Host herzustellen.
- Linux Kernel-based Virtual Machine (KVM) — Eine kostenlose Open-Source-Virtualisierungstechnologie. KVM ist in allen Versionen von Linux Version 2.6.20 und neuer enthalten. Storage Gateway wurde für die Distributionen CentOS/RHEL 7.7, RHEL 8.6, Ubuntu 16.04 LTS und Ubuntu 18.04 LTS 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. In der mitgelieferten Datei aws-storage-gateway.xml finden Sie empfohlene Startkonfigurationen. Der UEFI-Startmodus mit deaktiviertem Secure Boot (loader_secure=no) ist für File Gateway 2.x, Volume Gateway 3.x und Tape Gateway 3.x erforderlich.
- Nutanix AHV (Acropolis Hypervisor) ab Version 10.0.1.1 — Eine Virtualisierungsplattform, die in die Nutanix Hyper-Converged Infrastructure (HCI) -Lösung integriert ist. KVM-based
- Amazon-EC2-Instance: Storage Gateway stellt ein Amazon Machine Image (AMI) mit dem Abbild der Gateway-VM bereit. Weitere Informationen zur Bereitstellung von Gateways in Amazon EC2 finden Sie unter Stellen Sie einen Amazon EC2 EC2-Standardhost für S3 File Gateway bereit.
- Storage Gateway Hardware Appliance — Storage Gateway bietet eine physische Hardware-Appliance als lokale Bereitstellungsoption für Standorte mit begrenzter VM-Infrastruktur.

> **Note**
>
> Die Wiederherstellung eines Gateways von einer VM, die aus einem Snapshot oder Klon einer anderen Gateway-VM oder aus Ihrem Amazon-EC2-Computerabbild (AMI) erstellt wurde, wird von Storage Gateway nicht unterstützt. 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 Wiederherstellung nach dem unerwarteten Herunterfahren einer virtuellen Maschine.
Dynamischer Speicher und virtuelle Speicherballonierung werden von Storage Gateway nicht unterstützt.

Unterstützte NFS- und SMB-Clients für File Gateway

File Gateway unterstützt die folgenden Clients:

Version des Betriebssystems	Kernel-Version	Unterstützte Protokolle
Amazon Linux 2023	6.1 LTS	NFSv4.1, NFSv3
Amazon Linux 2	5,10 L	NFSv4.1, NFSv3
RHEL 9	5,14	NFSv4.1, NFSv3
REGEL 8.10	4,18	NFSv4.1, NFSv3
SUSE 15	6.4	NFSv4.1, NFSv3
Ubuntu 24.04 LTS	6,8 LTS	NFSv4.1, NFSv3
Ubuntu 22.04 LTS	5,15 L	NFSv4.1, NFSv3
Microsoft Windows Server 2025		SMBv2, SMBv3, NFSv3
Microsoft Windows Server 2022		SMBv2, SMBv3, NFSv3
Microsoft Windows 11		SMBv2, SMBv3, NFSv3
Microsoft Windows 10		SMBv2, SMBv3, NFSv3

> **Note**
>
> Für die SMB-Verschlüsselung (Server Message Block) sind Clients erforderlich, die SMB v3-Dialekte unterstützen.

Unterstützte Dateisystemoperationen für File Gateway

Der NFS- oder SMB-Client kann Dateien schreiben, lesen, löschen und kürzen. Wenn Clients Schreibvorgänge an sendenAWS Storage Gateway, wird synchron in den lokalen Cache geschrieben. 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 entfernte Objekte aus Amazon S3. Verzeichnisse werden in S3 als Ordnerobjekte verwaltet, wobei dieselbe Syntax wie in der Amazon S3 S3-Konsole verwendet wird.

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).

Verwaltung lokaler Festplatten für Ihr Gateway

Die virtuelle Maschine (VM) des Gateways verwendet die lokalen Festplatten, die Sie vor Ort zuweisen, als Puffer und Speicher. Ein File Gateway, das Sie auf einer Amazon EC2 EC2-Instance erstellen, verwendet Amazon EBS-Volumes als lokale Festplatten. Sie müssen die Anzahl und Größe von Festplatten bestimmen, die Sie Ihrem Gateway zuweisen möchten. Das Gateway verwendet den von Ihnen zugewiesenen Cache-Speicher, um Zugriff mit niedriger Latenz auf Ihre kürzlich abgerufenen Daten zu ermöglichen. Der Cache-Speicher dient als lokaler, dauerhafter Speicher für Daten, deren Upload auf Amazon S3 Amazon aussteht. File Gateways benötigen mindestens eine 150-GiB-Festplatte, um sie als Cache zu verwenden. Nach der Erstkonfiguration und Bereitstellung Ihres Gateways können Sie weitere Festplatten für den Cache-Speicher hinzufügen, wenn Ihre Arbeitslastanforderungen steigen. Dieser Abschnitt enthält die folgenden Themen, in denen Konzepte und Verfahren im Zusammenhang mit der Verwaltung lokaler Festplatten beschrieben werden.

Topics

- Bestimmen der Größe des lokalen Festplattenspeichers- Erfahren Sie, wie Sie die Anzahl und Größe der lokalen Cache-Festplatten ermitteln, die Sie Ihrem File Gateway zuweisen möchten.
- Konfiguration von zusätzlichem Cache-Speicher- Erfahren Sie, wie Sie die Cache-Speicherkapazität Ihres File Gateways erhöhen können, wenn sich Ihre Anwendungsanforderungen ändern.
- Verwendung von kurzlebigem Speicher mit EC2-Gateways- Erfahren Sie, wie Sie Datenverlust verhindern können, wenn Sie kurzlebigen Festplattenspeicher mit File Gateway verwenden.

Bestimmen der Größe des lokalen Festplattenspeichers

Wenn Sie ein S3 File Gateway bereitstellen, sollten Sie berücksichtigen, wie viel Cache-Laufwerk Sie zuweisen möchten. S3 File Gateway verwendet einen Algorithmus, der zuletzt verwendet wurde, um Daten automatisch aus dem Cache zu entfernen. Der Cache auf einem S3 File Gateway wird von allen Dateifreigaben auf diesem Gateway gemeinsam genutzt. Wenn Sie über mehrere aktive Shares verfügen, sollten Sie beachten, dass eine hohe Auslastung auf einem Share die Menge an Cache-Ressourcen, auf die ein anderes Share Zugriff hat, beeinflussen kann, was sich möglicherweise auf die Leistung auswirken kann.

Bei der Bestimmung, wie viel Cache-Laufwerk Sie für einen bestimmten Workload benötigen, ist es wichtig zu beachten, dass Sie Ihrem Gateway jederzeit eine Cache-Festplatte hinzufügen können (bis zu den aktuellen Kontingenten auf S3 File Gateway), aber Sie können den Cache für ein bestimmtes Gateway nicht verringern. Sie können eine grundlegende Analyse des Datensatzes durchführen, um die richtige Größe der Cache-Festplatte zu bestimmen, aber es gibt keine Möglichkeit, genau zu bestimmen, wie viele Daten „heiß“ sind und lokal gespeichert werden müssen, und wie viele Daten „kalt“ sind und in der Cloud gespeichert werden können. Workloads ändern sich im Laufe der Zeit, und S3 File Gateway bietet Flexibilität und Elastizität in Bezug auf die Menge der Ressourcen, die verbraucht werden können. Die Größe des Caches kann jederzeit erhöht werden. Daher ist es oft der kostengünstigste Ansatz, klein anzufangen und ihn nach Bedarf zu erhöhen.

Sie können beim Gateway-Setup eine anfängliche Näherung von 150 GiB verwenden, um Festplatten für den Cache-Speicher bereitzustellen. Anschließend können Sie die CloudWatch Betriebsmetriken von Amazon verwenden, um die Cache-Speichernutzung zu überwachen und bei Bedarf mehr Speicherplatz über die Konsole bereitzustellen. Weitere Informationen zur Verwendung der Metriken und dem Einrichten von Alarmen finden Sie unter Leistung und Optimierung.

> **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 selben Datenspeicher wie die VM oder in einem anderen Datenspeicher zu speichern. Wenn Sie mehr als einen Datenspeicher haben, empfehlen wir Ihnen dringend, einen Datenspeicher für den Cache-Speicher auszuwählen. Ein Datenspeicher, der nur von einer zugrunde liegenden physischen Festplatte unterstützt wird, kann in manchen Situationen zu Leistungseinbußen führen, wenn er für die Sicherung beider Cachespeicher verwendet wird. Dies gilt auch, wenn die Sicherung ist eine weniger leistungsfähige RAID-Konfiguration wie RAID 1 ist.

Konfiguration von zusätzlichem Cache-Speicher

Wenn sich Ihre Anwendungsanforderungen ändern, können Sie die Cache-Speicherkapazität des Gateways erhöhen. Sie können Ihrem Gateway Speicherkapazität hinzufügen, ohne die Funktionalität zu stören oder Ausfallzeiten zu verursachen. Weitere Speicherkapazität wird bei laufender Gateway-VM hinzugefügt.

> **Important**
>
> Wenn Sie einem vorhandenen Gateway Cache hinzufügen, müssen Sie neue Festplatten auf dem Gateway-Host-Hypervisor oder der Amazon EC2 EC2-Instance erstellen. Entfernen oder ändern Sie nicht die Größe vorhandener Festplatten, die bereits als Cache zugewiesen wurden.

Um zusätzlichen Cache-Speicher für Ihr Gateway zu konfigurieren

1. Stellen Sie eine oder mehrere neue Festplatten auf Ihrem Gateway-Host-Hypervisor oder in Ihrer Amazon-EC2-Instance bereit. Weitere Informationen dazu, wie Sie einen Datenträger in einem Hypervisor bereitstellen, finden Sie in der Dokumentation zu Ihrem Hypervisor. Informationen zur Bereitstellung von Amazon-EBS-Volumes für eine Amazon-EC2-Instance finden Sie unter Amazon-EBS-Volumes im Benutzerhandbuch für die Amazon Elastic Compute Cloud für Linux-Instances. In den folgenden Schritten konfigurieren Sie diese Festplatte als Cache-Speicher.

2. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
3. Wählen Sie im Navigationsbereich Gateways aus.
4. Suchen Sie nach Ihrem Gateway und wählen Sie es aus der Liste aus.
5. Wählen Sie im Menü Aktionen die Option Cache-Speicher konfigurieren aus.
6. Identifizieren Sie im Abschnitt Cache-Speicher konfigurieren die Festplatten, die Sie bereitgestellt haben. Wenn Ihre Festplatten nicht angezeigt werden, wählen Sie das Symbol „Aktualisieren“ aus, um die Liste zu aktualisieren. Wählen Sie für jede Festplatte im Dropdownmenü Zugewiesen für die Option Cache aus.

   > **Note**
   >
   > Cache ist die einzige verfügbare Option für die Zuweisung von Festplatten auf einem File Gateway.

7. Wählen Sie Änderungen speichern aus, um die Konfigurationseinstellungen zu speichern.

Verwendung 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.

Ephemere Festplatten bieten temporären Speicher auf Blockebene für Ihre Amazon EC2 EC2-Instance. Ephemere Festplatten eignen sich ideal für die temporäre Speicherung von Daten, die sich häufig ändern, z. B. Daten im Cache-Speicher eines Gateways. Wenn Sie Ihr Gateway mit einem Amazon EC2 Amazon Machine Image starten und der von Ihnen gewählte Instance-Typ kurzlebigen Speicher unterstützt, werden die kurzlebigen Festplatten automatisch aufgelistet. Sie können eine der Festplatten auswählen, um die Cache-Daten Ihres Gateways zu speichern. Weitere Informationen finden Sie im Amazon EC2 EC2-Instance-Speicher im Amazon EC2 EC2-Benutzerhandbuch.

Daten, die Anwendungen auf das Gateway schreiben, werden synchron im Cache auf den kurzlebigen Festplatten gespeichert und dann asynchron in einen dauerhaften Speicher in Amazon S3 for Windows File Server hochgeladen. Wenn die Amazon EC2 EC2-Instance gestoppt wird, nachdem Daten in den temporären Speicher geschrieben wurden, aber bevor ein asynchroner Upload stattfindet, können alle Daten, die noch nicht auf Amazon S3 Server hochgeladen wurden, verloren gehen. Sie können einen solchen Datenverlust verhindern, indem Sie die Schritte befolgen, bevor Sie die EC2-Instance, die Ihr Gateway hostet, neu starten oder beenden.

> **Important**
>
> Wenn Sie flüchtigen Speicher verwenden und Ihr Amazon-EC2-Gateway anhalten und starten, ist das Gateway dauerhaft offline. Dies geschieht, weil der physische Speicherdatenträger ersetzt wird. Für dieses Problem gibt es keine Lösung. Die einzige Lösung besteht darin, das Gateway zu löschen und ein neues auf einer neuen EC2-Instance zu aktivieren.

Die Schritte in diesem folgenden Verfahren sind spezifisch für File Gateways.

Um Datenverlust in File Gateways zu verhindern, die kurzlebige Festplatten verwenden

1. Stoppen Sie alle Prozesse, die in Amazon S3 schreiben.
2. Abonnieren Sie, um Benachrichtigungen von CloudWatch Events zu erhalten. Weitere Informationen finden Sie unter Über Dateioperationen benachrichtigt werden.
3. Rufen Sie die NotifyWhenUploaded API auf, um benachrichtigt zu werden, wenn geschriebene Daten dauerhaft in Amazon S3 gespeichert wurden, bis der kurzlebige Speicher verloren ging.
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 Metriken zur Dateifreigabe verstehen.
6. Sie können das File Gateway jetzt neu starten oder beenden, ohne dass das Risiko besteht, Daten zu verlieren.

Verwenden der AWS Storage Gateway Gateway-Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Die AWS Storage Gateway Hardware Appliance ist eine physische Hardware-Appliance, bei der die Storage Gateway Gateway-Software auf einer validierten Serverkonfiguration vorinstalliert ist. Sie können die Hardware-Appliances in Ihrer Bereitstellung über die Hardware-Appliance-Übersichtsseite in der AWS Storage Gateway Konsole verwalten.

Bei der Hardware-Appliance handelt es sich um einen hoch leistungsfähigen 1U-Server, den Sie in Ihrem Rechenzentrum oder On-Premises hinter Ihrer Unternehmens-Firewall bereitstellen können. Wenn Sie Ihre Hardware-Appliance kaufen und aktivieren, ordnet der Aktivierungsprozess die Hardware-Appliance Ihrer zu AWS-Konto. Nach der Aktivierung wird Ihre Hardware-Appliance in der Konsole auf der Übersichtsseite der Hardware-Appliance angezeigt. Sie können die Hardware-Appliance als Typ S3 File Gateway, FSx File Gateway, Tape Gateway oder Volume Gateway konfigurieren. Das Verfahren, mit dem Sie diese Gateway-Typen auf einer Hardware-Appliance bereitstellen, ist dasselbe wie auf einer virtuellen Plattform.

Eine Liste der unterstützten Regionen, AWS-Regionen in denen die AWS Storage Gateway Gateway-Hardware-Appliance aktiviert und verwendet werden kann, finden Sie unter Regionen der AWS Storage Gateway Gateway-Hardware-Appliance in der Allgemeine AWS-Referenz.

In den folgenden Abschnitten finden Sie Anweisungen zur Einrichtung, Rackmontage, Stromversorgung, Konfiguration, Aktivierung, Inbetriebnahme, Verwendung und Löschung einer AWS Storage Gateway Hardware-Appliance.

Themen

Einrichtung Ihrer AWS Storage Gateway Gateway-Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Nachdem Sie Ihre Storage Gateway Gateway-Hardware-Appliance erhalten haben, verwenden Sie die lokale Hardware-Appliance-Konsole, um das Netzwerk so zu konfigurieren, dass eine ständige Verbindung zu Ihrer Appliance hergestellt AWS und diese aktiviert wird. Bei der Aktivierung wird Ihre Appliance mit dem AWS Konto verknüpft, das während des Aktivierungsvorgangs verwendet wird. Nachdem die Appliance aktiviert wurde, können Sie ein S3 File Gateway, FSx File Gateway, Tape Gateway oder Volume Gateway von der Storage Gateway Gateway-Konsole aus starten.

Um die Hardware-Appliance zu installieren und zu konfigurieren, führen Sie folgende Schritte aus

1. Mounten Sie die Appliance in einem Rack und schließen Sie Strom- und Netzwerkkabel an. Weitere Informationen finden Sie unter Physische Installation Ihrer Hardware-Appliance.

2. Stellen Sie die Internetprotokolladressen der Version 4 (IPv4) für die Hardware-Appliance (den Host) ein. Weitere Informationen finden Sie unter Konfiguration der Netzwerkparameter der Hardware-Appliance.
3. Aktivieren Sie die Hardware-Appliance auf der Konsolen-Übersichtsseite der Hardware-Appliance in der AWS Region Ihrer Wahl. Weitere Informationen finden Sie unter Aktivierung Ihrer AWS Storage Gateway Gateway-Hardware-Appliance.
4. Erstellen Sie ein Gateway auf Ihrer Hardware-Appliance. Weitere Informationen finden Sie unter Erstellen Sie Ihr Gateway.

   Sie richten Gateways auf Ihrer Hardware-Appliance auf die gleiche Weise ein, wie Sie Gateways auf VMware ESXi, Microsoft Hyper-V, Linux kernelbasierter 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. Dadurch wird ein größerer Cache für den Zugriff auf eingehende Daten mit geringer Latenz bereitgestellt AWS. Wenn Sie das 5-TB-Modell bestellt haben, können Sie den nutzbaren Speicher auf 12 TB erhöhen, indem Sie fünf 1,92-TB-Laufwerke SSDs (Solid-State-Laufwerke) kaufen.

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

1. Setzen Sie die Hardware-Appliance auf die Werkseinstellungen zurück. Wenden Sie sich an den AWS Support, um Anweisungen dazu zu erhalten.
2. Fügen Sie der Appliance fünf 1,92 TB SSDs hinzu.

Optionen für Netzwerkschnittstellenkarte

Je nach Modell der Appliance, die Sie bestellt haben, kann sie mit einer RJ45 10G-Base-T-Kupfer- oder einer 10G-DA/SFP+-Netzwerkkarte geliefert werden.

- Konfiguration mit 10 NICs: G-Base-T
  - Verwenden Sie CAT6 Kabel für 10G oder CAT5 (e) für 1G
- 10G DA/SFP+ NIC-Konfiguration:
  - Verwenden Sie Twinax-Kupfer-Direktanschlusskabel bei einer Entfernung von bis zu 5 Metern

- Dell/Intel-kompatible optische SFP+-Module (SR oder LR)
- SFP/SFP+ Kupfer-Transceiver für 1 oder 10G-Base-T G-Base-T

Physische Installation Ihrer Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Bei Ihrer Appliance handelt es sich um einen 1U-Server, der in ein 19-Zoll-Rack nach dem International Electrotechnical Commission (IEC)-Branchenstandard passt.

Voraussetzungen

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

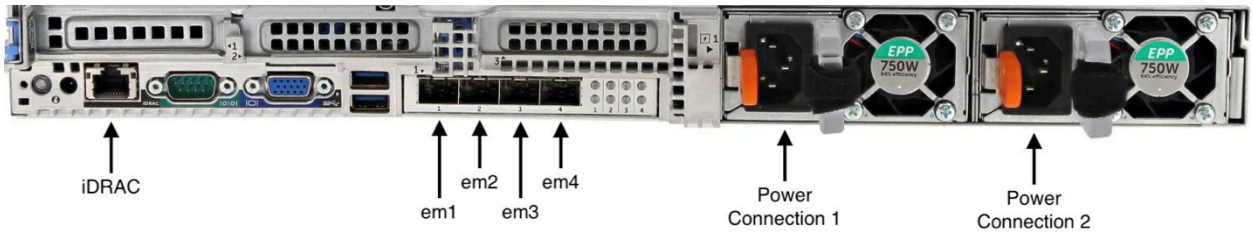
- Stromkabel: Benötigt wird ein Stromkabel. empfohlen werden zwei Stromkabel.
- Unterstützte Netzwerkverkabelung (abhängig davon, welche Netzwerkschnittstellenkarte (NIC) in der Hardware-Appliance enthalten ist). Twinax Copper DAC, optisches SFP+-Modul (Intel-kompatibel) oder SFP-Base-T-Kupfer-Transceiver.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

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

Um Ihre Hardware-Appliance physisch zu installieren

1. Entpacken Sie Ihre Hardware-Appliance und folgen Sie den Anweisungen in der Verpackung, um den Server im Rack zu montieren.

   Die folgende Abbildung zeigt die Rückseite der Hardware-Appliance mit Anschlüssen für Strom, Ethernet, Monitor, USB-Tastatur und iDRAC.
   Hardware-Appliance auf der Rückseite mit Etiketten für Netzwerk- und Stromanschlüsse.

   Hardware-Gerät auf einer Rückseite mit Netzwerk- und Stromanschlussetiketten.

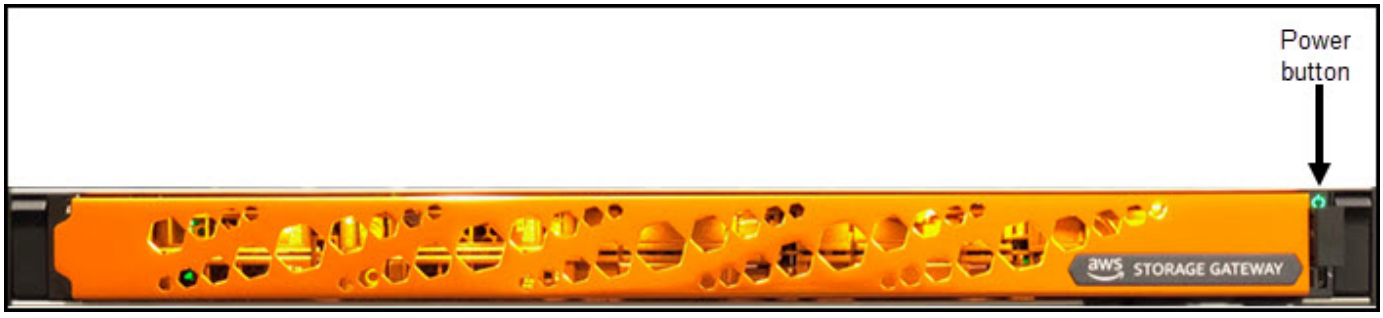
2. Schließen Sie an beide Netzteile ein Stromkabel an. Es ist möglich, nur einen Stromanschluss anzuschließen, aus Redundanzgründen empfehlen wir jedoch, beide Netzteile mit Strom zu verbinden.

3. 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.

4. Schließen Sie die Tastatur und den Monitor an.

5. Schalten Sie den Server durch Drücken der Taste Power (Ein/Aus) an der Vorderseite ein wie im folgenden Bild gezeigt.
   Vorderseite der Hardware-Appliance mit Netzschalter-Etikett.

Vorderseite der Hardware-Appliance mit Netzschalter-Etikett.

Nächster Schritt

Zugriff auf die Hardware-Appliance-Konsole

Zugriff auf die Hardware-Appliance-Konsole

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Wenn Sie Ihre Hardware-Appliance einschalten, erscheint die Hardware-Appliance-Konsole auf dem Monitor. Die Hardware-Appliance-Konsole bietet eine spezielle Benutzeroberfläche AWS , mit der Sie ein Administratorkennwort festlegen, anfängliche Netzwerkparameter konfigurieren und einen Support-Kanal öffnen können AWS.

Um mit der Hardware-Appliance-Konsole zu arbeiten, geben Sie Text über die Tastatur ein und bewegen Sie sich mit den `Left Arrow` Tasten Up `DownRight`,, und auf dem Bildschirm in die angegebene Richtung. 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.

Wenn die Hardware-Appliance-Konsole zum ersten Mal angezeigt wird, wird die Willkommensseite angezeigt, und Sie werden aufgefordert, ein Passwort für das Administrator-Benutzerkonto festzulegen, bevor Sie auf die Konsole zugreifen können.

Um ein Admin-Passwort festzulegen

- Gehen Sie bei der Aufforderung Bitte geben Sie Ihr Login-Passwort ein wie folgt vor:

a. Geben Sie in Set Password (Passwort festlegen) ein Passwort ein und drücken Sie anschließend `Down arrow`.

b. Geben Sie das Passwort in Confirm (Bestätigen) erneut ein und wählen Sie dann Save Password (Passwort speichern) aus.

Nachdem Sie Ihr Passwort festgelegt haben, wird die Startseite der Hardwarekonsole angezeigt. Auf der Startseite werden Netzwerkinformationen für die Netzwerkschnittstellen em1, em2, em3 und em4 angezeigt. Sie enthält die folgenden Menüoptionen:

- Konfigurieren des Netzwerks
- Öffnen Sie die Service Console
- Passwort ändern
- Loggen Sie sich ab
- Support-Konsole öffnen

Nächster Schritt

Konfiguration der Netzwerkparameter der Hardware-Appliance

Konfiguration der Netzwerkparameter der Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Nachdem die Hardware-Appliance hochgefahren ist und Sie Ihr Admin-Benutzerkennwort in der Hardwarekonsole wie unter beschrieben festgelegt habenZugriff auf die Hardware-Appliance-Konsole, konfigurieren Sie mithilfe des folgenden Verfahrens die Netzwerkparameter, mit denen Ihre Hardware-Appliance eine Verbindung herstellen kann. AWS

So richten Sie eine Netzwerkadresse ein

1. Wählen Sie auf der Startseite die Option Netzwerk konfigurieren aus und drücken Sie dann auf`Enter`. Die Seite „Netzwerk konfigurieren“ wird angezeigt. Auf der Seite „Netzwerk konfigurieren“ werden IP- und DNS-Informationen für jede der vier Netzwerkschnittstellen auf der Hardware-Appliance angezeigt. Sie enthält auch Menüoptionen zur Konfiguration von DHCP - oder statischen Adressen für jede dieser Schnittstellen.
2. Gehen Sie für die em1-Schnittstelle wie folgt vor:

   - Wählen Sie DHCP und drücken Sie`Enter`, um die IPv4 Adresse zu verwenden, die Ihr DHCP-Server (Dynamic Host Configuration Protocol) Ihrem physischen Netzwerkport zugewiesen hat.

     Notieren Sie sich diese Adresse für die spätere Verwendung im Aktivierungsschritt.
   - Wählen Sie Statisch und drücken Sie`Enter`, um eine statische IPv4 Adresse zu konfigurieren.

     Geben Sie eine gültige IP-Adresse, Subnetzmaske, Gateway und DNS-Serveradresse für die em1-Netzwerkschnittstelle ein.

     Wenn Sie fertig sind, wählen Sie Speichern und drücken Sie dann`Enter`, um die Konfiguration zu speichern.

   > **Note**
   >
   > Sie können dieses Verfahren verwenden, um neben em1 auch andere Netzwerkschnittstellen zu konfigurieren. Wenn Sie andere Schnittstellen konfigurieren, müssen diese dieselbe Always-On-Verbindung zu den in den Anforderungen aufgeführten AWS Endpunkten bereitstellen.
   > Network Bonding und Link Aggregation Control Protocol (LACP) werden von der Hardware-Appliance oder vom Storage Gateway nicht unterstützt.
   > Es wird nicht empfohlen, mehrere Netzwerkschnittstellen im selben Subnetz zu konfigurieren, da dies manchmal zu Routing-Problemen führen kann.

So melden Sie sich von der Hardwarekonsole ab

1. Wählen Sie Zurück und drücken Sie`Enter`, um zur Startseite zurückzukehren.

2. Wählen Sie Abmelden und drücken Sie`Enter`, um zur Willkommensseite zurückzukehren.

Nächster Schritt

[Aktivierung Ihrer AWS Storage Gateway Gateway-Hardware-Appliance]

Aktivierung Ihrer AWS Storage Gateway Gateway-Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Nachdem Sie Ihre IP-Adresse konfiguriert haben, geben Sie diese IP-Adresse auf der Hardware-Seite der AWS Storage Gateway Konsole ein, um Ihre Hardware-Appliance zu aktivieren. Der Aktivierungsprozess registriert die Appliance in Ihrem AWS Konto.

Sie können wählen, ob Sie Ihre Hardware-Appliance in einer der unterstützten Anwendungen aktivieren möchten AWS-Regionen. Eine Liste der unterstützten AWS-Regionen Regionen finden Sie unter Storage Gateway Gateway-Hardware-Appliance-Regionen in der Allgemeine AWS-Referenz.

So aktivieren Sie Ihre AWS Storage Gateway Gateway-Hardware-Appliance

1. Öffnen Sie die AWS Storage Gateway -Managementkonsole und melden Sie sich mit den Kontoanmeldeinformationen an, mit denen Sie Ihre Hardware aktivieren möchten.

   > **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 im Navigationsmenü auf der linken Seite Hardware aus.
3. Wählen Sie Appliance aktivieren aus.
4. Geben Sie für IP-Adresse die IP-Adresse ein, die Sie für Ihre Hardware-Appliance konfiguriert haben, und wählen Sie dann Verbinden aus.

   Weitere Informationen zur Konfiguration der IP-Adresse finden Sie unter Konfigurieren von Netzwerkparametern .
5. Geben Sie in Name einen Namen für Ihre Appliance ein. Namen können bis zu 255 Zeichen enthalten. Sie dürfen keinen Schrägstrich enthalten.
6. Geben Sie für Zeitzone der Hardware-Appliance die lokale Zeitzone ein, in der der Großteil des Workloads für das Gateway generiert wird. Wählen Sie dann Weiter aus.

   Die Zeitzone legt fest, wann Hardware-Updates ausgeführt werden. Standardmäßig werden Updates um 2 Uhr morgens ausgeführt. Idealerweise finden Updates, wenn die Zeitzone richtig eingestellt ist, standardmäßig außerhalb des lokalen Arbeitszeitfensters statt.
7. Überprüfen Sie die Aktivierungsparameter im Bereich „Detail der Hardware-Appliance“. Wählen Sie Vorherige aus, um zurückzugehen und Änderungen vorzunehmen, falls nötig. Wählen Sie andernfalls Aktivieren aus, um die Aktivierung abzuschließen.

Auf der Seite Hardware-Appliance-Übersicht wird ein Banner angezeigt, das die erfolgreiche Aktivierung der Hardware-Appliance bestätigt.

An diesem Punkt ist die Appliance mit Ihrem Konto verknüpft. Der nächste Schritt besteht darin, ein S3 File Gateway, FSx File Gateway, Tape Gateway oder Volume Gateway auf der neuen Appliance zu konfigurieren und zu starten.

Nächster Schritt

Erstellen Sie ein Gateway auf Ihrer Hardware-Appliance

Erstellen Sie ein Gateway auf Ihrer Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Sie können ein S3 File Gateway, FSx File Gateway, Tape Gateway oder Volume Gateway auf jeder AWS Storage Gateway Gateway-Hardware-Appliance in Ihrer Bereitstellung erstellen.

So erstellen Sie einen Gateway auf Ihrer Hardware-Appliance

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause.
2. Folgen Sie den unter Creating Your Gateway beschriebenen Verfahren, um den Storage Gateway Gateway-Typ, den Sie bereitstellen möchten, einzurichten, eine Verbindung herzustellen und zu konfigurieren.

Wenn Sie mit der Erstellung Ihres Gateways in der Storage-Gateway-Konsole fertig sind, beginnt die Storage-Gateway-Software automatisch mit der Installation auf der Hardware-Appliance. Wenn Sie das Dynamic Host Configuration Protocol (DHCP) verwenden, kann es 5 bis 10 Minuten dauern, bis ein Gateway in der Konsole als online angezeigt wird. Informationen zum Zuweisen einer statischen IP-Adresse zu Ihrem installierten Gateway finden Sie unter Konfiguration einer IP-Adresse für das Gateway.

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

Konfiguration einer Gateway-IP-Adresse auf der Hardware-Appliance

Konfiguration einer Gateway-IP-Adresse auf der Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

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-Maschine, die auf der Hardware-Appliance ausgeführt wird, eine weitere IP-Adresse zuweisen. Um einem auf Ihrer Hardware-Appliance installierten Gateway eine statische IP-Adresse zuzuweisen, konfigurieren Sie die IP-Adresse über die lokale Gateway-Konsole für dieses Gateway. Ihre Anwendungen (wie Ihr NFS- oder SMB-Client) stellen eine Verbindung zu dieser IP-Adresse her. Mit der Option Open Service Console können Sie von der Hardware-Appliance-Konsole aus auf die lokale Gateway-Konsole 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 aus und drücken Sie dann`Enter`, um die Anmeldeseite für die lokale Gateway-Konsole zu öffnen.
2. Auf der Anmeldeseite der AWS Storage Gateway lokalen Konsole werden Sie aufgefordert, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

   Das Standardkonto ist `admin` und das Standardpasswort ist `password`.

   > **Note**
   >
   > Wir empfehlen, das Standardpasswort zu ändern, indem Sie im Hauptmenü AWS Geräteaktivierung – Konfiguration die entsprechende Zahl für die Gateway-Konsole eingeben und dann den Befehl `passwd` ausführen. Weitere Informationen zum

Ausführen des Befehls finden Sie unter Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole. Sie können das Passwort auch von der Storage Gateway Gateway-Konsole aus festlegen. Weitere Informationen finden Sie unter Einstellen des Kennworts für die lokale Konsole von der Storage Gateway Gateway-Konsole aus.

3. Die Seite „AWS Geräteaktivierung — Konfiguration“ enthält die folgenden Menüoptionen:

   - HTTP/SOCKS-Proxykonfiguration
   - Netzwerkkonfiguration
   - Testen Sie die Netzwerkkonnektivität
   - Systemressourcencheck anzeigen
   - Systemzeitverwaltung
   - Informationen zur Lizenz
   - Eingabeaufforderung

   > **Note**
   >
   > Einige Optionen werden nur für bestimmte Gateway-Typen oder Hostplattformen angezeigt.

   Geben Sie die entsprechende Zahl ein, um zur Seite „Netzwerkkonfiguration“ zu gelangen.

4. Gehen Sie wie folgt vor, um die Gateway-IP-Adresse zu konfigurieren:

   - Um die von Ihrem DHCP-Server (Dynamic Host Configuration Protocol) zugewiesene IP-Adresse zu verwenden, geben Sie die entsprechende Zahl für DHCP konfigurieren ein und geben Sie dann auf der folgenden Seite gültige DHCP-Konfigurationsinformationen ein.
   - Um eine statische IP-Adresse zuzuweisen, geben Sie die entsprechende Zahl für Configure Static IP ein und geben Sie dann auf der folgenden Seite eine gültige IP-Adresse und DNS-Informationen ein.

   > **Note**
   >
   > Die IP-Adresse, die Sie hier angeben, muss sich im selben Subnetz befinden wie die IP-Adresse, die bei 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.

Mach der Aktivierung und Konfigurierung Ihrer Hardware-Appliance wird Ihre Appliance in der Konsole angezeigt. Jetzt können Sie das Setup- und Konfigurationsverfahren für Ihr Gateway in der Storage Gateway Gateway-Konsole fortsetzen. Detaillierte Anweisungen finden Sie unter Konfigurieren Ihres Amazon S3 File Gateways.

Gateway-Software von Ihrer Hardware-Appliance entfernen

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Wenn Sie ein bestimmtes Storage Gateway, das Sie auf einer Hardware-Appliance bereitgestellt haben, nicht mehr benötigen, können Sie die Gateway-Software von der Hardware-Appliance entfernen. Nachdem Sie die Gateway-Software entfernt haben, können Sie wählen, ob Sie stattdessen ein neues Gateway bereitstellen oder die Hardware-Appliance selbst aus der Storage Gateway Gateway-Konsole löschen möchten. Um Gateway-Software von Ihrer Hardware-Appliance zu entfernen, führen Sie die folgenden Schritte aus.

So entfernen Sie einen Gateway von einer Hardware-Appliance

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich auf der linken Seite der Konsolenseite Hardware aus und wählen Sie dann den Namen der Hardware-Appliance für die Appliance aus, von der Sie die Gateway-Software entfernen möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option Gateway entfernen aus.

   Das Bestätigungsdialogfeld wird angezeigt.
4. Stellen Sie sicher, dass Sie die Gateway-Software von der angegebenen Hardware-Appliance entfernen möchten, und geben Sie dann das Wort `remove` in das Bestätigungsfeld ein.
5. Wählen Sie Entfernen, um die Gateway-Software dauerhaft zu entfernen.

> **Note**
>
> Nachdem Sie die Gateway-Software entfernt haben, 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 Sie Ihr Gateway und entfernen Sie die zugehörigen 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 AWS Storage Gateway Gateway-Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren

Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

Wenn Sie eine AWS Storage Gateway Gateway-Hardware-Appliance, die Sie bereits aktiviert haben, nicht mehr benötigen, können Sie die Appliance vollständig aus Ihrem AWS Konto löschen.

> **Note**
>
> Um Ihre Appliance auf ein anderes AWS Konto zu verschieben oder AWS-Region, müssen Sie sie zunächst wie folgt löschen, dann den Support-Kanal des Gateways öffnen und Kontakt aufnehmen, Support um einen Soft-Reset durchzuführen. Weitere Informationen finden Sie unter Support Zugriff aktivieren, um Probleme mit Ihrem lokal gehosteten Gateway zu beheben. Aktivieren Sie den Support Zugriff, um Probleme mit Ihrem lokal .

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 unter Gateway-Software von Ihrer Hardware-Appliance entfernen.
2. Wählen Sie auf der Hardware-Seite der Storage-Gateway-Konsole die Hardware-Appliance, die Sie löschen möchten.
3. Wählen Sie unter Aktionen die Option Appliance löschen aus. Das Bestätigungsdialogfeld wird angezeigt.
4. Vergewissern Sie sich, dass Sie die angegebene Hardware-Appliance löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen.

   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 selbst.

Erstellen Sie Ihr Gateway

Die Übersichtsabschnitte auf dieser Seite bieten eine allgemeine Zusammenfassung der Funktionsweise des Storage Gateway Gateway-Erstellungsprozesses. step-by-stepVerfahren zum Erstellen eines bestimmten Gateway-Typs mithilfe der Storage Gateway Gateway-Konsole finden Sie in den folgenden Themen:

- Erstellen und Aktivieren eines Amazon S3 File Gateways
- Erstellen und aktivieren Sie ein Amazon FSx File Gateway
- Erstellen und aktivieren Sie ein Tape Gateway
- Erstellen und aktivieren Sie ein Volume Gateway

Überblick – Gateway-Aktivierung

Die Gateway-Aktivierung umfasst die Einrichtung Ihres Gateways, die Verbindung zu diesem AWS, die Überprüfung Ihrer Einstellungen und die Aktivierung.

Einrichten eines Gateways

Um Ihr Storage Gateway einzurichten, wählen Sie zunächst den Gateway-Typ aus, den Sie erstellen möchten, und die Hostplattform, auf der Sie die virtuelle Gateway-Appliance ausführen möchten. Anschließend laden Sie die Vorlage für die virtuelle Gateway-Appliance für die Plattform Ihrer Wahl herunter und stellen sie in Ihrer On-Premises-Umgebung bereit. Sie können Ihr Storage Gateway auch als physische Hardware-Appliance einsetzen, die Sie bei Ihrem bevorzugten Händler bestellen, oder als Amazon EC2 EC2-Instance in Ihrer AWS Cloud-Umgebung. Wenn Sie die Gateway-Appliance bereitstellen, weisen Sie lokalen physischen Festplattenspeicher auf dem Virtualisierungshost zu.

Verbinden mit AWS

Der nächste Schritt besteht darin, Ihr Gateway mit zu AWS verbinden. Dazu wählen Sie zunächst den Typ des Service-Endpunkts aus, den Sie für die Kommunikation zwischen der virtuellen Gateway-Appliance und den AWS Diensten in der Cloud verwenden möchten. Auf diesen Endpunkt kann über das öffentliche Internet oder nur von Ihrer Amazon VPC aus zugegriffen werden, wo Sie die volle Kontrolle über die Netzwerksicherheitskonfiguration haben. Anschließend geben Sie die IP-

Adresse oder den Aktivierungsschlüssel des Gateways an, den Sie erhalten können, indem Sie eine Verbindung zur lokalen Konsole auf der Gateway-Appliance herstellen.

Überprüfen und aktivieren

An dieser Stelle haben Sie die Möglichkeit, das von Ihnen gewählte Gateway und die Verbindungsoptionen zu überprüfen und gegebenenfalls Änderungen vorzunehmen. Wenn alles so eingerichtet ist, wie Sie es möchten, können Sie das Gateway aktivieren. Bevor Sie Ihr aktiviertes Gateway verwenden können, müssen Sie einige zusätzliche Einstellungen konfigurieren und Ihre Speicherressourcen erstellen.

Überblick – Gateway-Konfiguration

Nachdem Sie Ihr Storage Gateway aktiviert haben, müssen Sie einige zusätzliche Einrichtungsschritte durchführen. In diesem Schritt weisen Sie den physischen Speicher, den Sie auf der Gateway-Hostplattform bereitgestellt haben, so zu, dass er von der Gateway-Appliance entweder als Cache- oder Upload-Puffer verwendet wird. Anschließend konfigurieren Sie Einstellungen, um den Zustand Ihres Gateways mithilfe von CloudWatch Amazon-Protokollen und CloudWatch -Alarmen zu überwachen, und fügen bei Bedarf Tags hinzu, um das Gateway zu identifizieren. Bevor Sie Ihr aktiviertes Gateway verwenden können, müssen Sie einige zusätzliche Einstellungen konfigurieren und Ihre Speicherressourcen erstellen.

Überblick – Speicherressourcen

Nachdem Sie Ihr Storage Gateway aktiviert und konfiguriert haben, müssen Sie Cloud-Speicherressourcen erstellen, die es verwenden kann. Je nach Art des Gateways, das Sie erstellt haben, verwenden Sie die Storage Gateway Gateway-Konsole, um Volumes, Bänder oder Amazon S3- oder FSx Amazon-Dateifreigaben zu erstellen, um sie damit zu verknüpfen. Jeder Gateway-Typ verwendet seine jeweiligen Ressourcen, um den entsprechenden Typ der Netzwerkspeicherinfrastruktur zu emulieren, und überträgt die Daten, die Sie darauf schreiben, in die AWS -Cloud.

Erstellen und Aktivieren eines Amazon S3 File Gateways

In diesem Abschnitt finden Sie Anweisungen zum Erstellen, Bereitstellen und Aktivieren eines File Gateways in AWS Storage Gateway.

Themen

Einrichten eines Amazon S3 File Gateways

Um ein neues S3 File Gateway einzurichten

1. Öffnen Sie AWS-Managementkonsole at https://console.aws.amazon.com/storagegateway/home/ und wählen Sie den AWS-Region Ort aus, an dem Sie Ihr Gateway erstellen möchten.
2. Wählen Sie Gateway erstellen, um die Seite Gateway einrichten zu öffnen.
3. Gehen Sie im Abschnitt Gateway-Einstellungen wie folgt vor:

    a. Geben Sie in 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 in der AWS Storage Gateway Konsole zu finden.

    b. Wählen Sie Gateway-Zeitzone die lokale Zeitzone für den Teil der Welt aus, in dem Sie Ihr Gateway einsetzen möchten.
4. Wählen Sie im Abschnitt Gateway-Optionen für Gateway-Typ Amazon S3 File Gateway aus.
5. Gehen Sie im Abschnitt Plattform-Optionen wie folgt vor:

    a. Wählen Sie für Host-Plattform die Plattform aus, auf der Sie Ihr Gateway bereitstellen möchten. Folgen Sie anschließend den plattformspezifischen Anweisungen auf der Storage Gateway Gateway-Konsolenseite, um Ihre Host-Plattform einzurichten. Sie können aus den folgenden Optionen wählen:

        - VMware ESXi— Laden Sie die virtuelle Gateway-Maschine herunter, stellen Sie sie bereit und konfigurieren Sie sie mithilfe von VMware ESXi.
        - 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 Gateway-Maschine mithilfe der Linux-Kernel-basierten virtuellen Maschine (KVM) herunter, stellen Sie sie bereit und konfigurieren Sie sie. In der mitgelieferten aws-storage-gateway .xml-Datei finden Sie

empfohlene Startkonfigurationen. Der UEFI-Startmodus mit deaktiviertem Secure Boot (loader_secure=no) ist für File Gateway 2.x, Volume Gateway 3.x und Tape Gateway 3.x erforderlich.

- Nutanix AHV — Laden Sie die virtuelle Gateway-Maschine mithilfe der Linux-Kernel-basierten virtuellen Maschine (KVM) herunter, stellen Sie sie bereit und konfigurieren Sie sie. Das gleiche Image funktioniert sowohl für Linux KVM- als auch für Nutanix AHV-Hypervisor-Umgebungen.
- Amazon EC2 — Konfigurieren und starten Sie eine Amazon EC2 EC2-Instance zum Hosten Ihres Gateways.
- Hardware-Appliance — Bestellen Sie eine dedizierte physische Hardware-Appliance, um Ihr AWS Gateway zu hosten.

b. Aktivieren Sie bei Confirm Setup Gateway das Kontrollkästchen, um zu bestätigen, dass Sie die Bereitstellungsschritte für die von Ihnen gewählte Host-Plattform ausgeführt haben. Dieser Schritt gilt nicht für die Hostplattform der Hardware-Appliance.

6. Nachdem Ihr Gateway nun eingerichtet ist, müssen Sie auswählen, wie es eine Verbindung herstellen und mit ihm kommunizieren soll AWS. Wählen Sie Weiter aus, um fortzufahren.

Connect Sie Ihr Amazon S3 File Gateway mit AWS

Um ein neues S3 File Gateway zu verbinden AWS

1. Falls Sie dies noch nicht getan haben, führen Sie das unter Amazon S3 File Gateway einrichten beschriebene Verfahren durch. Wenn Sie fertig sind, wählen Sie Weiter, um die AWS Seite Connect in der AWS Storage Gateway Konsole zu öffnen.
2. Wählen Sie im Abschnitt Gateway-Verbindungsoptionen unter Verbindungsoptionen aus, wie Sie Ihr Gateway gegenüber AWS identifizieren möchten. Sie können aus den folgenden Optionen wählen:

   - IP-Adresse — Geben Sie die IP-Adresse Ihres Gateways in das entsprechende Feld ein. Diese IP-Adresse muss öffentlich sein 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 aus bei der lokalen Konsole des Gateways anmelden oder sie von Ihrer Amazon-EC2-Instance-Detailseite kopieren. Weitere Informationen finden Sie unter Die Gateway-IP-Adresse abrufen.

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

3. Gehen Sie im Abschnitt Endpunktoptionen wie folgt vor:

   a. Wählen Sie unter Service-Endpunkt den Endpunkttyp aus, mit dem Ihr Gateway kommunizieren wird AWS. Sie können aus den folgenden Optionen wählen:

      - Öffentlich zugänglich — Ihr Gateway kommuniziert mit Ihnen AWS über das öffentliche Internet. Wenn Sie diese Option auswählen, verwenden Sie das Kontrollkästchen FIPS-fähiger Endpunkt, um anzugeben, ob die Verbindung den Federal Information Processing Standards (FIPS) entsprechen muss.

        > **Note**
        >
        > Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-konformen Endpunkt. Weitere Informationen finden Sie unter Federal Information Processing Standard (FIPS) 140-2.
        > Der FIPS-Dienstendpunkt ist nur in einigen Regionen verfügbar. AWS Weitere Informationen finden Sie unter AWS Storage Gateway -Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.

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

        > **Note**
        >
        > Um einen VPC-Endpunkt anzugeben, der zu einem AWS-Konto anderen gehört als dem, den Sie derzeit für die Erstellung Ihres Gateways verwenden, müssen Sie seinen DNS-Namen oder seine IP-Adresse angeben.

b. Wählen Sie für die IP-Version die Protokollversion und den Endpunkt aus, mit AWS denen Ihr Gateway kommunizieren wird.

> **Note**
>
> Die IP-Adresse Ihres Gateways muss mit der IP-Version übereinstimmen, die Sie hier angeben. Dual-Stack-Endpunkte akzeptieren IPv4 zwar IPv6 Verbindungen, kommunizieren aber nur über die von Ihnen gewählte IP-Version mit Ihrem Gateway.

4. Nachdem Sie nun ausgewählt haben, mit welcher Verbindung Ihr Gateway verbunden werden soll AWS, müssen Sie das Gateway aktivieren. Wählen Sie Weiter aus, um fortzufahren.

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

Um die Einstellungen zu überprüfen und ein neues S3 File Gateway zu aktivieren

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

   - Einrichten eines Amazon S3 File Gateways
   - Connect Sie Ihr Amazon S3 File Gateway mit AWS

   Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Überprüfen und Aktivieren in der AWS Storage Gateway Konsole zu öffnen.
2. Überprüfen Sie die anfänglichen Gateway-Details für jeden Abschnitt auf der Seite.
3. Wenn ein Abschnitt Fehler enthält, wählen Sie Bearbeiten, um 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. Wählen Sie Weiter aus, um fortzufahren.

Konfigurieren Ihres Amazon S3 File Gateways

Um die Erstkonfiguration auf einem neuen S3 File Gateway durchzuführen

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

   - Einrichten eines Amazon S3 File Gateways
   - Connect Sie Ihr Amazon S3 File Gateway mit AWS
   - Überprüfen Sie die Einstellungen und aktivieren Sie Ihr Amazon S3 File Gateway

   Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Gateway konfigurieren in der AWS Storage Gateway Konsole zu öffnen.
2. Verwenden Sie im Abschnitt Speicher konfigurieren die Dropdownlisten, um dem Cache mindestens eine lokale Festplatte mit mindestens 150 Gibibyte (GiB) Kapazität zuzuweisen. Die in diesem Abschnitt aufgeführten lokalen Festplatten entsprechen dem physischen Speicher, den Sie auf Ihrer Hostplattform bereitgestellt haben.
3. Wählen Sie im Abschnitt CloudWatch Protokollgruppe aus, wie Amazon CloudWatch Logs eingerichtet werden soll, um den Zustand Ihres Gateways zu überwachen. Sie können aus den folgenden Optionen wählen:

   - Eine neue Protokollgruppe erstellen — Richten Sie eine neue Protokollgruppe ein, um Ihr Gateway zu überwachen.
   - Eine bestehende Protokollgruppe verwenden — Wählen Sie eine bestehende Protokollgruppe aus der entsprechenden Dropdownliste aus.
   - Protokollierung deaktivieren — Verwenden Sie Amazon CloudWatch Logs nicht zur Überwachung Ihres Gateways.

> **Note**
>
> Um Storage Gateway Gateway-Integritätsprotokolle zu erhalten, müssen die folgenden Berechtigungen in Ihrer Protokollgruppen-Ressourcenrichtlinie vorhanden sein. Ersetzen Sie die *highlighted section* ResourceArn-Informationen für Ihre Bereitstellung durch die spezifische Protokollgruppe.
>
> ```
> "Sid": "AWSLogDeliveryWrite20150319",
>       "Effect": "Allow",
>       "Principal": {
>         "Service": [
>           "delivery.logs.amazonaws.com"
>         ]
>       },
>       "Action": [
>         "logs:CreateLogStream",
>         "logs:PutLogEvents"
>       ],
>       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
> ```
>
> Das Element „Resource“ ist nur erforderlich, wenn Sie möchten, dass die Berechtigungen explizit für eine einzelne Protokollgruppe gelten.

4. Wählen Sie im Bereich CloudWatch Alarme aus, wie Sie CloudWatch Amazon-Alarme einrichten möchten, um Sie zu benachrichtigen, wenn die Metriken Ihres Gateways von den definierten Grenzwerten abweichen. Sie können aus den folgenden Optionen wählen:

   - Die empfohlenen Alarme von Storage Gateway erstellen — Alle empfohlenen CloudWatch Alarme werden automatisch erstellt, wenn das Gateway erstellt wird. Weitere Informationen zu empfohlenen Alarmen finden Sie unter Grundlegendes zu CloudWatch Alarmen.

     > **Note**
     >
     > Für diese Funktion sind CloudWatch Richtlinienberechtigungen erforderlich, die nicht automatisch als Teil der vorkonfigurierten Storage Gateway Gateway-Vollzugriffsrichtlinie gewährt werden. Stellen Sie sicher, dass Ihre Sicherheitsrichtlinie

die folgenden Berechtigungen gewährt, bevor Sie versuchen, empfohlene CloudWatch Alarme zu erstellen:

- `cloudwatch:PutMetricAlarm` – Alarme erstellen
- `cloudwatch:DisableAlarmActions` – Alarmaktionen deaktivieren
- `cloudwatch:EnableAlarmActions` – Alarmaktionen aktiveren
- `cloudwatch:DeleteAlarms` - Alarme löschen

- Benutzerdefinierten Alarm erstellen — Konfigurieren Sie einen neuen CloudWatch Alarm, der Sie über die Metriken Ihres Gateways informiert. Wählen Sie Alarm erstellen, um Metriken zu definieren und Alarmaktionen in der CloudWatch Amazon-Konsole festzulegen. Anweisungen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.
- Kein Alarm — Sie erhalten keine CloudWatch Benachrichtigungen über die Messwerte Ihres Gateways.

5. (Optional) Wählen Sie im Abschnitt Tags die Option Neues Tag hinzufügen aus und geben Sie dann ein Schlüssel-Wert-Paar ein, bei dem Groß- und Kleinschreibung beachtet werden muss, damit Sie auf den Listenseiten in der Konsole nach Ihrem Gateway suchen und filtern können. AWS Storage Gateway Wiederholen Sie diesen Schritt, um bei Bedarf weitere Tags hinzuzufügen.
6. (Optional) Wenn Ihr Gateway auf einem VMware Host bereitgestellt wird, der Teil eines VMware Hochverfügbarkeits-Clusters (HA) ist, wählen Sie im Abschnitt Konfiguration für VMware hohe Verfügbarkeit überprüfen die Option VMware HA verifizieren aus, um 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 die virtuelle Storage Gateway Gateway-Maschine (VM) wird neu gestartet.

7. Wählen Sie Konfigurieren, um die Erstellung Ihres Gateways abzuschließen.

Um den Status Ihres neuen Gateways zu überprüfen, suchen Sie auf der Gateway-Übersichtsseite der AWS Storage Gateway Konsole danach.

Nachdem Sie Ihr Gateway erstellt haben, müssen Sie eine Dateifreigabe erstellen, die es verwenden kann. Anweisungen finden Sie unter Erstellen einer Dateifreigabe.

Aktivierung eines Gateways in einer virtuellen privaten Cloud

Sie können eine private Verbindung zwischen Ihrer On-Premises-Gateway-Appliance und der cloudbasierten Speicherinfrastruktur herstellen. Sie können diese Verbindung verwenden, um Ihr Gateway zu aktivieren und es so zu konfigurieren, dass Daten an AWS Speicherdienste übertragen werden, ohne über das öffentliche Internet zu kommunizieren. Mit dem Amazon VPC-Service können Sie AWS Ressourcen, einschließlich privater Netzwerkschnittstellen-Endpunkte, in einer benutzerdefinierten Virtual Private Cloud (VPC) starten. Eine VPC gibt Ihnen die Kontrolle über Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways. Weitere Informationen finden Sie VPCs unter Was ist Amazon VPC? im Amazon VPC-Benutzerhandbuch.

Um Ihr Gateway in einer VPC zu aktivieren, verwenden Sie die Amazon VPC-Konsole, um einen VPC-Endpunkt für Storage Gateway zu erstellen, einen VPC-Endpunkt für Storage Gateway zu erstellen und aktivieren. Weitere Informationen finden Sie unter Connect Ihr Amazon S3 File Gateway, um .

Um Ihr S3 File Gateway für die Übertragung von Daten über die VPC zu konfigurieren, müssen Sie einen separaten VPC-Endpunkt für Amazon S3 erstellen und diesen VPC-Endpunkt dann angeben, wenn Sie Dateifreigaben für das Gateway erstellen.

> **Note**
>
> Sie müssen Ihr Gateway in derselben Region aktivieren, in der Sie den VPC-Endpunkt für Storage Gateway erstellen, und der Amazon S3-Speicher, den Sie für die Dateifreigabe konfigurieren, muss sich in derselben Region befinden, in der Sie den VPC-Endpunkt für Amazon S3 erstellen.

Erstellen Sie einen VPC-Endpunkt für Storage Gateway

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

So erstellen Sie einen VPC-Endpunkt für Storage Gateway

1. Melden Sie sich bei der an AWS-Managementkonsole 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. Wählen Sie auf der Seite Endpunkt erstellen die Option AWS -Services in Servicekategorie aus.
4. Wählen Sie für Servicename `com.amazonaws.`*`region`*`.storagegateway` aus. Zum 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 „DNS-Name aktivieren“ nicht 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 Endpunkt erstellen aus. 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. Verwenden Sie auf der Registerkarte Details des ausgewählten Storage-Gateway-Endpunkts unter DNS-Namen den ersten DNS-Namen, der keine Verfügbarkeitszone angibt. Ihr DNS-Name sollte dem folgenden Beispiel

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

Jetzt, da Sie über einen VPC-Endpunkt verfügen, können Sie Ihr Gateway erstellen und aktivieren. Weitere Informationen finden Sie unter Amazon S3 File Gateway und aktivieren.

Informationen zum Anfordern eines Aktivierungsschlüssels finden Sie unter Einen Aktivierungsschlüssel für Ihr Gateway .

> **Important**
>
> Um Ihr S3 File Gateway für die Übertragung von Daten über die VPC zu konfigurieren, müssen Sie einen separaten VPC-Endpunkt für Amazon S3 erstellen und diesen VPC-Endpunkt dann angeben, wenn Sie Dateifreigaben für das Gateway erstellen.
> Folgen Sie dazu den gleichen Schritten wie oben gezeigt, wählen Sie `com.amazonaws.region.s3` jedoch Service Name und anschließend die Routing-Tabelle aus, der Sie den S3-Endpunkt zuordnen möchten, und nicht die Gruppe. subnet/security Anweisungen finden Sie unter Einen Gateway-Endpunkt erstellen.

Erstellen einer Dateifreigabe

In diesem Abschnitt finden Sie Anweisungen zum Erstellen einer Dateifreigabe, auf die über das Network File System (NFS) oder das Server Message Block (SMB) -Protokoll zugegriffen werden kann.

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

Wenn Sie eine SMB-Dateifreigabe erstellen, können Sie einen von drei Authentifizierungsmodi 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 bestimmten Domänenbenutzern und -gruppen, die Sie angeben, wird Zugriff gewährt (über eine Zulassungsliste). Benutzern und Gruppen kann auch der Zugriff verweigert werden (über eine Verweigerungsliste).
- Eine SMB-Dateifreigabe mit Gastzugriff. Jeder Benutzer, der das Gastkennwort angeben kann, hat Zugriff auf diese Dateifreigabe.

> **Note**
>
> Dateifreigaben, die über das Gateway für NFS-Dateifreigaben exportiert werden, 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 Verwendung von Windows-ACLs zur Beschränkung des SMB-Dateifreigabezugriffs.

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

> **Important**
>
> Um eine Dateifreigabe zu erstellen, müssen Sie für ein File Gateway AWS -Security-Token-Service () AWS STS aktivieren. Wenn es an dem Ort, AWS-Region an dem Sie Ihr File Gateway erstellen, AWS STS nicht aktiviert ist, aktivieren Sie es. Informationen zur

Aktivierung finden Sie AWS STS unter Aktivierung und Deaktivierung AWS -Security-Token-Service in einer AWS Region im AWS Identity and Access ManagementBenutzerhandbuch.

Themen

Vermeidung unerwarteter Kosten beim Hochladen von Gateway-Daten

Wenn eine Datei von einem NFS-Client auf das File Gateway geschrieben wird, lädt das File Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von ihren Metadaten. Durch das Hochladen der Dateidaten wird ein S3-Objekt erstellt, und beim Hochladen der Metadaten für die Datei werden die Metadaten für das S3-Objekt aktualisiert. Durch diesen Vorgang wird eine zusätzliche Version des Objekts erstellt. Wenn die S3-Versionierung aktiviert ist, werden beide Versionen gespeichert.

Wenn Sie die Metadaten einer Datei ändern, die in Ihrem File Gateway gespeichert ist, wird ein neues S3-Objekt erstellt, das das vorhandene S3-Objekt ersetzt. Dieses Verhalten unterscheidet sich von der Bearbeitung einer Datei in einem Dateisystem, bei der die Bearbeitung einer Datei nicht dazu führt, dass eine neue Datei erstellt wird. Testen Sie alle Dateioperationen, die Sie mit AWS Storage Gateway verwenden möchten, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.

Erwägen Sie sorgfältig die Verwendung von S3 Versioning and Cross-Region Replication (CRR) in Amazon S3, wenn Sie Daten von Ihrem File Gateway hochladen. Das Hochladen von Dateien von Ihrem File Gateway zu Amazon S3, wenn die S3-Versionierung aktiviert ist, führt in der Regel zu mehr als einer Version eines S3-Objekts.

Bestimmte Workflows mit großen Dateien und Mustern beim Schreiben von Dateien, wie z. B. Datei-Uploads, die in mehreren Schritten ausgeführt werden, können die Anzahl der gespeicherten S3-Objektversionen erhöhen. Wenn der File Gateway-Cache aufgrund hoher Datei-Schreibraten

Speicherplatz freigeben muss, werden möglicherweise mehrere S3-Objektversionen erstellt. Diese Szenarien erhöhen den S3-Speicherplatz, wenn die S3-Versionierung aktiviert ist, und erhöhen die mit CRR verbundenen Übertragungskosten. Testen Sie alle Dateioperationen, die Sie mit Storage Gateway verwenden möchten, damit Sie verstehen, wie jeder Dateivorgang mit Amazon S3 S3-Speicher interagiert.

Wenn Sie das Rsync-Hilfsprogramm mit Ihrem File Gateway verwenden, werden temporäre Dateien im Cache und temporäre S3-Objekte in Amazon S3 erstellt. In dieser Situation fallen Gebühren für vorzeitiges Löschen in der Speicherklasse S3 Standard-Infrequent Access (S3 Standard-IA) an.

Verschlüsseln Sie von File Gateway in Amazon S3 gespeicherte Objekte

S3 File Gateway unterstützt die folgenden Methoden der serverseitigen Verschlüsselung für die in Amazon S3 gespeicherten Daten:

- SSE-S3— Standardmäßig verwenden alle neuen Objekte, die in Amazon S3 S3-Buckets hochgeladen werden, serverseitige Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln. Weitere Informationen finden Sie unter Verwenden der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.
- SSE-KMS— Sie können Ihre Dateifreigabe so konfigurieren, dass serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) verwalteten Schlüsseln verwendet wird. AWS KMSist ein Dienst, der sichere, hochverfügbare Hardware und Software kombiniert, um ein für die Cloud skaliertes Schlüsselverwaltungssystem bereitzustellen. Weitere Informationen finden Sie unter Was ist der AWS Key Management Service? im AWS Key Management ServiceEntwicklerhandbuch.
- DSSE-KMS— Die Dual-layer serverseitige Verschlüsselung mit AWS KMS Schlüsseln wendet zwei Verschlüsselungsebenen auf Objekte an, wenn sie auf Amazon S3 hochgeladen werden. Dies trägt dazu bei, die Compliance-Standards für mehrschichtige Verschlüsselung zu erfüllen. Weitere Informationen finden Sie unter Verwenden der serverseitigen Dual-Layer-Verschlüsselung mit AWS KMS Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Für die Nutzung von DSSE-KMS und AWS KMS Schlüsseln fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter AWS KMS Preise.

Sie können eine Verschlüsselungsmethode angeben, wenn Sie eine neue Dateifreigabe mithilfe der Storage Gateway Gateway-Konsole oder der Storage Gateway Gateway-API erstellen. Informationen zu Konsolenprozeduren finden Sie unter Erstellen Sie eine NFS-Dateifreigabe mit einer benutzerdefinierten Konfiguration oderErstellen Sie eine SMB-Dateifreigabe mit einer benutzerdefinierten Konfiguration. Informationen zu den entsprechenden API-Befehlen finden Sie unter CreateNFSFileShareoder CreateSMBFileSharein der AWSStorage Gateway API Reference.

Sie können die Verschlüsselungseinstellungen für eine bestehende Dateifreigabe auch mithilfe der Storage Gateway Gateway-Konsole oder der Storage Gateway Gateway-API aktualisieren. Informationen zum Konsolenverfahren finden Sie unterÄndern Sie die serverseitige Verschlüsselungsmethode für eine bestehende Dateifreigabe. Informationen zu den entsprechenden API-Befehlen finden Sie unter UpdateNFSFileShareoder UpdateSMBFileSharein der AWSStorage Gateway API Reference.

> **Note**
>
> Nachdem Sie die Verschlüsselungsmethode aktualisiert haben, verwendet das Gateway die neue Methode für alle neuen Objekte, die es in Amazon S3 erstellt, und für alle gespeicherten Objekte, die es in future aktualisiert oder ändert. Bestehende Amazon S3 S3-Objekte erhalten die neue Verschlüsselungsmethode nur, wenn sie vom Gateway aktualisiert oder geändert werden.

> **Important**
>
> Stellen Sie sicher, dass Ihre Dateifreigabe denselben Verschlüsselungstyp verwendet wie der Amazon S3 S3-Bucket, in dem Ihre Daten gespeichert werden.
> Wenn Sie Ihr File Gateway für die Verwendung SSE-KMS oder DSSE-KMS für die Verschlüsselung konfigurieren, müssen Sie der mit der Dateifreigabe verknüpften IAM-Rolle manuellkms:GenerateDataKey,,, und kms:DescribeKey Berechtigungen hinzufügenkms:Encrypt. kms:Decrypt kms:ReEncrypt* Weitere Informationen finden Sie unter Verwenden von Identity-Based Richtlinien (IAM-Richtlinien) für Storage Gateway.

Erstellen Sie eine NFS-Dateifreigabe

Das Network File System (NFS) -Protokoll ist ein Stateful-Filesharing-Protokoll für UNIX-basierte Systeme. Wenn ein NFS-fähiger Client und ein NFS-Server miteinander kommunizieren, fordert der Client mithilfe von Remote Procedure Calls (RPC) eine Datei oder ein Verzeichnis vom Server an. Der Server überprüft, ob die Datei oder das Verzeichnis verfügbar ist und ob der Client über die erforderlichen Zugriffsberechtigungen verfügt. Der Server mountet die Datei oder das Verzeichnis dann remote auf dem Client und teilt den Zugriff über eine virtuelle Verbindung. Für Client-Operationen ähnelt NFS die Verwendung der Remoteserverdatei dem Zugriff auf eine lokale Datei.

> **Note**
>
> Das NFS-Protokoll unterstützt maximal 16 Gruppen pro Benutzer. Benutzer können Probleme beim Mounten von NFS-Dateifreigaben haben, wenn sie zu mehr als 16 Gruppen gehören. Um Probleme beim Einbinden zu vermeiden, sollten Sie sicherstellen, dass Benutzer beim Zugriff auf NFS-Dateifreigaben Mitglieder von 16 oder weniger Gruppen sind.

In den folgenden Themen werden verschiedene Methoden zum Erstellen einer NFS-Dateifreigabe für Ihr File Gateway erläutert:

Inhalt

Erstellen Sie eine NFS-Dateifreigabe mit der Standardkonfiguration

In diesem Abschnitt wird erklärt, wie Sie mithilfe vorkonfigurierter Standardeinstellungen eine neue NFS-Dateifreigabe (Network File System) erstellen. Verwenden Sie diese Methode für einfache Bereitstellungen, den persönlichen Gebrauch, zum Testen oder als Möglichkeit, schnell mehrere Dateifreigaben bereitzustellen, die Sie später bearbeiten und anpassen möchten. Eine Liste der Standardeinstellungen für Dateifreigaben, die Sie mit diesem Verfahren erstellen, finden Sie unter Standardkonfigurationseinstellungen für NFS-Dateifreigaben. Wenn Sie eine detailliertere Steuerung benötigen oder erweiterte Einstellungen für Ihre Dateifreigabe verwenden möchten, finden Sie

weitere Informationen unter Erstellen einer NFS-Dateifreigabe mithilfe einer benutzerdefinierten Konfiguration.

> **Note**
>
> Wenn Sie Ihre Dateifreigabe über eine Virtual Private Cloud (VPC) mit Amazon S3 verbinden müssen, müssen Sie das benutzerdefinierte Konfigurationsverfahren befolgen. Sie können die VPC-Einstellungen für eine Dateifreigabe nicht bearbeiten, nachdem Sie sie erstellt haben.

> **Important**
>
> Die Verwendung von S3 Versioning, Cross-Region Replication oder dem Rsync-Hilfsprogramm beim Hochladen von Daten von einem File Gateway kann erhebliche Kostenauswirkungen haben. Weitere Informationen finden Sie unter Vermeidung unerwarteter Kosten beim Hochladen von Daten von File Gateway.

So erstellen Sie eine NFS-Dateifreigabe mit der Standardkonfiguration:

1. Öffnen Sie die AWS Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home/ und wählen Sie im linken Navigationsbereich Dateifreigaben aus.
2. Wählen Sie Create file share (Dateifreigabe erstellen) aus.
3. Wählen Sie für Gateway Ihr Amazon S3 File Gateway aus der Liste aus.
4. Wählen Sie für File Share Protocol NFS.
5. Führen Sie für den S3-Bucket einen der folgenden Schritte aus:
   - Wählen Sie einen vorhandenen Amazon S3 S3-Bucket in Ihrem Konto aus der Drop-down-Liste aus.
   - Wählen Sie in der Drop-down-Liste einen Bucket in einem anderen Konto aus und geben Sie dann den Namen des Buckets im Feld Kontoübergreifender Bucket-Name ein.
   - Wählen Sie Neuen S3-Bucket erstellen, wählen Sie dann aus, AWS-Region wo sich der Amazon S3 S3-Endpunkt für Ihren neuen Bucket befindet, und geben Sie einen eindeutigen S3-Bucket-Namen ein. Wählen Sie Create S3-Bucket, wenn Sie fertig sind.

Informationen zum Erstellen eines neuen Buckets finden Sie unter Wie erstelle ich einen S3-Bucket? im Amazon S3 S3-Benutzerhandbuch.

> **Note**
>
> S3 File Gateway unterstützt keine Amazon S3 S3-Buckets mit Punkten (`.`) im Bucket-Namen.
> Stellen Sie sicher, dass Ihr Bucket-Name den Regeln für die Bucket-Benennung in Amazon S3 entspricht. Weitere Informationen finden Sie unter Regeln für die Bucket-Benennung im Amazon Simple Storage Service-Benutzerhandbuch.

6. Überprüfen Sie die Einstellungen unter Standardkonfiguration und wählen Sie dann Create file share, um Ihre neue NFS-Dateifreigabe mit der Standardkonfiguration zu erstellen.

Nachdem Ihre NFS-Dateifreigabe erstellt wurde, können Sie ihre Konfigurationseinstellungen in der AWS Storage Gateway Gateway-Konsole auf der Registerkarte Details der Dateifreigabe einsehen. Informationen zum Mounten Ihrer Dateifreigabe finden Sie unter Mounten Ihrer NFS-Dateifreigabe auf Ihrem Client.

Standardkonfigurationseinstellungen für NFS-Dateifreigaben

Die folgenden Einstellungen gelten für alle neuen NFS-Dateifreigaben, die Sie mit der Standardkonfiguration erstellen. Nachdem Sie eine Dateifreigabe erstellt haben, können Sie sie auf der Seite Dateifreigaben in der AWS Storage Gateway Gateway-Konsole auswählen, um Details zu ihrer Konfiguration anzuzeigen.

> **Important**
>
> Die standardmäßige NFS-Dateifreigabekonfiguration bietet dem Besitzer des S3-Buckets, der der Dateifreigabe zugeordnet ist, vollständige Dateikontrolle und Zugriffsberechtigungen, auch wenn der Bucket einem anderen AWS Konto gehört. Weitere Informationen zur Verwendung Ihrer Dateifreigabe für den Zugriff auf Objekte in einem Bucket, der einem anderen Konto gehört, finden Sie unter. Verwenden einer Dateifreigabe für kontoübergreifenden Zugriff

Einstellung	Standardwert	Hinweise
Amazon S3 S3-Standort	Die Dateifreigabe stellt eine direkte Verbindung zum Amazon S3 S3-Bucket her und hat denselben Namen wie der Bucket. Ihr Gateway verwendet diesen Bucket zum Speichern und Abrufen von Dateien.	Der Name enthält kein Präfix.
AWS PrivateLink für S3	Die Dateifreigabe stellt keine Verbindung zu Amazon S3 über einen Schnittstellenendpunkt in Ihrer Virtual Private Cloud (VPC) her.	
Benachrichtigung beim Hochladen von Dateien	Aus	
Speicherklasse für neue Objekte	Amazon S3 Standard	Auf diese Weise können Sie Ihre Objektdaten, auf die häufig zugegriffen wird, redundant in mehreren Availability Zones speichern, die geografisch getrennt sind. Weitere Informationen zur Amazon S3 Standard Speicherklasse finden Sie unter Speicherklassen für Objekte mit häufigem Zugriff im Amazon Simple Storage Service-Benutzerhandbuch.
Verschlüsselung	Serverseitige Verschlüsselung mit verwalteten S3-Schlüsseln (SSE-S3)	Alle Amazon S3 S3-Objekte, die Ihr S3 File Gateway hochlädt, aktualisiert oder

Einstellung	Standardwert	Hinweise
		ändert, werden standardmäßig mit serverseitiger Verschlüs selung mit verwalteten Amazon S3 S3-Schlüsseln verschlüsselt.
Objekt-Metadaten	Erraten Sie den MIME-Typ	Dadurch kann Storage Gateway den MIME-Typ (Multipurpose Internet Mail Extension) für hochgelad ene Objekte anhand von Dateierweiterungen erraten. Für diese Option müssen die Zugriffskontrolllisten (ACLs) aktiviert sein für den Amazon S3 S3-Bucket, der mit Ihrer Dateifreigabe verknüpft ist. Wenn ACLs sind ausgescha ltet, die Dateifreigabe kann nicht auf den Amazon S3 S3-Bucket zugreifen und verbleibt im Status Nicht verfügbar auf unbestimmte Zeit.
Aktiviere, der Antragsteller zahlt	Aus	Weitere Informationen finden Sie unter Buckets mit Bezahlung durch den Anforderer.
Prüfungsprotokolle	Aus	Die Protokollierung bei einer Amazon CloudWatch Gruppe ist standardmäßig deaktiviert.

Einstellung	Standardwert	Hinweise
Zugriff auf Ihren S3-Bucket	Erstellen Sie eine neue IAM-Rolle	Die Standardoption ermöglicht es dem File Gateway, eine neue IAM-Rolle und den Zugriff darauf zu erstellen Richtlinie in Ihrem Namen. Allen NFS-Clients ist der Zugriff gestattet. Für Informationen über unterstützte NFS-Clients finden Sie unterUnterstützte NFS- und SMB-Clients für File Gateway.
Einhängeoptionen	• Squash-Level — Wurzelkürbis • Exportieren als — Lesen/Schreiben	Der Standardwert von Squash Level bedeutet, dass Zugriff für die Fernbedienung Der Superuser (root) ist dem User Identifier (UID) (65534) und dem Group Identifier (GID) (65534) zugeordnet.
Standardeinstellungen für Datei-Metadaten	• Verzeichnisberechtigungen — 0777 • Dateiberechtigungen — 0666 • Benutzerkennung (UID) — 65534 • Gruppenkennung (GID) — 65534	

Erstellen Sie eine NFS-Dateifreigabe mit einer benutzerdefinierten Konfiguration

Gehen Sie wie folgt vor, um eine NFS-Dateifreigabe (Network File System) mit einer benutzerdefinierten Konfiguration zu erstellen. Informationen zum Erstellen einer NFS-Dateifreigabe mithilfe der Standardkonfigurationseinstellungen finden Sie unter Erstellen einer NFS-Dateifreigabe mit der Standardkonfiguration.

> **Important**
>
> Die Verwendung von S3 Versioning, regionsübergreifender Replikation oder des Dienstprogramms Rsync beim Hochladen von Daten von einem File Gateway kann erhebliche Kostenauswirkungen haben. Weitere Informationen finden Sie unter Vermeidung unerwarteter Kosten beim Hochladen von Daten von File Gateway.

So erstellen Sie eine NFS-Dateifreigabe mit benutzerdefinierten Einstellungen

1. Öffnen Sie die AWS Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home/ und wählen Sie im linken Navigationsbereich Dateifreigaben aus.
2. Wählen Sie Create file share (Dateifreigabe erstellen) aus.
3. Wählen Sie Konfiguration anpassen. Sie können die anderen Felder auf dieser Seite vorerst ignorieren. In den nachfolgenden Schritten werden Sie aufgefordert, die Gateway-, Protokoll- und Speichereinstellungen zu konfigurieren.
4. Wählen Sie für Gateway das Amazon S3 File Gateway für Ihre neue Dateifreigabe für aus der Drop-down-Liste aus.
5. Wählen Sie für CloudWatch Protokollgruppe eine der folgenden Optionen aus der Drop-down-Liste aus:

   - Um die Protokollierung für diese Dateifreigabe zu deaktivieren, wählen Sie Protokollierung deaktivieren.
   - Um automatisch eine neue Protokollgruppe für diese Dateifreigabe zu erstellen, wählen Sie Created by Storage Gateway.
   - Um Integritäts- und Ressourcenbenachrichtigungen für diese Dateifreigabe an eine bestehende Protokollgruppe zu senden, wählen Sie die gewünschte Gruppe aus der Liste aus.

Weitere Informationen zu Audit-Logs finden Sie unter Grundlegendes zu S3 File Gateway-Auditprotokollen.

6. (Optional) Wählen Sie unter Tags — Optional die Option Neues Tag hinzufügen aus und geben Sie dann einen Schlüssel und einen Wert für Ihre Dateifreigabe ein.

   Ein Tag ist ein Schlüssel-Wert-Paar, bei dem Groß- und Kleinschreibung beachtet wird und Ihnen hilft, Ihre Storage Gateway Gateway-Ressourcen zu kategorisieren. Das Hinzufügen von Tags kann das Filtern und Suchen nach Ihrer Dateifreigabe vereinfachen. Sie können diesen Schritt wiederholen, um bis zu 50 Tags hinzuzufügen.

   Wählen Sie Weiter, wenn Sie fertig sind.

7. Führen Sie für den S3-Bucket einen der folgenden Schritte aus, um anzugeben, wo Ihre Dateifreigabe Dateien speichert und abruft:

   - Um die Dateifreigabe direkt mit einem vorhandenen S3-Bucket in Ihrem Amazon Web Services Services-Konto zu verbinden, wählen Sie den Bucket-Namen aus der Drop-down-Liste aus.
   - Um die Dateifreigabe mit einem vorhandenen S3-Bucket zu verbinden, der einem anderen Amazon Web Services Services-Konto als dem gehört, mit dem Sie die Dateifreigabe erstellt haben, wählen Sie In der Dropdownliste Ein Bucket in einem anderen Konto aus und geben Sie dann den kontoübergreifenden Bucket-Namen ein.
   - Um die Dateifreigabe mit einem neuen S3-Bucket zu verbinden, wählen Sie Create a new S3-Bucket aus, wählen Sie dann die Region aus, in der sich der Amazon S3 S3-Endpunkt für Ihren neuen Bucket befindet, und geben Sie einen eindeutigen S3-Bucket-Namen ein. Wenn Sie fertig sind, wählen Sie S3-Bucket erstellen. Weitere Informationen zum Erstellen neuer Buckets finden Sie unter Wie erstelle ich einen S3-Bucket? im Amazon S3 S3-Benutzerhandbuch.
   - Um die Dateifreigabe mithilfe eines Zugriffspunktnamens mit einem S3-Bucket zu verbinden, wählen Sie den Namen des Amazon S3 S3-Zugriffspunkts aus der Drop-down-Liste aus und geben Sie dann den Namen des Access Points ein. Wenn Sie einen neuen Access Point erstellen müssen, können Sie Create an S3 Access Point wählen. Weitere Anweisungen finden Sie unter Erstellen eines Access Points im Amazon S3 S3-Benutzerhandbuch. Weitere Informationen zu Access Points finden Sie unter Verwaltung des Datenzugriffs mit Amazon S3 S3-Zugriffspunkten und Delegieren der Zugriffskontrolle an Access Points im Amazon S3 S3-Benutzerhandbuch.

- Um die Dateifreigabe mithilfe eines Access Point-Alias mit einem S3-Bucket zu verbinden, wählen Sie den Amazon S3 S3-Zugriffspunkt-Alias aus der Drop-down-Liste aus und geben Sie dann den Access Point-Alias ein. Wenn Sie einen neuen Access Point erstellen müssen, können Sie Create an S3 Access Point wählen. Weitere Anweisungen finden Sie unter Erstellen eines Access Points im Amazon S3 S3-Benutzerhandbuch. Weitere Informationen zu Access Point-Aliasnamen finden Sie unter Verwenden eines Alias im Bucket-Stil für Ihren Access Point im Amazon S3 S3-Benutzerhandbuch.

> **Note**
>
> Jede Dateifreigabe kann nur mit einem S3-Bucket verbunden werden, aber mehrere Fileshares können eine Verbindung zu demselben Bucket herstellen. Wenn Sie mehr als eine Dateifreigabe mit demselben Bucket verbinden, müssen Sie jede Dateifreigabe so konfigurieren, dass sie ein eindeutiges, sich nicht überschneidendes S3-Bucket-Präfix verwendet, um Konflikte zu vermeiden read/write .
> S3 File Gateway unterstützt keine Amazon S3 S3-Buckets mit Punkten (`.`) im Bucket-Namen.
> Stellen Sie sicher, dass Ihr Bucket-Name den Regeln für die Bucket-Benennung in Amazon S3 entspricht. Weitere Informationen finden Sie unter Regeln für die Benennung von Buckets im Amazon Simple Storage Service-Benutzerhandbuch.

8. (Optional) Geben Sie für das S3-Bucket-Präfix ein Präfix für Ihre Dateifreigabe ein, das auf die Objekte angewendet werden soll, die sie in Amazon S3 erstellt. Präfixe sind eine Möglichkeit, Ihre Daten in S3 zu organisieren, ähnlich wie Verzeichnisse in herkömmlichen Dateistrukturen. Weitere Informationen finden Sie unter Objekte mithilfe von Präfixen organisieren im Amazon S3 S3-Benutzerhandbuch.

> **Note**
>
> - Wenn Sie mehr als eine Dateifreigabe mit demselben Bucket verbinden, müssen Sie jede Dateifreigabe so konfigurieren, dass sie ein eindeutiges, sich nicht überschneidendes Präfix verwendet, um Konflikte zu vermeiden. read/write
> - Das Präfix muss mit einem Schrägstrich enden (/).
> - Nachdem die Dateifreigabe erstellt wurde, kann das Präfix weder geändert noch gelöscht werden.

9. Wählen Sie für Region aus der Dropdownliste aus, AWS-Region wo sich der S3-Endpunkt für Ihren Bucket befindet. Dieses Feld wird nur angezeigt, wenn Sie einen Access Point oder einen Bucket in einem anderen Konto für den S3-Bucket angeben.
10. Wählen Sie für Speicherklasse für neue Objekte eine Speicherklasse aus der Dropdownliste aus. Weitere Informationen zu Speicherklassen finden Sie unter Speicherklassen mit einem File Gateway verwenden.
11. Gehen Sie für IAM-Rolle wie folgt vor, um eine IAM-Rolle für Ihre Dateifreigabe zu konfigurieren:

    - Um automatisch eine neue IAM-Rolle mit den erforderlichen Berechtigungen zu erstellen, damit Ihre Dateifreigabe ordnungsgemäß funktioniert, wählen Sie Created by Storage Gateway aus der Dropdownliste aus.
    - Um eine bestehende IAM-Rolle zu verwenden, wählen Sie den Rollennamen aus der Dropdownliste aus.
    - Um eine neue IAM-Rolle zu erstellen, wählen Sie Create a role aus. Weitere Anweisungen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst.

    Weitere Informationen darüber, wie IAM-Rollen den Zugriff zwischen Ihrer Dateifreigabe und Ihrem S3-Bucket steuern, finden Sie unter Zugriff auf einen Amazon S3 S3-Bucket gewähren.
12. Gehen Sie für Private Link nur dann wie folgt vor, wenn Sie Ihre Dateifreigabe für die Kommunikation AWS mit einem privaten Endpunkt in einer Virtual Private Cloud (VPC) konfigurieren müssen. Andernfalls überspringen Sie diesen Schritt. Weitere Informationen finden Sie unter Was ist AWS PrivateLink? im AWS PrivateLink Leitfaden.

    a. Wählen Sie VPC-Endpunkt verwenden aus.

    b. Führen Sie unter Identifizieren des VPC-Endpunkts durch einen der folgenden Schritte aus:

        - Wählen Sie VPC-Endpunkt-ID und dann den Endpunkt, den Sie verwenden möchten, aus der VPC-Endpunkt-Dropdownliste aus.
        - Wählen Sie DNS-Name aus und geben Sie dann den DNS-Namen für den Endpunkt ein, den Sie verwenden möchten.
13. Wählen Sie unter Verschlüsselung die Art der serverseitigen Verschlüsselung aus, die die Dateifreigabe für die in Amazon S3 gespeicherten Daten verwenden soll:

    - Um serverseitige Verschlüsselung zu verwenden, die mit Amazon S3 (SSE-S3) verwaltet wird, wählen Sie S3-Managed Keys (SSE-S3).

Weitere Informationen finden Sie unter Verwenden der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

- Um die serverseitige Verschlüsselung zu verwenden, die mit dem AWS Key Management Service (SSE-KMS) verwaltet wird, wählen Sie KMS-verwaltete Schlüssel (SSE-KMS). Wählen Sie für den primären KMS-Schlüssel einen vorhandenen AWS KMS-Schlüssel aus, oder wählen Sie Neuen KMS-Schlüssel erstellen, um in der Key Management Service () -Konsole einen neuen KMS-Schlüssel zu erstellen. AWS AWS KMS

  Weitere Informationen zu finden Sie AWS KMS unter Was ist der AWS Schlüsselverwaltungsdienst? im AWS Key Management Service Entwicklerhandbuch.

- Um die serverseitige Dual-Layer-Verschlüsselung zu verwenden, die mit dem AWS Key Management Service (DSSE-KMS) verwaltet wird, wählen Sie Serverseitige Dual-Layer-Verschlüsselung mit Schlüsseln (DSSE-KMS). AWS Key Management Service Wählen Sie für den primären KMS-Schlüssel einen vorhandenen AWS KMS-Schlüssel aus, oder wählen Sie Neuen KMS-Schlüssel erstellen, um in der Key Management Service () -Konsole einen neuen KMS-Schlüssel zu erstellen. AWS AWS KMS

  Weitere Informationen zu DSSE-KMS finden Sie unter Verwenden der dualen serverseitigen Verschlüsselung mit AWS KMS Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Für die Verwendung von DSSE-KMS und Schlüsseln fallen zusätzliche Gebühren an. AWS KMS Weitere Informationen finden Sie unter AWS KMS Preise.
> Um einen AWS KMS Schlüssel mit einem Alias anzugeben, der nicht aufgeführt ist, oder um einen AWS KMS Schlüssel aus einem anderen AWS Konto zu verwenden, müssen Sie den verwenden. AWS Command Line Interface Asymmetrische KMS-Schlüssel werden nicht unterstützt. Weitere Informationen finden Sie unter Create NFSFile Share in der AWS Storage Gateway API-Referenz.

> **Important**
>
> Stellen Sie sicher, dass Ihre Dateifreigabe denselben Verschlüsselungstyp verwendet wie der Amazon S3 S3-Bucket, in dem Ihre Daten gespeichert werden.

14. Wählen Sie für Guess MIME-Typen die Option Guess media MIME type aus, damit Storage Gateway den Medientyp für hochgeladene Objekte anhand ihrer Dateierweiterungen erraten kann.
15. Geben Sie unter Name der Dateifreigabe einen Namen für Ihre Dateifreigabe ein.

> **Note**
>
> Ein gültiger NFS-Dateifreigabename darf nur die folgenden Zeichen enthalten: `a` `A` - `zZ`, `0` -9, `-`.`.`, und`_`.

16. Wählen Sie für Upload-Ereignisse die Option Ereignis protokollieren, wenn eine Datei erfolgreich vom Gateway hochgeladen wurde, wenn Sie möchten, dass Ihr Gateway CloudWatch Protokollereignisse aufzeichnet, wenn es erfolgreich Dateien auf Amazon S3 hochlädt. Die Benachrichtigungsverzögerung steuert die Mindestverzögerung zwischen dem letzten Schreibvorgang des Clients und der Generierung der `ObjectUploaded` Protokollbenachrichtigung. Da Clients in kurzer Zeit viele kleine Schreibvorgänge in Dateien ausführen können, empfehlen wir, diesen Parameter so lange wie möglich festzulegen, um zu vermeiden, dass mehrere Benachrichtigungen für dieselbe Datei schnell hintereinander generiert werden. Weitere Informationen finden Sie unter Benachrichtigung über Datei-Uploads erhalten.

> **Note**
>
> Diese Einstellung hat keinen Einfluss auf den Zeitpunkt, zu dem das Objekt auf S3 hochgeladen wird, sondern nur auf den Zeitpunkt der Benachrichtigung.
> Diese Einstellung soll keinen genauen Zeitpunkt angeben, zu dem die Benachrichtigung gesendet wird. In einigen Fällen benötigt das Gateway möglicherweise mehr als die angegebene Verzögerungszeit, um Benachrichtigungen zu generieren und zu senden.

Wählen Sie Weiter, wenn Sie fertig sind.

17.

18. Wählen Sie für File Share Protocol die Option NFS aus.
19. Führen Sie für den Clientzugriff einen der folgenden Schritte aus, um anzugeben, welche NFS-Clients auf Ihre Dateifreigabe zugreifen können:

    - Um alle eingehenden Client-Verbindungen zu akzeptieren, wählen Sie Alle NFS-Clients aus.
    - Um eingehende Client-Verbindungen nur von bestimmten IP-Adressen zu akzeptieren, wählen Sie Bestimmte NFS-Clients und anschließend Client hinzufügen aus. Geben Sie für Zulässige Clients eine gültige IP-Adresse oder einen gültigen CIDR-Block an, von dem Verbindungen akzeptiert werden sollen. Wenn Sie zusätzliche IP-Adressen angeben müssen, wählen Sie Add another client aus.

    > **Note**
    >
    > Wir empfehlen, die Beschränkung des Zugriffs auf Ihre Dateifreigabe mithilfe der Option Spezifische NFS-Clients zu konfigurieren. Wenn Sie dies nicht tun, kann jeder Client in Ihrem Netzwerk auf die Dateifreigabe zugreifen.

20. Wählen Sie unter Zugriffstyp eine der folgenden Optionen aus:

    - Wählen Sie Lesen/Schreiben, um Clients das Lesen und Schreiben von Dateien auf der Dateifreigabe zu ermöglichen.
    - Wählen Sie Schreibgeschützt, damit Clients Dateien lesen, aber nicht in die Dateifreigabe schreiben können.

    > **Note**
    >
    > Wenn Sie bei Dateifreigaben, die auf einem Microsoft Windows-Client bereitgestellt sind, Schreibgeschützt wählen, wird möglicherweise eine Meldung über einen unerwarteten Fehler angezeigt, der Sie daran hindert, den Ordner zu erstellen. Sie können diese Meldung ignorieren.

21. Wählen Sie für Zugriffsebene eine der folgenden Optionen aus:

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

22. (Optional) Wählen Sie für Automatisierte Cacheaktualisierung aus S3 die Option Cache-Aktualisierungsintervall festlegen und legen Sie dann die Zeit in Minuten oder Tagen fest, zu der der Cache der Dateifreigabe mithilfe von Time To Live (TTL) aktualisiert werden soll. TTL ist die Zeitspanne seit der letzten Aktualisierung. Nach Ablauf des TTL-Intervalls führt der Zugriff auf ein Verzeichnis dazu, dass File Gateway den Inhalt dieses Verzeichnisses aus dem Amazon S3 S3-Bucket aktualisiert.

    > **Note**
    >
    > Wenn dieser Wert kürzer als 30 Minuten ist, kann sich dies negativ auf die Gateway-Leistung auswirken, wenn häufig eine große Anzahl von Amazon S3 S3-Objekten erstellt oder gelöscht wird.

23. Wählen Sie unter Standardeinstellungen für Dateimetadaten die Option Standardmetadaten für S3-Objekte ändern aus, die nicht von Ihrem Gateway erstellt oder geändert wurden, wenn Sie möchten, dass Ihr Gateway Dateimetadaten (einschließlich Unix-Berechtigungen) auf bereits vorhandene Objekte anwendet, die es in Ihrem S3-Bucket entdeckt. Geben Sie in den entsprechenden Feldern die Verzeichnisberechtigungen, Dateiberechtigungen, Benutzer-ID und Gruppen-ID an, die Sie anwenden möchten.
24. Wählen Sie für Dateibesitz und -berechtigungen die Option Dem Besitzer des S3-Buckets das volle Eigentum an den vom Gateway erstellten Dateien geben aus, einschließlich Lese-, Schreib-, Bearbeitungs- und Löschberechtigungen, wenn das AWS Konto, dem der S3-Bucket gehört, die volle Kontrolle über alle Objekte haben soll, die von Ihrer Dateifreigabe in den Bucket geschrieben werden.

    Wählen Sie Weiter, wenn Sie fertig sind.
25. Überprüfen Sie die Konfiguration der Dateifreigabe. Wählen Sie Bearbeiten, um die Einstellungen für jeden Abschnitt zu ändern, den Sie ändern möchten. Wenn Sie fertig sind, wählen Sie Erstellen.

Nachdem Ihre NFS-Dateifreigabe erstellt wurde, können Sie ihre Konfigurationseinstellungen in der AWS Storage Gateway Gateway-Konsole auf der Registerkarte Details der Dateifreigabe einsehen. Anweisungen zum Mounten Ihrer Dateifreigabe finden Sie unter Mounten Ihrer NFS-Dateifreigabe auf Ihrem Client.

Eine SMB-Dateifreigabe erstellen

Das Server Message Block (SMB) -Protokoll ist tief in die Microsoft Windows-Produktsuite integriert und bleibt das Standardprotokoll für die gemeinsame Nutzung von Dateien für Windows-Betriebssysteme. Der Prozess der Client-Server-Kommunikation ähnelt in hohem Maße dem von NFS, es gibt jedoch Unterschiede in einigen Details und Betriebsmechanismen. In SMB werden Dateisysteme beispielsweise nicht auf dem lokalen SMB-Client bereitgestellt. Stattdessen wird über einen Netzwerkpfad auf eine Netzwerkfreigabe zugegriffen, die auf dem SMB-Server gehostet wird.

In den Themen dieses Abschnitts werden verschiedene Methoden zum Erstellen einer SMB-Dateifreigabe für Ihr File Gateway erläutert.

Inhalt

Erstellen Sie eine SMB-Dateifreigabe mit der Standardkonfiguration

In diesem Abschnitt wird erklärt, wie Sie mithilfe vorkonfigurierter Standardeinstellungen eine neue SMB-Dateifreigabe (Server Message Block) erstellen. Verwenden Sie diese Methode für einfache Bereitstellungen, den persönlichen Gebrauch, zum Testen oder als Möglichkeit, schnell mehrere Dateifreigaben bereitzustellen, die Sie später bearbeiten und anpassen möchten. Eine Liste der Standardeinstellungen für Dateifreigaben, die Sie mit diesem Verfahren erstellen, finden Sie unter Standardkonfigurationseinstellungen für SMB-Dateifreigaben. Wenn Sie eine detailliertere Steuerung benötigen oder erweiterte Einstellungen für Ihre Dateifreigabe verwenden möchten, finden Sie weitere Informationen unter Erstellen einer SMB-Dateifreigabe mit einer benutzerdefinierten Konfiguration.

> **Note**
>
> Wenn Sie Ihre Dateifreigabe über eine Virtual Private Cloud (VPC) mit Amazon S3 verbinden müssen, müssen Sie das benutzerdefinierte Konfigurationsverfahren befolgen. Sie können die VPC-Einstellungen für eine Dateifreigabe nicht bearbeiten, nachdem Sie sie erstellt haben.

> **Important**
>
> Die Verwendung von S3 Versioning, Cross-Region Replication oder dem Rsync-Hilfsprogramm beim Hochladen von Daten von einem File Gateway kann erhebliche Kostenauswirkungen haben. Weitere Informationen finden Sie unter Vermeidung unerwarteter Kosten beim Hochladen von Daten von File Gateway.

Voraussetzungen

Gehen Sie wie folgt vor, bevor Sie Ihre Dateifreigabe erstellen:

- Konfigurieren Sie die SMB-Sicherheitseinstellungen für Ihr File Gateway. Anweisungen finden Sie unter Eine Sicherheitsstufe für Ihr Gateway festlegen.
- Konfigurieren Sie entweder Microsoft Active Directory oder den Gastzugriff für die Authentifizierung. Anweisungen finden Sie unter Verwenden von Active Directory zur Benutzerauthentifizierung oder Bereitstellen von Gastzugriff auf Ihre Dateifreigabe.
- Stellen Sie sicher, dass die erforderlichen Ports in Ihrer Sicherheitsgruppe geöffnet sind. Weitere Informationen finden Sie unter Portanforderungen.

So erstellen Sie eine SMB-Dateifreigabe mit der Standardkonfiguration:

1. Öffnen Sie die AWS Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home/ und wählen Sie im linken Navigationsbereich Dateifreigaben aus.
2. Wählen Sie Create file share (Dateifreigabe erstellen) aus.
3. Wählen Sie für Gateway das Amazon S3 File Gateway aus der Drop-down-Liste aus.
4. Wählen Sie für File Share Protocol die Option SMB aus.
5. Führen Sie für den S3-Bucket einen der folgenden Schritte aus:
   - Wählen Sie einen vorhandenen Amazon S3 S3-Bucket in Ihrem Konto aus der Drop-down-Liste aus.
   - Wählen Sie in der Drop-down-Liste einen Bucket in einem anderen Konto aus und geben Sie dann den Namen des Buckets im Feld Kontoübergreifender Bucket-Name ein.
   - Wählen Sie Neuen S3-Bucket erstellen, wählen Sie dann aus, AWS-Region wo sich der Amazon S3 S3-Endpunkt für Ihren neuen Bucket befindet, und geben Sie einen eindeutigen S3-Bucket-Namen ein. Wählen Sie Create S3-Bucket, wenn Sie fertig sind.

Informationen zum Erstellen eines neuen Buckets finden Sie unter Wie erstelle ich einen S3-Bucket? im Amazon S3 S3-Benutzerhandbuch.

> **Note**
>
> S3 File Gateway unterstützt keine Amazon S3 S3-Buckets mit Punkten (`.`) im Bucket-Namen.
> Stellen Sie sicher, dass Ihr Bucket-Name den Regeln für die Bucket-Benennung in Amazon S3 entspricht. Weitere Informationen finden Sie unter Regeln für die Benennung von Buckets im Amazon Simple Storage Service-Benutzerhandbuch.

6. Benutzerauthentifizierung: Wählen Sie die Authentifizierungsmethode, die Sie verwenden möchten, aus der Dropdownliste aus:

   - Um das Microsoft Active Directory Ihres Unternehmens AWS Managed Microsoft AD zu verwenden oder den Benutzerzugriff auf Ihre SMB-Dateifreigabe zu authentifizieren, wählen Sie Active Directory. Ihr Gateway muss mit einer Domäne verbunden sein, um diese Methode verwenden zu können. Weitere Informationen finden Sie unter Verwenden von Active Directory zur Benutzerauthentifizierung.

   > **Note**
   >
   > Für die Verwendung AWS Managed Microsoft AD mit einem Amazon EC2 EC2-Gateway müssen Sie die Amazon EC2 EC2-Instance in derselben VPC wie die erstellen AWS Managed Microsoft AD, die `_workspaceMembers` Sicherheitsgruppe zur Amazon EC2 EC2-Instance hinzufügen und der AD-Domain mit den Administratoranmeldedaten von beitreten. AWS Managed Microsoft AD Weitere Informationen zu finden Sie im AWS Managed Microsoft AD Administratorhandbuch.AWS Directory Service
   > Weitere Informationen zu Amazon EC2 finden Sie in der Amazon Elastic Compute Cloud-Dokumentation.

   Wenn der Beitrittsstatus anzeigt, dass Ihr Gateway bereits einer Active Directory-Domain beigetreten ist, fahren Sie mit dem nächsten Schritt fort. Andernfalls gehen Sie wie folgt vor:

   1. Wählen Sie Konfigurieren aus.

2. Geben Sie unter Domain den Namen der Active Directory-Domäne ein, der Ihr Gateway beitreten soll.
3. Geben Sie den Benutzernamen und das Passwort ein, mit denen das Gateway der Domäne beitritt.
4. (Optional) Geben Sie unter Organisationseinheit (OU) die angegebene Organisationseinheit ein, die Ihr Active Directory für neue Computerobjekte verwendet.
5. (Optional) Geben Sie für Domänencontroller (DC) den Namen des Domänencontrollers ein, über den Ihr Gateway eine Verbindung zu Active Directory herstellt. Sie können dieses Feld leer lassen, damit DNS automatisch einen DC auswählt.
6. Wählen Sie Active Directory beitreten.

> **Note**
>
> Durch den Beitritt zu einer Domäne wird ein Active Directory-Konto im Standardcontainer (der keine Organisationseinheit ist) erstellt, das die Gateway-ID als Kontonamen verwendet (z. B. SGW-1234ADE). Es ist nicht möglich, den Namen dieses Kontos anzupassen.
> Wenn Ihre Active Directory-Umgebung erfordert, dass Sie Konten vorab bereitstellen, um den Domänenbeitritt zu erleichtern, müssen Sie dieses Konto im Voraus erstellen.
> Wenn Ihre Active Directory-Umgebung über eine festgelegte Organisationseinheit für neue Computerobjekte verfügt, müssen Sie diese Organisationseinheit angeben, wenn Sie der Domäne beitreten.

- Um jedem, der das von Ihnen konfigurierte Gastkennwort bereitstellt, kennwortgeschützten Zugriff zu gewähren, wählen Sie Gastzugriff. Ihr File Gateway muss nicht Teil einer Microsoft Active Directory-Domäne sein, um diese Methode verwenden zu können. Wählen Sie Configure, um Ihr Gast-Passwort anzugeben, und wählen Sie dann Save.

7. Überprüfen Sie die Einstellungen unter Standardkonfiguration und wählen Sie dann Dateifreigabe erstellen, um Ihre neue SMB-Dateifreigabe mit der Standardkonfiguration zu erstellen.

Nachdem Ihre SMB-Dateifreigabe erstellt wurde, können Sie ihre Konfigurationseinstellungen in der AWS Storage Gateway Gateway-Konsole auf der Registerkarte Details der Dateifreigabe einsehen. Informationen zum Mounten Ihrer Dateifreigabe finden Sie unter Mounten Ihrer SMB-Dateifreigabe auf Ihrem Client.

Standardkonfigurationseinstellungen für SMB-Dateifreigaben

Die folgenden Einstellungen gelten für alle neuen SMB-Dateifreigaben, die Sie mit der Standardkonfiguration erstellen. Nachdem Sie eine Dateifreigabe erstellt haben, können Sie sie auf der Seite Dateifreigaben in der AWS Storage Gateway Gateway-Konsole auswählen, um Details zu ihrer Konfiguration anzuzeigen.

> **Important**
>
> Die Standardkonfiguration für SMB-Dateifreigaben bietet dem Besitzer des S3-Buckets, der der Dateifreigabe zugeordnet ist, volle Dateikontrolle und Zugriffsberechtigungen, auch wenn der Bucket einem anderen Amazon Web Services Services-Konto gehört. Weitere Informationen zur Verwendung Ihrer Dateifreigabe für den Zugriff auf Objekte in einem Bucket, der einem anderen Konto gehört, finden Sie unter Verwenden einer Dateifreigabe für den kontoübergreifenden Zugriff.

Einstellung	Standardwert	Hinweise
Amazon S3 S3-Standort	Die Dateifreigabe stellt eine direkte Verbindung zum Amazon S3 S3-Bucket her und hat denselben Namen wie der Bucket. Ihr Gateway verwendet diesen Bucket zum Speichern und Abrufen von Dateien.	Der Name enthält kein Präfix.
AWS PrivateLink für S3	Die Dateifreigabe stellt keine Verbindung zu Amazon S3 über einen Schnittstellenendpunkt in Ihrer Virtual Private Cloud (VPC) her.	
Benachrichtigung beim Hochladen von Dateien	Aus	

Einstellung	Standardwert	Hinweise
Speicherklasse für neue Objekte	Amazon S3 Standard	Auf diese Weise können Sie Ihre Objektdaten, auf die häufig zugegriffen wird, redundant in mehreren Availability Zones speichern , die geografisch getrennt sind. Weitere Informationen zur Amazon S3 Standard Speicherklasse finden Sie unter Speicherklassen für Objekte mit häufigem Zugriff im Amazon Simple Storage Service-Benutzerhandbuch.
Verschlüsselung	Serverseitige Verschlüsselung mit verwalteten S3-Schlüsseln (SSE-S3)	Alle Amazon S3 S3-Objekte, die Ihr S3 File Gateway hochlädt, aktualisiert oder ändert, werden standardmäßig mit serverseitiger Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln verschlüsselt.

Einstellung	Standardwert	Hinweise
Objekt-Metadaten	Erraten Sie den MIME-Typ	Dadurch kann Storage Gateway den MIME-Typ (Multipurpose Internet Mail Extension) für hochgelad ene Objekte anhand von Dateierweiterungen erraten. Für diese Option müssen die Zugriffskontrolllisten (ACLs) für den Amazon S3 S3-Bucket aktiviert sein, der mit Ihrer Dateifreigabe verknüpft ist. ACLs Wenn ausgeschaltet, die Dateifreigabe kann nicht auf den Amazon S3 S3-Bucket zugreifen und verbleibt im Status Nicht verfügbar auf unbestimmte Zeit.
Zugriffsbasierte Aufzählung	Nicht aktiviert	Die Dateien und Ordner auf der Dateifreigabe sind für alle Benutzer sichtbar während der Verzeichnisaufzählung. Bei der zugriffsbasierten Aufzählung handelt es sich um ein System, das die Aufzählung von filtert Dateien und Ordner auf einer SMB-Dateifreigabe, basierend auf dem Zugriff auf die Freigabe Kontrolllisten (ACLs).

Einstellung	Standardwert	Hinweise
Aktiviere, dass der Antragsteller zahlt	Aus	Weitere Informationen finden Sie unter Buckets mit Bezahlung durch den Anforderer.
Opportunistisches Sperren	Ein	Auf diese Weise kann die Dateifreigabe opportunistisches Sperren zur Optimierung verwenden die Strategie zum Puffern von Dateien. In den meisten Fällen verbessert sich die Aktivierung von opportunistischem Sperren Leistung, insbesondere im Hinblick auf den Windows-Kontext Menüs.
Prüfungsprotokolle	Aus	Die Protokollierung bei einer Amazon CloudWatch Gruppe ist standardmäßig deaktiviert.
Berücksichtigung von Groß- und Kleinschreibung	Aus	Auf diese Weise kann der Client die Berücksichtigung der Groß- und Kleinschreibung steuern.
Zugriff auf Ihren S3-Bucket	Erstellen Sie eine neue IAM-Rolle	Die Standardoption ermöglicht es dem File Gateway, eine neue IAM-Rolle und den Zugriff darauf zu erstellen Richtlinie in Ihrem Namen.

Erstellen Sie eine SMB-Dateifreigabe mit einer benutzerdefinierten Konfiguration

Gehen Sie wie folgt vor, um eine SMB-Dateifreigabe (Server Message Block) mit einer benutzerdefinierten Konfiguration zu erstellen. Informationen zum Erstellen einer SMB-Dateifreigabe mithilfe der Standardkonfigurationseinstellungen finden Sie unter Erstellen einer SMB-Dateifreigabe mit der Standardkonfiguration.

> **Important**
>
> Die Verwendung von S3 Versioning, regionsübergreifender Replikation oder des Dienstprogramms Rsync beim Hochladen von Daten von einem File Gateway kann erhebliche Kostenauswirkungen haben. Weitere Informationen finden Sie unter Vermeidung unerwarteter Kosten beim Hochladen von Daten von File Gateway.

Voraussetzungen

Gehen Sie wie folgt vor, bevor Sie Ihre Dateifreigabe erstellen:

- Konfigurieren Sie die SMB-Sicherheitseinstellungen für Ihr File Gateway. Anweisungen finden Sie unter Eine Sicherheitsstufe für Ihr Gateway festlegen.
- Konfigurieren Sie entweder Microsoft Active Directory oder den Gastzugriff für die Authentifizierung. Anweisungen finden Sie unter Verwenden von Active Directory zur Benutzerauthentifizierung oder Bereitstellen von Gastzugriff auf Ihre Dateifreigabe.
- Stellen Sie sicher, dass die erforderlichen Ports in Ihrer Sicherheitsgruppe geöffnet sind. Weitere Informationen finden Sie unter Portanforderungen.

Um eine SMB-Dateifreigabe mit benutzerdefinierten Einstellungen zu erstellen

1. Öffnen Sie die AWS Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home/ und wählen Sie im linken Navigationsbereich Dateifreigaben aus.
2. Wählen Sie Create file share (Dateifreigabe erstellen) aus.
3. Wählen Sie Konfiguration anpassen. Sie können die anderen Felder auf dieser Seite vorerst ignorieren. In den nachfolgenden Schritten werden Sie aufgefordert, die Gateway-, Protokoll- und Speichereinstellungen zu konfigurieren.

4. Wählen Sie für Gateway das Amazon S3 File Gateway aus der Drop-down-Liste aus.
5. Wählen Sie für die CloudWatch Protokollgruppe eine der folgenden Optionen aus der Drop-down-Liste aus:

   - Um die Protokollierung für diese Dateifreigabe zu deaktivieren, wählen Sie Protokollierung deaktivieren.
   - Um automatisch eine neue Protokollgruppe für diese Dateifreigabe zu erstellen, wählen Sie Created by Storage Gateway.
   - Um Integritäts- und Ressourcenbenachrichtigungen für diese Dateifreigabe an eine bestehende Protokollgruppe zu senden, wählen Sie die gewünschte Gruppe aus der Liste aus.

   Weitere Informationen zu Audit-Logs finden Sie unter Grundlegendes zu S3 File Gateway-Auditprotokollen.
6. (Optional) Wählen Sie unter Tags — Optional die Option Neues Tag hinzufügen aus und geben Sie dann einen Schlüssel und einen Wert für Ihre Dateifreigabe ein. Ein Tag ist ein Schlüssel-Wert-Paar, bei dem Groß- und Kleinschreibung beachtet wird und Ihnen hilft, Ihre Storage Gateway Gateway-Ressourcen zu kategorisieren. Das Hinzufügen von Tags kann das Filtern und Suchen nach Ihrer Dateifreigabe vereinfachen. Sie können diesen Schritt wiederholen, um bis zu 50 Tags hinzuzufügen.

   Wählen Sie Weiter, wenn Sie fertig sind.
7. Führen Sie für einen S3-Bucket einen der folgenden Schritte aus, um anzugeben, wo Dateien gespeichert und abgerufen werden sollen:

   - Um die Dateifreigabe direkt mit einem vorhandenen S3-Bucket in Ihrem Amazon Web Services Services-Konto zu verbinden, wählen Sie den Bucket-Namen aus der Drop-down-Liste aus.
   - Um die Dateifreigabe mit einem vorhandenen S3-Bucket zu verbinden, der einem anderen Amazon Web Services Services-Konto als dem gehört, das Sie zum Erstellen der Dateifreigabe verwenden, wählen Sie In der Dropdownliste Ein Bucket in einem anderen Konto aus und geben Sie dann den kontoübergreifenden Bucket-Namen ein.
   - Um die Dateifreigabe mit einem neuen S3-Bucket zu verbinden, wählen Sie Create a new S3-Bucket aus, wählen Sie dann die Region aus, in der sich der Amazon S3 S3-Endpunkt für Ihren neuen Bucket befindet, und geben Sie einen eindeutigen S3-Bucket-Namen ein. Wenn Sie fertig sind, wählen Sie S3-Bucket erstellen. Weitere Informationen zum Erstellen neuer Buckets finden Sie unter Wie erstelle ich einen S3-Bucket? im Amazon S3 S3-Benutzerhandbuch.

- Um die Dateifreigabe mithilfe eines Zugriffspunktnamens mit einem S3-Bucket zu verbinden, wählen Sie den Namen des Amazon S3 S3-Zugriffspunkts aus der Drop-down-Liste aus und geben Sie dann den Namen des Access Points ein. Wenn Sie einen neuen Access Point erstellen müssen, können Sie Create an S3 Access Point wählen. Weitere Anweisungen finden Sie unter Erstellen eines Access Points im Amazon S3 S3-Benutzerhandbuch. Weitere Informationen zu Access Points finden Sie unter Verwaltung des Datenzugriffs mit Amazon S3 S3-Zugriffspunkten und Delegieren der Zugriffskontrolle an Access Points im Amazon S3 S3-Benutzerhandbuch.
- Um die Dateifreigabe mithilfe eines Access Point-Alias mit einem S3-Bucket zu verbinden, wählen Sie den Amazon S3 S3-Zugriffspunkt-Alias aus der Drop-down-Liste aus und geben Sie dann den Access Point-Alias ein. Wenn Sie einen neuen Access Point erstellen müssen, können Sie Create an S3 Access Point wählen. Weitere Anweisungen finden Sie unter Erstellen eines Access Points im Amazon S3 S3-Benutzerhandbuch. Weitere Informationen zu Access Point-Aliasnamen finden Sie unter Verwenden eines Alias im Bucket-Stil für Ihren Access Point im Amazon S3 S3-Benutzerhandbuch.

> **Note**
>
> Jede Dateifreigabe kann nur mit einem S3-Bucket verbunden werden, aber mehrere Fileshares können eine Verbindung zu demselben Bucket herstellen. Wenn Sie mehr als eine Dateifreigabe mit demselben Bucket verbinden, müssen Sie jede Dateifreigabe so konfigurieren, dass sie ein eindeutiges, sich nicht überschneidendes S3-Bucket-Präfix verwendet, um Konflikte zu vermeiden read/write .
>
> S3 File Gateway unterstützt keine Amazon S3 S3-Buckets mit Punkten (`.`) im Bucket-Namen.
>
> Stellen Sie sicher, dass Ihr Bucket-Name den Regeln für die Bucket-Benennung in Amazon S3 entspricht. Weitere Informationen finden Sie unter Regeln für die Bucket-Benennung im Amazon Simple Storage Service-Benutzerhandbuch.

8. (Optional) Geben Sie für das S3-Bucket-Präfix ein Präfix für Ihre Dateifreigabe ein, das auf die Objekte angewendet werden soll, die sie in Amazon S3 erstellt. Präfixe sind eine Möglichkeit, Ihre Daten in S3 zu organisieren, ähnlich wie Verzeichnisse in herkömmlichen Dateistrukturen. Weitere Informationen finden Sie unter Objekte mithilfe von Präfixen organisieren im Amazon S3 S3-Benutzerhandbuch.

> **Note**
>
> - Wenn Sie mehr als eine Dateifreigabe mit demselben Bucket verbinden, müssen Sie jede Dateifreigabe so konfigurieren, dass sie ein eindeutiges, sich nicht überschneidendes Präfix verwendet, um Konflikte zu vermeiden. read/write
> - Das Präfix muss mit einem Schrägstrich enden (/).
> - Nachdem die Dateifreigabe erstellt wurde, kann das Präfix weder geändert noch gelöscht werden.

9. Wählen Sie für Region aus der Dropdownliste aus, AWS-Region wo sich der S3-Endpunkt für Ihren Bucket befindet. Dieses Feld wird nur angezeigt, wenn Sie einen Access Point oder einen Bucket in einem anderen Konto für den S3-Bucket angeben.
10. Wählen Sie für Speicherklasse für neue Objekte eine Speicherklasse aus der Dropdownliste aus. Weitere Informationen zu Speicherklassen finden Sie unter Speicherklassen mit einem File Gateway verwenden.
11. Gehen Sie für IAM-Rolle wie folgt vor, um eine IAM-Rolle für Ihre Dateifreigabe zu konfigurieren:

    - Um automatisch eine neue IAM-Rolle mit den erforderlichen Berechtigungen zu erstellen, damit Ihre Dateifreigabe ordnungsgemäß funktioniert, wählen Sie Created by Storage Gateway aus der Dropdownliste aus.
    - Um eine bestehende IAM-Rolle zu verwenden, wählen Sie den Rollennamen aus der Dropdownliste aus.
    - Um eine neue IAM-Rolle zu erstellen, wählen Sie Create a role aus. Weitere Anweisungen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst.

    Weitere Informationen darüber, wie IAM-Rollen den Zugriff zwischen Ihrer Dateifreigabe und Ihrem S3-Bucket steuern, finden Sie unter Zugriff auf einen Amazon S3-Bucket gewähren.
12. Gehen Sie für Private Link nur dann wie folgt vor, wenn Sie Ihre Dateifreigabe für die Kommunikation AWS mit einem privaten Endpunkt in einer Virtual Private Cloud (VPC) konfigurieren müssen. Andernfalls überspringen Sie diesen Schritt. Weitere Informationen finden Sie unter Was ist AWS PrivateLink? im AWS PrivateLink Leitfaden.

    a. Wählen Sie VPC-Endpunkt verwenden aus.

b. Führen Sie unter Identifizieren des VPC-Endpunkts durch einen der folgenden Schritte aus:

   - Wählen Sie VPC-Endpunkt-ID und dann den Endpunkt, den Sie verwenden möchten, aus der VPC-Endpunkt-Dropdownliste aus.
   - Wählen Sie DNS-Name aus und geben Sie dann den DNS-Namen für den Endpunkt ein, den Sie verwenden möchten.

13. Wählen Sie für Verschlüsselung den Typ der Verschlüsselungsschlüssel aus, die zum Verschlüsseln von Objekten verwendet werden sollen, die Ihr File Gateway in Amazon S3 speichert:

    - Um serverseitige Verschlüsselung zu verwenden, die mit Amazon S3 (SSE-S3) verwaltet wird, wählen Sie S3-Managed Keys (SSE-S3).

      Weitere Informationen finden Sie unter Verwenden der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

    - Um die serverseitige Verschlüsselung zu verwenden, die mit dem AWS Key Management Service (SSE-KMS) verwaltet wird, wählen Sie KMS-verwaltete Schlüssel (SSE-KMS). Wählen Sie für den primären KMS-Schlüssel einen vorhandenen AWS KMS-Schlüssel aus, oder wählen Sie Neuen KMS-Schlüssel erstellen, um einen neuen KMS-Schlüssel in der AWS Key Management Service () -Konsole zu erstellen.AWS KMS

      Weitere Informationen zu finden Sie AWS KMS unter Was ist der AWS Schlüsselverwaltungsdienst? im AWS Key Management Service Entwicklerhandbuch.

    - Um die serverseitige Dual-Layer-Verschlüsselung zu verwenden, die mit dem AWS Key Management Service (DSSE-KMS) verwaltet wird, wählen Sie Serverseitige Dual-Layer-Verschlüsselung mit Schlüsseln (DSSE-KMS). AWS Key Management Service Wählen Sie für den primären KMS-Schlüssel einen vorhandenen AWS KMS-Schlüssel aus, oder wählen Sie Neuen KMS-Schlüssel erstellen, um in der Key Management Service () -Konsole einen neuen KMS-Schlüssel zu erstellen. AWS AWS KMS

      Weitere Informationen zu DSSE-KMS finden Sie unter Verwenden der dualen serverseitigen Verschlüsselung mit AWS KMS Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Für die Verwendung von DSSE-KMS und Schlüsseln fallen zusätzliche Gebühren an. AWS KMS Weitere Informationen finden Sie unter AWS KMS Preise.
> Um einen AWS KMS Schlüssel mit einem Alias anzugeben, der nicht aufgeführt ist, oder um einen AWS KMS Schlüssel aus einem anderen AWS Konto zu verwenden, müssen Sie den verwenden. AWS Command Line Interface Asymmetrische KMS-Schlüssel werden nicht unterstützt. Weitere Informationen finden Sie unter Create SMBFile Share in der AWS Storage Gateway API-Referenz.

> **Important**
>
> Stellen Sie sicher, dass Ihre Dateifreigabe denselben Verschlüsselungstyp verwendet wie der Amazon S3 S3-Bucket, in dem Ihre Daten gespeichert werden.

14. Wählen Sie für Guess MIME-Typen die Option Guess media MIME type aus, damit Storage Gateway den MIME-Typ (Multipurpose Internet Mail Extension) für hochgeladene Objekte anhand ihrer Dateierweiterungen erraten kann.
15. Geben Sie unter Name der Dateifreigabe einen Namen für Ihre Dateifreigabe ein.

> **Note**
>
> Ein gültiger SMB-Dateifreigabename darf die folgenden Zeichen nicht enthalten: `[ ]#,;,<,>,:,",\,/,,|, ? *+`, oder ASCII-Steuerzeichen. `1-31`

16. Wählen Sie für Upload-Ereignisse die Option Ereignis protokollieren, wenn eine Datei erfolgreich vom Gateway hochgeladen wurde, wenn Sie möchten, dass Ihr Gateway CloudWatch Protokollereignisse aufzeichnet, wenn es erfolgreich Dateien auf Amazon S3 hochlädt. Die Benachrichtigungsverzögerung steuert die Verzögerung zwischen dem letzten Schreibvorgang des Clients und der Generierung der `ObjectUploaded` Protokollbenachrichtigung. Da Clients in kurzer Zeit viele kleine Schreibvorgänge in Dateien ausführen können, empfehlen wir, diesen Parameter so lange wie möglich festzulegen, um zu vermeiden, dass mehrere Benachrichtigungen für dieselbe Datei schnell hintereinander generiert werden. Weitere Informationen finden Sie unter Benachrichtigung über Datei-Uploads erhalten.

> **Note**
>
> Diese Einstellung hat keinen Einfluss auf den Zeitpunkt, zu dem das Objekt auf S3 hochgeladen wird, sondern nur auf den Zeitpunkt der Benachrichtigung.
> Diese Einstellung ist nicht dazu gedacht, einen genauen Zeitpunkt anzugeben, zu dem die Benachrichtigung gesendet wird. In einigen Fällen benötigt das Gateway möglicherweise mehr als die angegebene Verzögerungszeit, um Benachrichtigungen zu generieren und zu senden.

Wählen Sie Weiter, wenn Sie fertig sind.

17. Wählen Sie für File Share Protocol die Option SMB aus.
18. Wählen Sie für die Benutzerauthentifizierung die Authentifizierungsmethode, die Sie verwenden möchten, aus der Dropdownliste aus:

    - Um das Microsoft Active Directory Ihres Unternehmens AWS Managed Microsoft AD zu verwenden oder den Benutzerzugriff auf Ihre SMB-Dateifreigabe zu authentifizieren, wählen Sie Active Directory. Ihr Gateway muss mit einer Domäne verbunden sein, um diese Methode verwenden zu können. Weitere Informationen finden Sie unter Verwenden von Active Directory zur Benutzerauthentifizierung.

      > **Note**
      >
      > Für die Verwendung AWS Managed Microsoft AD mit einem Amazon EC2 EC2-Gateway müssen Sie die Amazon EC2 EC2-Instance in derselben VPC wie die erstellen AWS Managed Microsoft AD, die `_workspaceMembers` Sicherheitsgruppe zur Amazon EC2 EC2-Instance hinzufügen und der AD-Domain mit den Admin-Anmeldeinformationen von beitreten. AWS Managed Microsoft AD
      > Weitere Informationen zu finden Sie im AWS Managed Microsoft AD Administratorhandbuch.AWS Directory Service
      > Weitere Informationen zu Amazon EC2 finden Sie in der Amazon Elastic Compute Cloud-Dokumentation.

    Wenn der Beitrittsstatus anzeigt, dass Ihr Gateway bereits einer Active Directory-Domain beigetreten ist, fahren Sie mit dem nächsten Schritt fort. Andernfalls gehen Sie wie folgt vor:

1. Wählen Sie Konfigurieren aus.
2. Geben Sie unter Domain den Namen der Active Directory-Domäne ein, der Ihr Gateway beitreten soll.
3. Geben Sie den Benutzernamen und das Passwort ein, mit denen das Gateway der Domäne beitritt.
4. (Optional) Geben Sie unter Organisationseinheit (OU) die angegebene Organisationseinheit ein, die Ihr Active Directory für neue Computerobjekte verwendet.
5. (Optional) Geben Sie für Domänencontroller (DC) den Namen des Domänencontrollers ein, über den Ihr Gateway eine Verbindung zu Active Directory herstellt. Sie können dieses Feld leer lassen, damit DNS automatisch einen DC auswählt.
6. Wählen Sie Active Directory beitreten.

> **Note**
>
> Durch den Beitritt zu einer Domäne wird ein Active Directory-Konto im Standardcontainer (der keine Organisationseinheit ist) erstellt, wobei die Gateway-ID des Gateways als Kontoname verwendet wird (z. B. SGW-1234ADE). Es ist nicht möglich, den Namen dieses Kontos anzupassen.
> Wenn Ihre Active Directory-Umgebung erfordert, dass Sie Konten vorab bereitstellen, um den Domänenbeitritt zu erleichtern, müssen Sie dieses Konto im Voraus erstellen.
> Wenn Ihre Active Directory-Umgebung über eine festgelegte Organisationseinheit für neue Computerobjekte verfügt, müssen Sie diese Organisationseinheit angeben, wenn Sie der Domäne beitreten.

- Um jedem, der das von Ihnen konfigurierte Gastkennwort bereitstellt, kennwortgeschützten Zugriff zu gewähren, wählen Sie Gastzugriff. Ihr File Gateway muss nicht Teil einer Microsoft Active Directory-Domäne sein, um diese Methode verwenden zu können. Wählen Sie Configure, um Ihr Gast-Passwort anzugeben, und wählen Sie dann Speichern.

19. Gehen Sie für den Benutzerzugriff wie folgt vor, um anzugeben, welche SMB-Clients auf Ihre Dateifreigabe zugreifen können:

    - Um allen Benutzern, die sich erfolgreich über Active Directory authentifiziert haben, Zugriff zu gewähren, wählen Sie Alle AD-authentifizierten Benutzer aus.
    - Um bestimmten Benutzern oder Gruppen den Zugriff zu gewähren oder zu verweigern, wählen Sie Bestimmte AD-authentifizierte Benutzer oder Gruppen aus und gehen Sie dann wie folgt vor:

- Wählen Sie unter Zulässige Benutzer und Gruppen die Option Zulässigen Benutzer hinzufügen oder Zulässige Gruppe hinzufügen aus und geben Sie einen Active Directory-Benutzer oder eine Active Directory-Gruppe ein, dem/der Sie den Dateifreigabezugriff gewähren möchten. Wiederholen Sie diesen Vorgang, um so viele Benutzer und Gruppen wie nötig zuzulassen
- Wählen Sie für Verweigerte Benutzer und Gruppen die Option Abgelehnten Benutzer hinzufügen oder Verweigerte Gruppe hinzufügen aus und geben Sie einen Active Directory-Benutzer oder eine Active Directory-Gruppe ein, dem/der Sie den Dateifreigabezugriff verweigern möchten. Wiederholen Sie diesen Vorgang, um so vielen Benutzern und Gruppen wie nötig den Zugriff zu verweigern.

> **Note**
>
> Der Abschnitt Dateifreigabezugriff für Benutzer und Gruppen wird nur angezeigt, wenn die Benutzerauthentifizierung auf Active Directory eingestellt ist.
> Geben Sie bei der Angabe von Benutzern oder Gruppen die Domäne nicht an. Der Domänenname wird durch die Mitgliedschaft des Gateways in dem spezifischen Active Directory impliziert, mit dem es verbunden ist.

20. (Optional) Geben Sie für Admin-Benutzer eine durch Kommas getrennte Liste von Active Directory-Benutzern und -Gruppen ein. Admin-Benutzer erhalten das Recht, die Zugriffskontrolllisten (ACLs) für alle Dateien und Ordner in der Dateifreigabe zu aktualisieren. Gruppen muss das `@` Zeichen vorangestellt werden, zum Beispiel. `@group1`
21. Wählen Sie für Zugriffstyp eine der folgenden Optionen aus:

    - Wählen Sie Lesen/Schreiben, um Clients das Lesen und Schreiben von Dateien auf der Dateifreigabe zu ermöglichen.
    - Wählen Sie Schreibgeschützt aus, damit Clients Dateien lesen, aber nicht in die Dateifreigabe schreiben können.

    > **Note**
    >
    > Wenn Sie bei Dateifreigaben, die auf einem Microsoft Windows-Client bereitgestellt sind, Schreibgeschützt wählen, wird möglicherweise eine Meldung über einen

unerwarteten Fehler angezeigt, der Sie daran hindert, den Ordner zu erstellen. Sie können diese Meldung ignorieren.

22. Wählen Sie für Datei- und Verzeichniszugriffskontrolle eine der folgenden Optionen aus:

    - Um detaillierte Berechtigungen für Dateien und Ordner in Ihrer SMB-Dateifreigabe festzulegen, wählen Sie Windows-Zugriffssteuerungsliste aus. Weitere Informationen finden Sie unter Steuern des Zugriffs auf eine SMB-Dateifreigabe mithilfe von Microsoft Windows ACLs .
    - Wenn Sie POSIX-Berechtigungen verwenden möchten, um den Zugriff auf Dateien und Verzeichnisse zu steuern, die über Ihre SMB-Dateifreigabe gespeichert sind, wählen Sie POSIX-Berechtigungen.

23. Führen Sie für eine Access-basierte Aufzählung einen der folgenden Schritte aus:

    - Um die Dateien und Ordner auf der Freigabe nur für Benutzer mit Lesezugriff sichtbar zu machen, wählen Sie Dateien und Verzeichnisse ausblenden, für die der Benutzer keine Zugriffsrechte hat.
    - Um die Dateien und Ordner auf der Freigabe während der Verzeichnisaufzählung für alle Benutzer sichtbar zu machen, aktivieren Sie das Kontrollkästchen nicht.

    > **Note**
    >
    > Bei der zugriffsbasierten Aufzählung handelt es sich um ein System, das die Aufzählung von Dateien und Ordnern auf einer SMB-Dateifreigabe anhand der Zugriffskontrolllisten der Freigabe () filtert. ACLs

24. Wählen Sie für Dateizugriffsoptionen eine der folgenden Optionen aus:

    - Um die Dateipufferungsstrategie der Dateifreigabe mithilfe von opportunistischem Sperren zu optimieren, wählen Sie Opportunistische Sperre. In den meisten Fällen verbessert die Aktivierung von opportunistischem Sperren die Leistung, insbesondere im Hinblick auf Windows-Kontextmenüs.
    - Damit das Gateway — und nicht der SMB-Client — die Berücksichtigung der Groß- und Kleinschreibung von Dateinamen steuern kann, wählen Sie Berücksichtigung von Groß- und Kleinschreibung erzwingen aus.
    - Um beide Einstellungen zu deaktivieren, wählen Sie Keine aus.

> **Note**
>
> Um Dateizugriffskonflikte zu vermeiden, schließen sich diese Einstellungen gegenseitig aus und können nicht gleichzeitig aktiviert werden.

25. (Optional) Wählen Sie für Automatisierte Cacheaktualisierung von S3 die Option Cache-Aktualisierungsintervall festlegen und legen Sie dann mithilfe von Time To Live (TTL) die Zeit in Minuten oder Tagen fest, zu der der Cache der Dateifreigabe aktualisiert werden soll. TTL ist die Zeitspanne seit der letzten Aktualisierung. Nach Ablauf des TTL-Intervalls aktualisiert das File Gateway beim Zugriff auf ein Verzeichnis den Inhalt dieses Verzeichnisses aus dem Amazon S3 S3-Bucket.

    > **Note**
    >
    > Wenn dieser Wert kürzer als 30 Minuten ist, kann sich dies negativ auf die Gateway-Leistung auswirken, wenn häufig eine große Anzahl von Amazon S3 S3-Objekten erstellt oder gelöscht wird.

26. Wählen Sie für Dateibesitz und Berechtigungen die Option Dem Besitzer des S3-Buckets das volle Eigentum an den vom Gateway erstellten Dateien geben aus, einschließlich Lese-, Schreib-, Bearbeitungs- und Löschberechtigungen, wenn das AWS Konto, dem der S3-Bucket gehört, die volle Kontrolle über alle Objekte haben soll, die von Ihrer Dateifreigabe in den Bucket geschrieben werden.

    Wählen Sie Weiter, wenn Sie fertig sind.

27. Überprüfen Sie die Konfiguration der Dateifreigabe. Wählen Sie Bearbeiten, um die Einstellungen für jeden Abschnitt zu ändern, den Sie ändern möchten. Wenn Sie fertig sind, wählen Sie Erstellen.

Nachdem Ihre SMB-Dateifreigabe erstellt wurde, können Sie ihre Konfigurationseinstellungen in der AWS Storage Gateway Gateway-Konsole auf der Registerkarte Details der Dateifreigabe einsehen. Anweisungen zum Mounten Ihrer Dateifreigabe finden Sie unter Mounten Ihrer SMB-Dateifreigabe auf Ihrem Client.

Eine Dateifreigabe kopieren

> **Note**
>
> Die Funktion zum Kopieren von Dateifreigaben ist nur über die Storage Gateway Gateway-Konsole verfügbar. Für diese Funktion gibt es keinen entsprechenden AWS CLI-Befehl oder keine API-Aktion.

Sie können die Storage Gateway Gateway-Konsole verwenden, um eine bestehende NFS- oder SMB-Dateifreigabe auf ein anderes Gateway zu kopieren. Durch das Kopieren einer Dateifreigabe wird eine neue Dateifreigabe auf dem Ziel-Gateway erstellt, die auf denselben Amazon S3 S3-Bucket wie die Quelldateifreigabe verweist, wobei die meisten Konfigurationseinstellungen der ursprünglichen Freigabe beibehalten werden. Dies soll in erster Linie bei Gateway-Migrationen helfen, sodass Sie eine Dateifreigabe auf ein Ersatz-Gateway verschieben können, ohne die Konfiguration manuell neu erstellen zu müssen. Nachdem Sie sich vergewissert haben, dass die kopierte Dateifreigabe auf dem neuen Gateway ordnungsgemäß funktioniert, sollten Sie die ursprüngliche Dateifreigabe vom Quell-Gateway löschen.

Überlegungen

Bevor Sie eine Dateifreigabe kopieren, sollten Sie Folgendes beachten:

- Das Ziel-Gateway muss sich im Status Aktiv befinden.
- Sowohl das Quell- als auch das Ziel-Gateway müssen Amazon S3 File Gateway-Gateways sein. Sie können keine Dateifreigaben zwischen verschiedenen Gateway-Typen kopieren.
- Die kopierte Dateifreigabe verweist auf denselben Amazon S3 S3-Bucket wie die Quelle. Wir empfehlen nicht, beide Dateifreigaben über einen längeren Zeitraum aktiv zu verwalten. Wenn von mehreren Gateways gleichzeitig in denselben Amazon S3 S3-Bucket geschrieben wird, kann dies zu Dateninkonsistenzen, Cache-Konflikten und unerwartetem Verhalten führen. Nachdem Sie sich vergewissert haben, dass die kopierte Dateifreigabe ordnungsgemäß funktioniert, löschen Sie die Quell-Dateifreigabe.
- Beim Kopiervorgang wird das Dateifreigabeprotokoll (NFS oder SMB) beibehalten. Sie können den Protokolltyp während des Kopiervorgangs nicht ändern.
- Wenn die Quelldateifreigabe eine IAM-Rolle für den Amazon S3 S3-Bucket-Zugriff verwendet, können Sie wählen, ob Sie dieselbe Rolle für die kopierte Dateifreigabe verwenden, eine andere

bestehende Rolle auswählen oder die Konsole automatisch eine neue Rolle erstellen lassen möchten.

- Wenn für die Quelldateifreigabe die CloudWatch Protokollgruppenüberwachung konfiguriert ist, können Sie wählen, ob Sie dieselbe Protokollgruppe verwenden, eine andere Protokollgruppe auswählen oder die Konsole automatisch eine neue Protokollgruppe erstellen lassen möchten.
- Wenn Sie eine SMB-Dateifreigabe zwischen Gateways kopieren, die zu verschiedenen Active Directory-Domänen gehören, oder zwischen einem Gateway mit Active Directory-Authentifizierung und einem Gateway mit Gastzugriff, überprüfen Sie nach Abschluss des Kopiervorgangs Ihre SMB-Zugriffseinstellungen, um sicherzustellen, dass die Zugriffsberechtigungen korrekt konfiguriert sind.
- Wenn die Quell- und Ziel-Gateways unterschiedliche VPC-Konfigurationen haben (z. B. ist ein Gateway in einer VPC aktiviert und das andere nicht), verwendet die kopierte Dateifreigabe die Netzwerkkonfiguration des Ziel-Gateways.

> **Important**
>
> Beim Kopieren einer SMB-Dateifreigabe werden Zugriffskontrolllisten (ACLs) auf Stammebene nicht in die neue Dateifreigabe kopiert. Die kopierte Dateifreigabe wird mit Standard-Root-ACLs erstellt. Wenn Sie benutzerdefinierte Root-ACLs auf der Quelldateifreigabe konfiguriert haben, müssen Sie diese nach Abschluss des Kopiervorgangs auf der kopierten Dateifreigabe manuell neu konfigurieren.

Kopieren Sie eine Dateifreigabe auf ein anderes Gateway

So kopieren Sie eine Dateifreigabe mit der Storage Gateway Gateway-Konsole

1. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich die Option Dateifreigaben aus.
3. Wählen Sie die Dateifreigabe aus, die Sie kopieren möchten.
4. Wählen Sie im Menü Aktionen die Option Dateifreigabe auf ein anderes Gateway kopieren aus.
5. Wählen Sie für Gateway das Ziel-Gateway aus, auf dem Sie die Kopie erstellen möchten.
6. Wählen Sie für die IAM-Rolle eine der folgenden Optionen:

- Dieselbe IAM-Rolle verwenden — Verwendet dieselbe IAM-Rolle wie die Quelldateifreigabe. Wählen Sie diese Option, wenn das Ziel-Gateway dieselben Berechtigungen für den Zugriff auf den Amazon S3 S3-Bucket verwenden soll.
- Wählen Sie eine bestehende IAM-Rolle aus — Wählen Sie eine andere IAM-Rolle aus der Liste aus. Stellen Sie sicher, dass die Rolle die erforderlichen Amazon S3 S3-Berechtigungen gewährt.
- Auto-generate eine neue IAM-Rolle — Die Konsole erstellt eine neue IAM-Rolle mit den erforderlichen Berechtigungen für den Amazon S3 S3-Bucket.

7. Wählen Sie für Protokollgruppe eine der folgenden Optionen:

   - Dieselbe Protokollgruppe verwenden — Sendet Integritätsprotokolle an dieselbe CloudWatch Protokollgruppe wie die Quelldateifreigabe.
   - Eine bestehende Protokollgruppe auswählen — Wählen Sie eine andere CloudWatch Protokollgruppe aus der Liste aus.
   - Auto-generate eine neue Protokollgruppe — Die Konsole erstellt eine neue CloudWatch Protokollgruppe für die kopierte Dateifreigabe.

8. Wählen Sie Dateifreigabe kopieren.

Die neue Dateifreigabe wird in der Liste Dateifreigaben mit dem Status Wird erstellt angezeigt. Sobald die Freigabe verfügbar ist, können Sie sie mit demselben Protokoll wie die Quellfreigabe auf Ihren Clients bereitstellen.

Einstellungen werden beim Kopieren beibehalten

Wenn Sie eine Dateifreigabe kopieren, werden die folgenden Einstellungen von der Quelldateifreigabe auf die neue Kopie übertragen:

- Name und Präfix des Amazon S3 S3-Buckets
- Speicherklasse
- Einstellungen für die Objektverschlüsselung (SSE-S3 SSE-KMS, oder DSSE-KMS)
- Fileshare-Protokoll (NFS oder SMB)
- Einstellungen für die Cache-Aktualisierung
- Squash-Einstellungen und Client-Zugriff (NFS-Dateifreigaben)

- SMB-Zugriffseinstellungen, einschließlich Authentifizierungsmethode, Sichtbarkeit von Dateifreigaben und zugriffsbasierter Aufzählung (SMB-Dateifreigaben)
- Zulässige und verweigerte Benutzer und Gruppen (SMB-Dateifreigaben)

Die folgenden Einstellungen werden nicht kopiert und verwenden die Konfiguration oder Standardeinstellungen des Ziel-Gateways:

- Gateway-Netzwerkkonfiguration (VPC-Endpunkt, öffentlicher Endpunkt)
- Active Directory-Domänenmitgliedschaft (verwendet die AD-Konfiguration des Ziel-Gateways)
- Grenzwerte für die Bandbreitenrate (verwendet die Grenzwerte des Ziel-Gateways)
- Root-level ACLs (SMB-Dateifreigaben — die kopierte Freigabe wird mit Standard-Root-ACLs erstellt)

Mounten und Verwenden Ihrer Dateifreigabe

Die Themen in diesem Abschnitt enthalten Anweisungen dazu, wie Sie Ihre Dateifreigabe auf Ihrem Client bereitstellen, Ihre Dateifreigabe verwenden, Ihr File Gateway testen und nicht mehr benötigte Ressourcen wie Gateways, Amazon EC2 EC2-Instances oder lokale Ressourcen bereinigen, VMs die Sie möglicherweise zu Testzwecken erstellen. Weitere Informationen zu unterstützten Network File System (NFS) - und Service Message Block (SMB) -Clients finden Sie unter. Unterstützte NFS- und SMB-Clients für File Gateway

> **Note**
>
> AWS-Managementkonsole Es enthält auch Beispielbefehle, mit denen Sie Ihre Dateifreigabe mounten können.

Topics

- Mounten Sie Ihre NFS-Dateifreigabe auf Ihrem Client- Erfahren Sie, wie Sie Ihre NFS-Dateifreigabe auf einem Laufwerk auf Ihrem Client mounten und sie Ihrem Amazon S3 S3-Bucket zuordnen.
- Mounten Sie Ihre SMB-Dateifreigabe auf Ihrem Client- Erfahren Sie, wie Sie Ihre SMB-Dateifreigabe mounten und einem Laufwerk zuordnen, auf das Ihr Kunde Zugriff hat.
- Verwenden von Dateifreigaben für Buckets mit bereits vorhandenen Objekten- Erfahren Sie, wie Sie eine Dateifreigabe in einem Amazon S3 S3-Bucket mit Objekten exportieren, die außerhalb des File Gateways mit NFS oder SMB erstellt wurden.
- Testen Sie Ihr S3 File Gateway- Erfahren Sie, wie Sie Ihr Gateway testen können, indem Sie Dateien und Ordner auf Ihr zugeordnetes Laufwerk kopieren und überprüfen, ob sie automatisch in Ihrem Amazon S3 S3-Bucket erscheinen.

Mounten Sie Ihre NFS-Dateifreigabe auf Ihrem Client

Gehen Sie wie folgt vor, um Ihre NFS-Dateifreigabe auf einem Laufwerk auf Ihrem Client zu mounten und sie Ihrem Amazon S3-Bucket zuzuordnen.

So mounten Sie eine Dateifreigabe und ordnen 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 *[GatewayVMIPAddress]*:/*[FileShareName]* *[ClientMountPath]*

   - Geben Sie für Windows-Clients den folgenden Befehl an der Befehlszeile ein (cmd.exe).

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

   Nehmen wir beispielsweise an, dass auf einem Windows-Client die IP-Adresse Ihrer VM 123.123.1.2 lautet und der Name Ihrer Dateifreigabe lautet. `test-fileshare` 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-fileshare T:

   > **Note**
   >
   > Beachten Sie beim Mounten von Dateifreigaben Folgendes:
   >
   > - Standardmäßig verwendet Windows einen Softmount für NFS-Shares. Bei Soft-Mounts wird das Timeout leichter überschritten, wenn Verbindungsprobleme auftreten. Wir empfehlen die Verwendung eines Hard Mounts für kritische Workloads, da Hard Mounts sicherer sind und Ihre Daten besser schützen. Um eine Hardmount zu verwenden, stellen Sie sicher, dass Ihr Befehl den `-o mtype=hard` Switch verwendet.
   > - S3 File Gateway unterstützt das Sperren von NFS-Dateien nicht. Verwenden Sie beim Mounten von NFS-Dateifreigaben immer die `-o nolock` Option zum Deaktivieren der Dateisperre.
   > - Möglicherweise gibt es einen Fall, in dem ein Ordner und ein Objekt in einem Amazon S3 S3-Bucket existieren und denselben Namen haben. In diesem Fall ist, wenn der

Objektname keinen abschließenden Schrägstrich enthält, nur der Ordner in einem File Gateway sichtbar. Wenn ein Bucket beispielsweise ein Objekt mit dem Namen `test` oder `test/` und einen Ordner mit dem Namen enthält`test/test1`, `test/test1` sind diese nur `test/` in einem File Gateway sichtbar.

- Möglicherweise müssen Sie die Dateifreigabe nach einem Client-Neustart erneut mounten.
- 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]

Mounten Sie Ihre SMB-Dateifreigabe auf Ihrem Client

Gehen Sie wie folgt vor, um Ihre SMB-Dateifreigabe bereitzustellen und sie einem Laufwerk zuzuordnen, auf das Ihr Client zugreifen kann. Im Bereich File Gateway der Konsole werden die unterstützten Mount-Befehle aufgeführt, die Sie für SMB-Clients verwenden können. 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`) — Verwenden Sie die Befehlszeile, um Ihre Dateifreigabe zu mounten. Speichern Sie Ihre Anmeldeinformationen mit `cmdkey` und mounten Sie dann das Laufwerk mit den `/savecred` Schaltern `net use /persistent:yes` und schließen Sie sie ein, wenn Sie möchten, dass die Verbindung auch nach Systemneustarts bestehen bleibt. Die spezifischen Befehle, die Sie verwenden, unterscheiden sich je nachdem, ob Sie das Laufwerk für den Zugriff auf Microsoft Active Directory (AD) oder für den Gastbenutzerzugriff bereitstellen möchten. Im Folgenden finden Sie Beispiele.
- Datei-Explorer (Map Network Drive) — Verwenden Sie den Windows-Datei-Explorer, um Ihre Dateifreigabe zu mounten. Konfigurieren Sie die Einstellungen, um anzugeben, ob die

Verbindung auch nach Systemneustarts bestehen bleiben soll und Sie zur Eingabe von Netzwerkanmeldeinformationen aufgefordert werden sollen.

- PowerShell script — Erstellen Sie ein benutzerdefiniertes PowerShell Skript, um Ihre Dateifreigabe zu mounten. Abhängig von den Parametern, die Sie im Skript angeben, kann die Verbindung auch nach Systemneustarts bestehen, und die Freigabe kann für das Betriebssystem entweder sichtbar oder unsichtbar sein, während sie 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 Gastbenutzerpasswort haben, bevor Sie versuchen, die Dateifreigabe bereitzustellen.

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

1. Stellen Sie sicher, dass der Microsoft AD-Benutzer über die erforderlichen Berechtigungen für die SMB-Dateifreigabe verfügt, bevor Sie die Dateifreigabe in das System des Benutzers einbinden.
2. Geben Sie in der Befehlszeile Folgendes ein, um die Dateifreigabe bereitzustellen:

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

So mounten Sie Ihre SMB-Dateifreigabe mit einer bestimmten Kombination von Anmeldeinformationen mithilfe der Befehlszeile:

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

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

3. Geben Sie an der Befehlszeile Folgendes ein, um die Dateifreigabe bereitzustellen:

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

So mounten Sie Ihre SMB-Dateifreigabe für Gastbenutzer mithilfe der Befehlszeile:

1. Stellen Sie sicher, dass Sie das Gastbenutzerpasswort haben, bevor Sie die Dateifreigabe bereitstellen.
2. Geben Sie an der Befehlszeile Folgendes ein, um die Gastanmeldedaten 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:$Gateway
   ID\smbguest /persistent:yes /savecred
   ```

> **Note**
>
> Beachten Sie beim Mounten von Dateifreigaben Folgendes:
>
> - Möglicherweise gibt es einen Fall, in dem ein Ordner und ein Objekt in einem Amazon S3 S3-Bucket existieren und denselben Namen haben. In diesem Fall ist, wenn der Objektname keinen abschließenden Schrägstrich enthält, nur der Ordner in einem File Gateway sichtbar. Wenn ein Bucket beispielsweise ein Objekt mit dem Namen `test` oder `test/` und einen Ordner mit dem Namen enthält`test/test1`, `test/test1` sind diese nur `test/` in einem File Gateway sichtbar.
> - Sofern Sie Ihre Dateifreigabeverbindung nicht so konfigurieren, dass Ihre Benutzeranmeldedaten gespeichert und auch nach Systemneustarts erhalten bleiben, müssen Sie Ihre Dateifreigabe möglicherweise bei jedem Neustart Ihres Clientsystems erneut bereitstellen.

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 Dieser PC aus. Wählen Sie dann auf der Registerkarte Computer die Option Netzlaufwerk zuordnen aus.
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.

> **Note**
>
> Alle Dateien oder Verzeichnisse, die mit einem Punkt (`.`) beginnen, werden in Windows als versteckt markiert. Um diese Dateien und Verzeichnisse sichtbar zu machen, müssen Sie im Windows-Datei-Explorer auf der Registerkarte Ansicht das Kontrollkästchen Versteckte Objekte aktivieren.

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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
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 allowed/denied Benutzer bearbeiten, um Benutzer und Gruppen hinzuzufügen oder zu löschen, und geben Sie dann die erlaubten und verweigerten Benutzer und Gruppen in die Felder Zulässige Benutzer, Abgelehnte Benutzer, Zulässige Gruppen und 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.

> **Note**
>
> Gruppen muss das `@` Zeichen vorangestellt werden. Zulässige Formate sind: `DOMAIN \User1user1,@group1`, und`@DOMAIN\group1`.

5. Wenn Sie fertig sind, wählen Sie Speichern.

   Wenn Sie zugelassene Benutzer und Gruppen eingeben, erstellen Sie eine Zulassungsliste. Ohne eine Zulassungsliste können alle authentifizierten Microsoft AD-Benutzer auf die SMB-Dateifreigabe zugreifen. Alle Benutzer und Gruppen, die als verweigert markiert sind, werden einer Sperrliste hinzugefügt und können nicht auf die SMB-Dateifreigabe zugreifen. In Fällen, in denen ein Benutzer oder eine Gruppe sowohl auf der Verweigerungsliste als auch auf der Zulassungsliste steht, hat die Verweigerungsliste Vorrang.

   Sie können die Zugriffskontrolllisten (ACLs) auf Ihrer SMB-Dateifreigabe aktivieren. Informationen zum Aktivieren finden Sie ACLs unterVerwendung von Windows-ACLs zur Beschränkung des SMB-Dateifreigabezugriffs.

Nächster Schritt

Testen Sie Ihr S3 File Gateway

Verwenden von Dateifreigaben für Buckets mit bereits vorhandenen Objekten

Sie können eine Dateifreigabe in einem Amazon S3 S3-Bucket mit Objekten exportieren, 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 Sie 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 des Amazon S3 S3-Bucket-Objekt-Caches”.

> **Note**
>
> Wir empfehlen nicht, mehrere Writer für einen Amazon S3 S3-Bucket zu haben. Lesen Sie in diesem Fall unbedingt den Abschnitt „Kann ich mehrere Autoren für meinen Amazon S3 S3-Bucket verwenden?“ in den häufig gestellten Fragen zu Storage Gateway.

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

Für SMB können Sie eine Freigabe mit Microsoft AD oder Gastzugriff für einen Amazon S3 S3-Bucket mit bereits 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

Verwenden Sie das folgende Verfahren, um Ihr Gateway zu testen, indem Sie Dateien und Ordner auf Ihr zugeordnetes Laufwerk kopieren und überprüfen, ob sie automatisch in Ihrem Amazon S3 S3-Bucket erscheinen.

Um Dateien von Ihrem Windows-Client auf Amazon S3 hochzuladen

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 S3-Managementkonsole zu Ihrem zugewiesenen Bucket. Sie sollten die Dateien und Ordner sehen, die Sie in den von Ihnen angegebenen Amazon S3 S3-Bucket kopiert haben.

   Sie können die von Ihnen erstellte Dateifreigabe auf der Registerkarte Dateifreigaben in der AWS Storage Gateway Management Console sehen.

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

> **Note**
>
> File Gateways unterstützen das Erstellen von festen oder symbolischen Links auf einer Dateifreigabe nicht.

Beachten Sie die folgenden Punkte zur 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 in S3 als Ordnerobjekte verwaltet, wobei dieselbe Syntax wie in der Amazon S3 S3-Konsole verwendet wird. Sie können leere Verzeichnisse umbenennen.
- Die rekursive Dateisystem-Operationsleistung (z. B. `ls -l`) hängt von der Anzahl der Objekte in Ihrem Bucket ab.

Verwaltung Ihres Amazon S3 File Gateway

Die Themen in diesem Abschnitt enthalten Informationen zur Verwaltung Ihrer Amazon S3 File Gateway-Ressourcen. Das Gateway-Management umfasst die Erteilung von Zugriffsberechtigungen für Ihr Gateway auf Dateifreigaben und Amazon S3 S3-Buckets, die Bearbeitung von Informationen und Einstellungen für Gateways und Dateifreigaben, das Löschen von Dateifreigaben, das Aktualisieren zwischengespeicherter Objekte und das Verständnis von Betriebsstatusindikatoren für Gateways und Dateifreigaben.

Topics

- Bearbeiten Sie grundlegende Gateway-Informationen- Erfahren Sie, wie Sie die Storage Gateway Gateway-Konsole verwenden, um grundlegende Informationen für ein vorhandenes Gateway zu bearbeiten, darunter den Gateway-Namen, die Zeitzone und die CloudWatch Protokollgruppe.
- Zugriff und Berechtigungen gewähren- Erfahren Sie, wie Sie mithilfe von IAM-Rollen Ihrem Gateway Zugriffsberechtigungen für Amazon S3 S3-Buckets und Amazon VPC-Endpunkte gewähren, bestimmte Sicherheitsprobleme verhindern und Dateifreigaben kontenübergreifend mit Buckets verbinden können. AWS
- Löschen Sie eine Dateifreigabe- Erfahren Sie, wie Sie eine Dateifreigabe mithilfe der Storage Gateway Gateway-Konsole löschen.
- SMB-Einstellungen des Gateways bearbeiten- Erfahren Sie, wie Sie SMB-Einstellungen auf Gateway-Ebene bearbeiten, die die Sicherheitsstrategie, die Active Directory-Authentifizierung, den Gastzugriff, lokale Gruppenberechtigungen und die Sichtbarkeit von Dateifreigaben für SMB-Dateifreigaben auf einem Gateway steuern.
- Bearbeiten Sie die Einstellungen für die SMB-Dateifreigabe- Erfahren Sie, wie Sie Einstellungen bearbeiten, um Name, Protokollierung, Cacheaktualisierung, Speicherklasse, Dateiexport und mehr für eine SMB-Dateifreigabe zu konfigurieren.
- Beschränken Sie den SMB-Dateifreigabezugriff- Erfahren Sie, wie Sie zugelassene oder verweigerte Benutzer oder Gruppen hinzufügen, um den Zugriff auf Ihre SMB-Dateifreigabe einzuschränken.
- Bearbeiten Sie die Einstellungen für die NFS-Dateifreigabe- Erfahren Sie, wie Sie Einstellungen bearbeiten, um Name, Protokollierung, Cache-Aktualisierung, Speicherklasse, Dateiexport und mehr für eine NFS-Dateifreigabe zu konfigurieren.

- Bearbeiten Sie die Standardeinstellungen für die NFS-Dateifreigabe- Erfahren Sie, wie Sie Standard-Metadatenwerte bearbeiten, die Unix-Berechtigungen für Dateien und Ordner auf NFS-Dateifreigaben beinhalten.
- Beschränken Sie den Zugriff auf NFS-Dateifreigaben- Erfahren Sie, wie Sie den Zugriff auf Clients von bestimmten IP-Adressen oder IP-Bereichen für Ihren NFS-Fileshare einschränken können.
- Aktualisieren des Amazon S3 S3-Bucket-Objekt-Caches- Erfahren Sie, wie Sie den S3-Bucket-Objekt-Cache für eine Dateifreigabe aktualisieren und einen Zeitplan für die automatische Aktualisierung des Caches konfigurieren.
- Verwenden der S3-Objektsperre- Erfahren Sie, wie Amazon S3 File Gateway mit der S3 Object Lock-Funktion funktioniert.
- Status der Dateifreigabe- Erfahren Sie, wie Sie den Dateifreigabestatus anzeigen und interpretieren können.
- Gateway-Status- Erfahren Sie, wie Sie den Gateway-Status anzeigen und interpretieren können.
- Verwaltung der Bandbreite für Ihr Amazon S3 File Gateway- Erfahren Sie, wie Sie den Upload-Durchsatz von Ihrem Gateway begrenzen AWS können, um die vom Gateway verwendete Netzwerkbandbreite zu kontrollieren.

Bearbeiten Sie grundlegende Informationen für ein S3 File Gateway

Sie können die Storage Gateway Gateway-Konsole verwenden, um grundlegende Informationen für ein vorhandenes Gateway zu bearbeiten, einschließlich des Gateway-Namens, der Zeitzone und der CloudWatch Protokollgruppe.

So bearbeiten Sie grundlegende Informationen für ein vorhandenes Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend das Gateway aus, für das Sie grundlegende Informationen bearbeiten möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option Gateway-Informationen bearbeiten aus.
4. Geben Sie in Gateway-Name einen Namen für Ihren Gateway ein. Sie können nach diesem Namen suchen, um Ihr Gateway auf den Listenseiten in der Storage Gateway Gateway-Konsole zu finden.

> **Note**
>
> Gateway-Namen müssen zwischen 2 und 255 Zeichen lang sein und dürfen keinen Schrägstrich (\oder/) enthalten.
> Wenn Sie den Namen eines Gateways ändern, werden alle CloudWatch Alarme, die zur Überwachung des Gateways eingerichtet wurden, deaktiviert. Um die Alarme wieder zu verbinden, aktualisieren Sie die GatewayNamefür jeden Alarm in der CloudWatch Konsole.

5. Wählen Sie Gateway-Zeitzone die lokale Zeitzone für den Teil der Welt aus, in dem Sie Ihr Gateway einsetzen möchten.
6. Wählen Sie unter Wählen Sie, wie Sie die Protokollgruppe einrichten möchten, aus, wie Amazon CloudWatch Logs eingerichtet werden soll, um den Zustand Ihres Gateways zu überwachen. Sie können aus den folgenden Optionen wählen:

   - Eine neue Protokollgruppe erstellen — Richten Sie eine neue Protokollgruppe ein, um Ihr Gateway zu überwachen.
   - Eine bestehende Protokollgruppe verwenden — Wählen Sie eine bestehende Protokollgruppe aus der entsprechenden Dropdownliste aus.
   - Protokollierung deaktivieren — Verwenden Sie Amazon CloudWatch Logs nicht zur Überwachung Ihres Gateways.
7. Wenn Sie mit der Änderung der Einstellungen, die Sie ändern möchten, fertig sind, wählen Sie Änderungen speichern.

Gewährung von Zugriff und Berechtigungen für Fileshares und Buckets

Nachdem Ihr S3 File Gateway aktiviert ist und läuft, können Sie weitere Dateifreigaben hinzufügen und Zugriff auf Amazon S3 S3-Buckets gewähren, einschließlich Buckets, die sich von Ihren Gateways und Dateifreigaben unterscheiden AWS-Konten . In den folgenden Abschnitten wird beschrieben, wie Sie mithilfe von IAM-Rollen Ihrem Gateway Zugriffsberechtigungen für Amazon S3 S3-Buckets und VPC-Endpunkte gewähren, bestimmte Sicherheitsprobleme verhindern und Dateifreigaben mit Buckets verbinden können. AWS-Konten

Informationen zum Erstellen einer neuen Dateifreigabe finden Sie unter. Erstellen einer Dateifreigabe

Dieser Abschnitt enthält die folgenden Themen, die zusätzliche Informationen darüber enthalten, wie Sie Zugriff und Berechtigungen für Dateifreigaben und Amazon S3 S3-Buckets gewähren können:

Topics

- Zugriff auf einen Amazon S3 S3-Bucket gewähren- Erfahren Sie, wie Sie Ihrem File Gateway Zugriff gewähren, um Dateien in Ihren Amazon S3 S3-Bucket hochzuladen und Aktionen an allen Access Points oder Amazon Virtual Private Cloud (Amazon VPC) -Endpunkten durchzuführen, die es für die Verbindung mit dem Bucket verwendet.
- Serviceübergreifende Confused-Deputy-Prävention- Erfahren Sie, wie Sie ein häufig auftretendes Sicherheitsproblem verhindern können, bei dem eine Entität, die nicht zur Ausführung einer Aktion berechtigt ist, eine Entität mit mehr Rechten dazu zwingen kann, die Aktion auszuführen.
- Verwenden einer Dateifreigabe für kontoübergreifenden Zugriff- Erfahren Sie, wie Sie Zugriff für ein Amazon Web Services Services-Konto gewähren und Benutzern dieses Kontos Zugriff auf Ressourcen gewähren, die zu einem anderen Amazon Web Services Services-Konto gehören.

Zugriff auf einen Amazon S3 S3-Bucket gewähren

Wenn Sie eine Dateifreigabe erstellen, benötigt Ihr File Gateway Zugriff, um Dateien in Ihren Amazon S3 S3-Bucket hochzuladen und Aktionen auf allen Access Points oder Virtual Private Cloud (VPC) -Endpunkten auszuführen, die es für die Verbindung mit dem Bucket verwendet. Um diesen Zugriff zu gewähren, nimmt Ihr File Gateway eine AWS Identity and Access Management (IAM) -Rolle an, 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 Ihr S3-Bucket und alle zugehörigen Access Points oder VPC-Endpoints über eine Zugriffsrichtlinie verfügen, die der IAM-Rolle den Zugriff darauf ermöglicht.

Sie können die Rolle und die Zugriffsrichtlinie selbst erstellen, oder Ihr File Gateway kann sie für Sie erstellen. Wenn Ihr File Gateway die Richtlinie für Sie erstellt, enthält die Richtlinie eine Liste von S3-Aktionen. Informationen zu Rollen und Berechtigungen finden Sie im IAM-Benutzerhandbuch unter Eine Rolle erstellen, um Berechtigungen AWS-Service an eine zu delegieren.

Das folgende Beispiel ist eine Vertrauensrichtlinie, die es Ihrem File Gateway ermöglicht, eine IAM-Rolle anzunehmen.

JSON

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

Important

Storage Gateway kann bestehende Servicerollen übernehmen, die mithilfe der `iam:PassRole` Richtlinienaktion übergeben werden, unterstützt jedoch keine IAM-Richtlinien, die den `iam:PassedToService` Kontextschlüssel verwenden, um die Aktion auf bestimmte Dienste zu beschränken.
Weitere Informationen finden Sie in folgenden Themen im AWS Identity and Access Management -Benutzerhandbuch:

- IAM: Übergibt eine IAM-Rolle an einen bestimmten Dienst AWS
- Einem Benutzer Berechtigungen zur Übergabe einer Rolle an einen Dienst gewähren AWS
- Verfügbare Schlüssel für IAM

Wenn Sie nicht möchten, dass Ihr File Gateway in Ihrem Namen eine Richtlinie erstellt, können Sie Ihre eigene Richtlinie erstellen und sie an Ihre Dateifreigabe anhängen. Weitere Information dazu finden Sie unter Erstellen einer Dateifreigabe.

Die folgende Beispielrichtlinie ermöglicht es Ihrem File Gateway, alle in der Richtlinie aufgeführten Amazon S3 S3-Aktionen durchzuführen. Der erste Teil der Anweisung definiert, dass alle aufgeführten Aktionen auf den S3-Bucket `amzn-s3-demo-bucket` angewendet werden dürfen. Der

zweite Teil legt fest, dass die aufgeführten Aktionen auf alle Objekte in `amzn-s3-demo-bucket` angewendet werden dürfen.

JSON

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

Die folgende Beispielrichtlinie ähnelt der vorherigen, ermöglicht Ihrem File Gateway jedoch die Durchführung von Aktionen, die für den Zugriff auf einen Bucket über einen Zugriffspunkt erforderlich sind.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Wenn Sie Ihre Dateifreigabe über einen VPC-Endpunkt mit einem S3-Bucket verbinden müssen, finden Sie weitere Informationen unter Endpunktrichtlinien für Amazon S3 im AWS PrivateLink Benutzerhandbuch.

> **Note**
>
> Für verschlüsselte Buckets muss das Fileshare den Schlüssel im Ziel-S3-Bucket-Konto verwenden.

> **Note**
>
> Wenn Ihr File Gateway SSE-KMS oder DSSE-KMS für die Verschlüsselung verwendet, stellen Sie sicher, dass die der Dateifreigabe zugeordnete IAM-Rolle die Berechtigungen kms:encrypt, kms:Decrypt, kms: *, kms: und kms: umfasst. ReEncrypt GenerateDataKey DescribeKey Weitere Informationen finden Sie unter Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für Storage Gateway.

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zum Problem des verwirrten Stellvertreters führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). 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 Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS Storage Gateway Ressource einen anderen Dienst gewähren. 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 Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:servicename::123456789012:*`.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Storage Gateway verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Sid": "ConfusedDeputyPreventionExamplePolicy",
       "Effect": "Allow",
       "Principal": {
         "Service": "storagegateway.amazonaws.com"
       },
       "Action": "sts:AssumeRole",
       "Condition": {
         "StringEquals": {
           "aws:SourceAccount": "444455556666"
         },
         "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-
east-1:444455556666:gateway/sgw-123456DA"
        }
      }
    }
  ]
}
```

Verwenden einer Dateifreigabe für kontoübergreifenden Zugriff

Kontoübergreifender Zugriff liegt vor, wenn einem Amazon Web Services Services-Konto und Benutzern dieses Kontos Zugriff auf Ressourcen gewährt wird, die zu einem anderen Amazon Web Services Services-Konto gehören. Mit 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, die einem Amazon Web Services Services-Konto gehört, 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, auf den Sie zugreifen müssen, und auf die Objekte in diesem Bucket gewährt hat. Informationen zur Gewährung dieses Zugriffs finden Sie unter Beispiel 2: Bucket-Besitzer, der kontoübergreifende Bucket-Berechtigungen gewährt im Amazon Simple Storage Service-Benutzerhandbuch. Eine Liste der erforderlichen Berechtigungen finden Sie unter Zugriff auf einen Amazon S3 S3-Bucket gewähren.
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 Zugriff auf einen Amazon S3 S3-Bucket gewähren.

   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 Zugriff auf einen Amazon S3 S3-Bucket gewähren.
3. Wählen Sie Gateway-Dateien, auf die der Besitzer des S3-Buckets zugreifen kann, wenn Sie Ihre Dateifreigabe erstellen oder die Dateifreigabeeinstellungen im Home bearbeiten. https://console.aws.amazon.com/storagegateway/

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 von Dateien über Ihre lokalen Anwendungen nicht an den Amazon S3 S3-Bucket weitergegeben, mit dem Sie arbeiten.

Ressourcen

Weitere Informationen zu Zugriffsrichtlinien und Zugriffskontrolllisten finden Sie unter:

Richtlinien für die Verwendung der verfügbaren Zugriffsrichtlinienoptionen im Amazon Simple Storage Service-Benutzerhandbuch

Übersicht über Zugriffssteuerungsliste (ACL) im Benutzerhandbuch für Amazon Simple Storage Service

Löschen Sie eine Dateifreigabe

Wenn Sie eine Dateifreigabe nicht mehr benötigen, können Sie sie aus der Storage Gateway Gateway-Konsole löschen. Wenn Sie eine Dateifreigabe löschen, wird das Gateway von dem Amazon S3 S3-Bucket getrennt, dem die Dateifreigabe zugeordnet ist. 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 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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Dateifreigaben und anschließend eine oder mehrere Dateifreigaben zum Löschen aus.
3. Klicken Sie bei Actions (Aktionen) auf Delete file share (Dateifreigabe löschen). Das Bestätigungsdialogfeld wird angezeigt.
4. Vergewissern Sie sich, dass Sie die angegebenen Dateifreigaben löschen möchten, geben Sie dann das Wort Löschen in das Bestätigungsfeld ein und wählen Sie 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. Beispielsweise möchten Sie möglicherweise absichtlich Daten verwerfen, die geschrieben, aber noch nicht hochgeladen wurden, oder der Amazon S3 S3-Bucket, der die Dateifreigabe unterstützt, wurde möglicherweise bereits gelöscht, sodass das Hochladen der angegebenen Daten nicht mehr möglich ist.

In diesen Fällen können Sie das Löschen der Dateifreigabe erzwingen, indem Sie die API-Operation AWS-Managementkonsole oder verwenden. `DeleteFileShare` Durch diesen Vorgang wird der Datenupload gestoppt. Wenn dies der Fall ist, geht die Dateifreigabe in den Status FORCE_DELETING über. Gehen Sie wie folgt vor, um das Löschen einer Dateifreigabe mithilfe der Storage Gateway Gateway-Konsole zu erzwingen.

So erzwingen Sie die eine Dateifreigabe

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie auf der Seite mit der Liste der Dateifreigaben die Dateifreigabe aus, die Sie im obigen Verfahren zum Löschen markiert haben, um deren Details anzuzeigen. Nach einigen Sekunden wird auf der Registerkarte „Details“ eine Benachrichtigung über den Löschvorgang angezeigt.
3. Überprüfen Sie in der Meldung, die auf der Registerkarte Details angezeigt wird, die ID der Dateifreigabe, die Sie gewaltsam löschen möchten, aktivieren Sie das Bestätigungsfeld und wählen Sie Löschen jetzt erzwingen aus.

> **Note**
>
> Sie können die Löschoperation nicht rückgängig machen.
> Wenn Sie eine Dateifreigabe gewaltsam löschen, verbleiben Teile teilweise übertragener Dateien aus mehrteiligen Uploads möglicherweise auf Amazon S3, wo Speichergebühren anfallen können. Wir empfehlen, eine Amazon S3 S3-Bucket-Lebenszyklusregel zu konfigurieren, um diese Dateibestandteile automatisch zu löschen. Weitere Informationen finden Sie unter Bewährte Methoden: Verwaltung mehrteiliger Uploads.

Sie können den DeleteFileShareAPI-Vorgang auch verwenden, um das Löschen der Dateifreigabe zu erzwingen. Für das Löschen einer Dateifreigabe mithilfe der API ist die `storagegateway:DeleteFileShare` IAM-Richtlinienberechtigung erforderlich.

SMB-Einstellungen für ein Gateway bearbeiten

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

Um SMB-Einstellungen auf Gateway-Ebene zu bearbeiten

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option SMB-Einstellungen bearbeiten aus und wählen Sie dann die Einstellungen aus, die Sie bearbeiten möchten.

Dieser Abschnitt enthält die folgenden Themen, die zusätzliche Informationen und Verfahren zur Konfiguration der einzelnen SMB-Einstellungen für Ihr Gateway enthalten.

Topics

- Legen Sie die Gateway-Sicherheitsstufe fest- Erfahren Sie, wie Sie eine Sicherheitsstufe festlegen, um Verbindungsanforderungen wie SMB-Signierung und Verschlüsselung (Server Message Block) festzulegen und ob Verbindungen von SMB-Clients, Version 1, zugelassen werden sollen.
- Konfigurieren Sie die Active Directory-Authentifizierung- Erfahren Sie, wie Sie Ihr Unternehmens-Active Directory oder AWS Managed Microsoft AD für den benutzerauthentifizierten Zugriff auf Ihre SMB-Dateifreigabe konfigurieren.
- Bieten Sie Gastzugriff- Erfahren Sie, wie Sie Ihr Gateway so konfigurieren, dass jedem Benutzer, der den richtigen Benutzernamen und das richtige Passwort für das Gastkonto angegeben hat, Gastzugriff gewährt wird.
- Konfigurieren Sie lokale Gruppen- Erfahren Sie, wie Sie lokale Gruppen konfigurieren, um Active Directory-Benutzern spezielle Dateifreigabeberechtigungen zu gewähren.
- Legen Sie die Sichtbarkeit der Dateifreigabe fest- Erfahren Sie, wie Sie angeben, ob die Shares auf einem Gateway sichtbar sind, wenn Shares für Benutzer aufgelistet werden.

Legen Sie eine Sicherheitsstufe für Ihr Gateway fest

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

So konfigurieren Sie die Sicherheitsstufe

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option SMB-Einstellungen bearbeiten und anschließend SMB-Sicherheitseinstellungen aus.
4. Wählen Sie für Security level (Sicherheitsstufe) eine der folgenden Optionen aus:

> **Note**
>
> Informationen zur Konfiguration dieser Einstellung mithilfe der AWS API finden Sie unter SMBSecurityStrategie aktualisieren in der AWS Storage Gateway API-Referenz. Eine höhere Sicherheitsstrategieebene kann sich auf die Leistung des Gateways auswirken.

- AES256 Verschlüsselung erzwingen — Wenn Sie diese Option wählen, lässt S3 File Gateway nur Verbindungen von SMBv3 Clients zu, die 256-Bit-AES-Verschlüsselungsalgorithmen verwenden. 128-Bit-Algorithmen sind nicht zulässig. Diese Option wird für Umgebungen empfohlen, in denen sensible Daten verarbeitet werden. Es funktioniert mit allen aktuellen SMB-Clients unter Microsoft Windows.
- Verschlüsselung erzwingen — Wenn Sie diese Option wählen, erlaubt S3 File Gateway nur Verbindungen von SMBv3 Clients, auf denen die Verschlüsselung aktiviert ist. Sowohl 256-Bit- als auch 128-Bit-Algorithmen sind zulässig. Diese Option wird für Umgebungen empfohlen, in denen sensible Daten verarbeitet werden. Es funktioniert mit allen aktuellen SMB-Clients unter Microsoft Windows.

- Signierung erzwingen — Wenn Sie diese Option wählen, erlaubt S3 File Gateway nur Verbindungen von SMBv2 oder SMBv3 Clients, auf denen die Signatur aktiviert ist. Diese Option funktioniert mit allen aktuellen SMB-Clients unter Microsoft Windows.
- Vom Kunden ausgehandelt — Wenn Sie diese Option wählen, werden Anfragen auf der Grundlage dessen eingerichtet, was vom Kunden ausgehandelt wurde. 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 Speichern.

Verwenden Sie Active Directory, um Benutzer zu authentifizieren

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

> **Note**
>
> Mithilfe Directory Service können Sie einen gehosteten Active Directory-Domänendienst in der erstellen. AWS Cloud
> Für die Verwendung AWS Managed Microsoft AD mit einem Amazon EC2 EC2-Gateway müssen Sie die Amazon EC2 EC2-Instance in derselben VPC wie die erstellen AWS Managed Microsoft AD, die Sicherheitsgruppe _WorkspaceMembers zur Amazon EC2 EC2-Instance hinzufügen und der AD-Domain mit den Administratoranmeldedaten von beitreten. AWS Managed Microsoft AD
> Weitere Informationen zu finden Sie im Administratorhandbuch. AWS Managed Microsoft ADAWS Directory Service

Weitere Informationen zu Amazon EC2 finden Sie in der Amazon Elastic Compute Cloud-Dokumentation.

Sie können auch Zugriffskontrolllisten (ACLs) auf Ihrer SMB-Dateifreigabe aktivieren. Informationen zur Aktivierung finden Sie ACLs unterVerwendung von Windows-ACLs zur Beschränkung des SMB-Dateifreigabezugriffs.

So aktivieren Sie die Active Directory-Authentifizierung

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option SMB-Einstellungen bearbeiten und anschließend Active Directory-Einstellungen aus.
4. Geben Sie als Domänenname den Namen der Active Directory-Domäne ein, der Ihr Gateway beitreten soll.

> **Note**
>
> Für Active Directory status (Active Directory-Status) wird Detached (Getrennt) angezeigt, wenn ein Gateway noch nie einer Domäne beigetreten ist.
> Ihr Active Directory-Dienstkonto muss über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter Berechtigungsanforderungen für Active Directory-Dienstkonten Berechtigungsanforderungen für .
> Durch den Beitritt zu einer Domäne wird ein Active Directory-Computerkonto im Standardcomputercontainer (der keine Organisationseinheit ist) erstellt, wobei die Gateway-ID des Gateways als Kontoname verwendet wird (z. B. SGW-1234ADE). Es ist nicht möglich, den Namen dieses Kontos anzupassen.
> Wenn Ihre Active Directory-Umgebung erfordert, dass Sie Konten vorab bereitstellen, um den Domänenbeitritt zu erleichtern, müssen Sie dieses Konto im Voraus erstellen.
> Wenn Ihre Active Directory-Umgebung über eine festgelegte Organisationseinheit für neue Computerobjekte verfügt, müssen Sie diese Organisationseinheit angeben, wenn Sie der Domäne beitreten.

Wenn Ihr Gateway einem Active Directory-Verzeichnis nicht beitreten kann, versuchen Sie, mithilfe der JoinDomainAPI-Operation eine Verbindung mit der IP-Adresse des Verzeichnisses herzustellen.

5. Geben Sie für Domänenbenutzer und Domänenkennwort die Anmeldeinformationen für das Active Directory-Dienstkonto ein, mit dem das Gateway der Domäne beitritt.
6. (Optional) Geben Sie unter Organisationseinheit (OU) die angegebene Organisationseinheit ein, die Ihr Active Directory für neue Computerobjekte verwendet.
7. (Optional) Geben Sie für Domänencontroller (DC) den Namen eines oder mehrerer Controller ein, DCs über die Ihr Gateway eine Verbindung zu Active Directory herstellt. Sie können mehrere DCs als kommagetrennte Liste eingeben. Sie können dieses Feld leer lassen, damit DNS automatisch einen DC auswählt.
8. Wählen Sie Änderungen speichern aus.

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. Wählen Sie im Dropdownmenü Aktionen die Option Einstellungen für den Dateifreigabezugriff bearbeiten aus.
3. Wählen Sie im Abschnitt Dateifreigabezugriff für Benutzer und Gruppen Ihre Einstellungen aus.

   Wählen Sie für Zulässige Benutzer und Gruppen die Option Zulässigen Benutzer hinzufügen oder Zulässige Gruppe hinzufügen aus und geben Sie einen AD-Benutzer oder eine AD-Gruppe ein, dem/der Sie Fileshare-Zugriff gewähren möchten. Wiederholen Sie diesen Vorgang, um so viele Benutzer und Gruppen wie nötig zuzulassen.

   Wählen Sie für Verweigerte Benutzer und Gruppen die Option Abgelehnten Benutzer hinzufügen oder Verweigerte Gruppe hinzufügen aus und geben Sie einen AD-Benutzer oder eine AD-Gruppe ein, dem/der Sie den Dateifreigabezugriff verweigern möchten. Wiederholen Sie diesen Vorgang, um so vielen Benutzern und Gruppen wie nötig den Zugriff zu verweigern.

   Note

   Der Abschnitt Dateifreigabezugriff für Benutzer und Gruppen wird nur angezeigt, wenn Active Directory ausgewählt ist.

Gruppen muss das @ Zeichen vorangestellt werden. Zulässige Formate sind: `DOMAIN\User1`user1,`@group1`, und`@DOMAIN\group1`.
Wenn Sie Listen mit erlaubten und abgelehnten Benutzern und Gruppen konfigurieren, gewährt Windows ACLs keinen Zugriff, der diese Listen außer Kraft setzt.
Die Listen „Zulässige“ und „Abgelehnte Benutzer“ und „Gruppen“ werden zuvor ausgewertet und legen fest ACLs, welche Benutzer die Dateifreigabe bereitstellen oder darauf zugreifen können. Wenn Benutzer oder Gruppen in die Liste der zugelassenen Benutzer oder Gruppen aufgenommen werden, gilt die Liste als aktiv, und nur diese Benutzer können die Dateifreigabe bereitstellen.
Nachdem ein Benutzer eine Dateifreigabe bereitgestellt hat, bieten ACLs Sie einen detaillierteren Schutz, der steuert, auf welche spezifischen Dateien oder Ordner der Benutzer zugreifen kann. Weitere Informationen finden Sie unter Windows ACLs auf einer neuen SMB-Dateifreigabe aktivieren.

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

Ermöglichen Sie Gastzugriff auf Ihre Dateifreigabe

Sie können Ihr S3 File Gateway so konfigurieren, dass jeder Benutzer, der den richtigen Benutzernamen und das richtige Passwort für das Gastkonto angeben kann, den Gastzugriff gewährt. Wenn Sie möchten, dass dies die einzige Methode ist, mit der Benutzer auf Ihr File-Gateway zugreifen können, müssen Sie das Gateway nicht mit einer Microsoft Active Directory-Domäne verbinden. Sie können diese Gastzugriffsmethode auch verwenden, um Dateifreigaben auf einem S3-Dateigateway zu erstellen, das Mitglied einer Active Directory-Domäne ist.

Wenn Sie eine Dateifreigabe für die Verwendung der Authentifizierungsmethode Gastzugriff konfigurieren, lautet der Gastzugriffsbenutzername`smbguest`. Bevor Sie eine Dateifreigabe mithilfe des Gastzugriffs erstellen können, müssen Sie das Standardkennwort für den `smbguest` Benutzer ändern.

Sie können das folgende Verfahren verwenden, um das Passwort für den Gastbenutzer zu ändern`smbguest`.

So ändern Sie das Passwort für den Gastzugriff

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.

2. Wählen Sie im Navigationsbereich auf der linken Seite der Konsolenseite die Option Gateways aus und wählen Sie dann den Namen des Gateways, für das Sie Gastzugriff gewähren möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option SMB-Einstellungen bearbeiten und dann Gastzugriffseinstellungen aus.
4. Geben Sie unter Gastpasswort das Gastzugriffspasswort ein, das Sie einrichten möchten, und wählen Sie dann Änderungen speichern aus.

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 gewähren.

Sie können die Einstellungen für lokale Gruppen verwenden, um Gateway-Administratorberechtigungen zuzuweisen. Gateway-Administratoren können das Microsoft Management Console-Snap-In für gemeinsame Ordner verwenden, um das Schließen geöffneter und gesperrter Dateien zu erzwingen.

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

Um Gateway-Administratoren zuzuweisen

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Wählen Sie im Dropdownmenü „Aktionen“ die Option „SMB-Einstellungen bearbeiten“ und anschließend „Lokale Gruppeneinstellungen“ aus.
4. Wählen Sie im Bereich Einstellungen für lokale Gruppen Ihre Einstellungen aus. Dieser Abschnitt wird nur für Dateifreigaben angezeigt, die Active Directory verwenden.

   Fügen Sie für Gateway-Administratoren Active Directory-Benutzer und -Gruppen hinzu, denen Sie lokale Gateway-Administratorberechtigungen gewähren möchten. Fügen Sie einen Benutzer

oder eine Gruppe pro Zeile hinzu, einschließlich des Domänennamens. Beispiel, **`corp\Domain Admins`**. Um zusätzliche Zeilen zu erstellen, wählen Sie Neuen Gateway-Admin hinzufügen.

> **Note**
>
> Beim Bearbeiten von Gateway-Admins werden alle SMB-Dateifreigaben getrennt und erneut verbunden.

5. Wählen Sie Änderungen speichern und anschließend Weiter, um die angezeigte Warnmeldung zu bestätigen.

Legen Sie die Sichtbarkeit der Dateifreigabe fest

Die Sichtbarkeit von Dateifreigaben steuert, ob die Freigaben auf einem Gateway sichtbar sind, wenn Shares für Benutzer aufgelistet werden, z. B. in einer Netzansicht oder in einer Suchliste. Wenn die Dateifreigaben auf einem Gateway sichtbar sind, können Clients die Shares mit einem Dateibrowser leicht finden, sofern sie die Gateway-IP-Adresse oder den DNS-Namen kennen. Wenn die Dateifreigaben nicht sichtbar sind, müssen die Clients zusätzlich zur Gateway-IP oder dem DNS-Namen auch den Namen der Dateifreigabe kennen, um die Freigaben ermitteln zu können.

> **Note**
>
> Diese Einstellung ist keine effektive Methode, um den Zugriff auf die Dateifreigaben in Ihrer Bereitstellung zu sichern. Aus Sicherheitsgründen empfehlen wir, Berechtigungen so zu konfigurieren, dass der Zugriff auf bestimmte Benutzer und Gruppen beschränkt wird. Anweisungen finden Sie unter Beschränken Sie den Benutzer- und Gruppenzugriff für Ihre SMB-Dateifreigabe.

So legen Sie die Sichtbarkeit von Dateifreigaben fest

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend das Gateway aus, für das Sie die SMB-Einstellungen bearbeiten möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option SMB-Einstellungen bearbeiten und anschließend Sichtbarkeitseinstellungen für Dateifreigaben aus.

4. Aktivieren Sie unter Sichtbarkeitsstatus das Kontrollkästchen, wenn die Freigaben auf diesem Gateway angezeigt werden sollen, wenn das Gateway Freigaben für Benutzer auflistet. Lassen Sie das Kontrollkästchen deaktiviert, wenn die Freigaben auf diesem Gateway nicht angezeigt werden sollen, wenn das Gateway Freigaben für Benutzer auflistet.

Bearbeiten Sie die Einstellungen für Ihre SMB-Dateifreigabe

Sie können die folgenden Einstellungen für eine bestehende SMB-Dateifreigabe bearbeiten:

- Name der Dateifreigabe — wählen Sie einen Namen für die Dateifreigabe
- Audit-Logs — schalten Sie Audit-Logs ein oder aus
- Liste vorhandener Protokollgruppen — wählen Sie eine bestehende Protokollgruppe für Audit-Logs
- Aktualisierungszeit für Datei-Caches außerhalb des Gateways — geben Sie das Intervall an, in dem der Cache der Dateifreigabe aktualisiert werden soll

> **Note**
>
> Wenn dieser Wert kürzer als 30 Minuten ist, kann sich dies negativ auf die Gateway-Leistung auswirken, wenn häufig eine große Anzahl von Amazon S3 S3-Objekten erstellt oder gelöscht wird.

- Abrechnungszeit für Upload-Ereignisse — geben Sie an, wie viele Sekunden nach dem letzten Zeitpunkt, zu dem ein Client in eine Datei geschrieben hat, gewartet werden soll, bevor eine `ObjectUploaded` Benachrichtigung generiert wird
- Speicherklasse für neue Objekte — wählen Sie eine Speicherklasse aus, die für neue Objekte verwendet werden soll, die in Ihrem Amazon S3 S3-Bucket erstellt wurden
- MIME-Typ erraten — wählen Sie aus, ob Storage Gateway den MIME-Typ für hochgeladene Objekte anhand von Dateierweiterungen erraten soll
- Gateway-Dateien, auf die der S3-Bucket-Besitzer zugreifen kann — wählen Sie, ob Dateien auf dem Gateway für das AWS Konto zugänglich sein sollen, dem der Amazon S3 S3-Bucket gehört, der mit der Dateifreigabe verknüpft ist
- Aktivieren Sie, dass der Antragsteller zahlt — wählen Sie aus, ob Konten, die Daten aus der Dateifreigabe lesen oder Daten aus der Dateifreigabe abrufen, die Zugriffsgebühren zahlen sollen und nicht der Bucket-Besitzer

- Exportieren als — Wählen Sie aus, ob Dateien mit Lese-/Schreibzugriff oder schreibgeschützt exportiert werden
- Datei- und Verzeichniszugriff gesteuert von — wählen Sie aus, ob Sie Windows ACLs - oder POSIX-Berechtigungen zur Steuerung des Datei- und Verzeichniszugriffs verwenden möchten
- Opportunistische Sperre (Oplock) — Wählen Sie aus, ob die Dateifreigabe opportunistische Sperren verwenden darf, um die Strategie zur Dateipufferung zu optimieren
- Berücksichtigung der Groß- und Kleinschreibung erzwingen — legen Sie fest, ob der Client oder das Gateway die Groß- und Kleinschreibung bei Datei- und Verzeichnisnamen berücksichtigt

> **Note**
>
> Wenn für die Dateifreigabe derzeit die Option Berücksichtigung von Groß- und Kleinschreibung erzwingen aktiviert ist, kann eine Deaktivierung dazu führen, dass auf Dateien mit identischen Namen, aber unterschiedlichen Groß- und Kleinschreibung (z. B. file.txt, File.txt) nicht zugegriffen werden kann. Clients, bei denen die Groß- und Kleinschreibung nicht beachtet wird, können weiterhin nur auf eine Version zugreifen.

- Zugriffsbasierte Aufzählung von Dateien und Verzeichnissen: Wählen Sie aus, ob die Dateien und Ordner auf der Freigabe während der Verzeichnisaufzählung für alle Benutzer sichtbar sein sollen oder nur für Benutzer, die Lesezugriff haben

> **Note**
>
> Sie können eine bestehende Dateifreigabe nicht so bearbeiten, dass sie auf einen neuen Bucket oder Access Point verweist, oder die VPC-Endpunkteinstellungen 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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie die Option File shares (Dateifreigaben) und wählen Sie dann die Dateifreigabe, die Sie aktualisieren möchten.
3. Wählen Sie für Actions die Option Edit file share settings.
4. Bearbeiten Sie alle Einstellungen, die Sie ändern möchten.

5. Wählen Sie Speichern.

Beschränken Sie den Benutzer- und Gruppenzugriff für Ihre SMB-Dateifreigabe

Wir empfehlen, zugelassene oder verweigerte Benutzer oder Gruppen hinzuzufügen, um den Zugriff auf Ihre Dateifreigabe einzuschränken. Wenn Sie dies nicht tun, steht die Dateifreigabe allen authentifizierten Benutzern zur Verfügung.

Um die SMB-Zugriffseinstellungen zu bearbeiten

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Dateifreigaben und dann die SMB-Dateifreigabe aus, die Sie bearbeiten möchten.
3. Wählen Sie unter Aktionen die Option Einstellungen für den Dateifreigabezugriff bearbeiten aus.
4. Wählen Sie im Abschnitt Dateifreigabezugriff für Benutzer und Gruppen Ihre Einstellungen aus.

   Wählen Sie für Zulässige Benutzer und Gruppen die Option Zulässigen Benutzer hinzufügen oder Zulässige Gruppe hinzufügen aus und geben Sie einen AD-Benutzer oder eine AD-Gruppe ein, dem/der Sie Fileshare-Zugriff gewähren möchten. Wiederholen Sie diesen Vorgang, um so viele Benutzer und Gruppen wie nötig zuzulassen. Allen Benutzern, die nicht in der Liste „Zulässige Benutzer und Gruppen“ aufgeführt sind, wird der Zugriff verweigert.

   Wählen Sie für Verweigerte Benutzer und Gruppen die Option Abgelehnten Benutzer hinzufügen oder Verweigerte Gruppe hinzufügen aus und geben Sie einen AD-Benutzer oder eine AD-Gruppe ein, dem/der Sie den Dateifreigabezugriff verweigern möchten. Wiederholen Sie diesen Vorgang, um so vielen Benutzern und Gruppen wie nötig den Zugriff zu verweigern. Wenn die Liste Zulässige Benutzer und Gruppen leer ist, wird allen Benutzern mit Ausnahme der Benutzer und Gruppen auf der Liste Abgelehnte Benutzer und Gruppen Zugriff gewährt.

   > **Note**
   >
   > Geben Sie nur den AD-Benutzer- oder Gruppennamen ein. Der Domänenname wird durch die Mitgliedschaft des Gateways in dem spezifischen AD impliziert, zu dem das Gateway gehört.

Wenn Sie keine erlaubten oder abgelehnten Benutzer oder Gruppen angeben, kann jeder authentifizierte AD-Benutzer die Dateifreigabe exportieren.

Ändern Sie die serverseitige Verschlüsselungsmethode für eine bestehende Dateifreigabe

Das folgende Verfahren beschreibt, wie Sie die serverseitige Verschlüsselungsmethode für eine bestehende NFS- oder SMB-Dateifreigabe mithilfe der Storage Gateway Gateway-Konsole ändern. Informationen zum Ausführen dieser Aktion mithilfe der Storage Gateway API finden Sie unter Update NFSFile Share oder Update SMBFile Share in der AWS Storage Gateway API-Referenz.

Note

Bei der Aktualisierung der Verschlüsselungsmethode wird die neue Methode auf bestehende Objekte angewendet, die nach dem Update in den Amazon S3 S3-Buckets gespeichert wurden.
Wenn Sie Ihr File Gateway so konfigurieren, dass SSE-KMS für die Verschlüsselung verwendet wird, müssen Sie der IAM-Rolle `kms:Encrypt` `kms:Decrypt` `kms:ReEncrypt*kms:GenerateDataKey`, die der Dateifreigabe zugeordnet ist, manuell `kms:DescribeKey` Berechtigungen hinzufügen. Weitere Informationen finden Sie unter Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für Storage Gateway.

So ändern Sie die serverseitige Verschlüsselungsmethode für eine NFS- oder SMB-Dateifreigabe

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Dateifreigaben und dann die Dateifreigabe aus, für die Sie die Verschlüsselungsmethode ändern möchten.
3. Wählen Sie unter Aktionen die Option Dateifreigabeverschlüsselung bearbeiten aus.
4. Wählen Sie unter Verschlüsselung den Verschlüsselungstyp aus, den Sie für Dateien im Ruhezustand in Amazon S3 verwenden möchten:
   - Um serverseitige Verschlüsselung zu verwenden, die mit Amazon S3 (SSE-S3) verwaltet wird, wählen Sie S3-Managed Keys (SSE-S3). Weitere Informationen finden Sie unter Verwenden

der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

- Um die serverseitige Verschlüsselung zu verwenden, die mit dem AWS Key Management Service (SSE-KMS) verwaltet wird, wählen Sie KMS-verwaltete Schlüssel (SSE-KMS). Wählen Sie für den primären KMS-Schlüssel einen vorhandenen AWS KMS-Schlüssel aus, oder wählen Sie Neuen KMS-Schlüssel erstellen, um in der Key Management Service () -Konsole einen neuen KMS-Schlüssel zu erstellen. AWS AWS KMS

  Weitere Informationen zu finden Sie AWS KMS unter Was ist der AWS Schlüsselverwaltungsdienst? im AWS Key Management Service Entwicklerhandbuch.

- Um die serverseitige Dual-Layer-Verschlüsselung zu verwenden, die mit dem AWS Key Management Service (DSSE-KMS) verwaltet wird, wählen Sie Serverseitige Dual-Layer-Verschlüsselung mit Schlüsseln (DSSE-KMS). AWS Key Management Service Wählen Sie für den primären KMS-Schlüssel einen vorhandenen AWS KMS-Schlüssel aus, oder wählen Sie Neuen KMS-Schlüssel erstellen, um in der Key Management Service () -Konsole einen neuen KMS-Schlüssel zu erstellen. AWS AWS KMS

  Weitere Informationen zu DSSE-KMS finden Sie unter Verwenden der dualen serverseitigen Verschlüsselung mit AWS KMS Schlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Für die Verwendung von DSSE-KMS und Schlüsseln fallen zusätzliche Gebühren an. AWS KMS Weitere Informationen finden Sie unter AWS KMS Preise.
> Um einen AWS KMS Schlüssel mit einem Alias anzugeben, der nicht aufgeführt ist, oder um einen AWS KMS Schlüssel aus einem anderen AWS Konto zu verwenden, müssen Sie den verwenden. AWS Command Line Interface Asymmetrische KMS-Schlüssel werden nicht unterstützt. Weitere Informationen finden Sie unter Create SMBFile Share in der AWS Storage Gateway API-Referenz.

5. Wählen Sie Änderungen speichern, wenn Sie fertig sind.

Bearbeiten Sie die Einstellungen für Ihre NFS-Dateifreigabe

Gehen Sie wie folgt vor, um die Einstellungen für eine bestehende NFS-Dateifreigabe zu bearbeiten, nachdem Sie sie erstellt haben.

> **Note**
>
> Sie können eine bestehende Dateifreigabe nicht so bearbeiten, dass sie auf einen neuen Bucket oder Access Point verweist, oder die VPC-Endpunkteinstellungen 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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie die Option File shares (Dateifreigaben) und wählen Sie dann die Dateifreigabe, die Sie aktualisieren möchten.
3. Wählen Sie für Actions die Option Edit file share settings.
4. Geben Sie unter Name der Dateifreigabe einen Namen für die Dateifreigabe ein.
5. Wählen Sie für Audit-Logs eine der folgenden Optionen aus:

   - Um eine neue Protokollgruppe für diese Dateifreigabe zu erstellen, wählen Sie Neue Protokollgruppe erstellen.
   - Um Integritäts- und Ressourcenbenachrichtigungen für diese Dateifreigabe an eine bestehende Protokollgruppe zu senden, wählen Sie Verwenden und vorhandene Protokollgruppe und wählen Sie dann die gewünschte Gruppe aus der Liste aus.
   - Um die Protokollierung für diese Dateifreigabe zu deaktivieren, wählen Sie Protokollierung deaktivieren.

   Weitere Informationen zu Audit-Logs finden Sie unter Grundlegendes zu S3 File Gateway-Auditprotokollen.
6. Wählen Sie für die Aktualisierungszeit des Datei-Caches außerhalb des Gateways die Option Aktualisierungsintervall festlegen und legen Sie dann die Zeit in Minuten oder Tagen fest, zu der der Cache der Dateifreigabe mithilfe von Time To Live (TTL) aktualisiert werden soll. TTL ist die Zeitspanne seit der letzten Aktualisierung. Nach Ablauf des TTL-Intervalls aktualisiert das File Gateway beim Zugriff auf ein Verzeichnis den Inhalt dieses Verzeichnisses aus dem Amazon S3 S3-Bucket.

> **Note**
>
> Wenn dieser Wert kürzer als 30 Minuten ist, kann sich dies negativ auf die Gateway-Leistung auswirken, wenn häufig eine große Anzahl von Amazon S3 S3-Objekten erstellt oder gelöscht wird.

7. Wählen Sie für Abrechnungszeit für Upload-Ereignisse die Option Abrechnungszeit festlegen und geben Sie dann die Abrechnungszeit in Sekunden ein. Die Abrechnungszeit bestimmt die minimale Verzögerung zwischen dem letzten Schreibvorgang des Clients und der Generierung der Protokollbenachrichtigung. `ObjectUploaded` Da Clients in kurzer Zeit viele kleine Schreibvorgänge in Dateien ausführen können, empfehlen wir, diesen Parameter so lange wie möglich festzulegen, um zu vermeiden, dass mehrere Benachrichtigungen für dieselbe Datei schnell hintereinander generiert werden. Weitere Informationen finden Sie unter Benachrichtigung über Datei-Uploads erhalten.
8. Wählen Sie für Speicherklasse für neue Objekte eine Speicherklasse aus der Dropdownliste aus. Weitere Informationen zu Speicherklassen finden Sie unter Speicherklassen mit einem File Gateway verwenden.
9. Gehen Sie unter Objektmetadaten wie folgt vor:

   a. Wählen Sie MIME-Typ erraten, wenn Sie Storage Gateway erlauben möchten, den Medientyp für hochgeladene Objekte anhand ihrer Dateierweiterungen zu erraten.

   b. Wählen Sie Gateway-Dateien aus, auf die der Besitzer des S3-Buckets Zugriff hat, wenn das AWS Konto, dem der S3-Bucket gehört, das volle Eigentum an den vom Gateway erstellten Dateien haben soll, einschließlich Lese-, Schreib-, Bearbeitungs- und Löschberechtigungen.
10. Wählen Sie „Anforderer zahlt aktivieren“ aus, wenn Sie möchten, dass der Dateianforderer und nicht der Bucket-Besitzer die Kosten für die Datenanforderung und den Download aus dem S3-Bucket trägt.
11.
12. Wählen Sie unter Zugriffsebene eine der folgenden Optionen aus:

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

13. Wählen Sie für Exportieren als eine der folgenden Optionen aus:

    - Um Clients das Lesen und Schreiben von Dateien auf der Dateifreigabe zu ermöglichen, wählen Sie Lesen/Schreiben.
    - Wählen Sie Schreibgeschützt, damit Clients Dateien lesen, aber nicht in die Dateifreigabe schreiben können.

    > **Note**
    >
    > Wenn Sie bei Dateifreigaben, die auf einem Microsoft Windows-Client bereitgestellt sind, Schreibgeschützt wählen, wird möglicherweise eine Meldung über einen unerwarteten Fehler angezeigt, der Sie daran hindert, den Ordner zu erstellen. Sie können diese Meldung ignorieren.

14. Wenn Sie mit der Bearbeitung der Einstellungen fertig sind, wählen Sie Änderungen speichern.

Bearbeiten Sie die Metadaten-Standardeinstellungen für Ihre NFS-Dateifreigabe

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

Wenn Ihr S3 File Gateway Dateien und Ordner in Amazon S3 speichert, werden die Unix-Dateiberechtigungen in Objektmetadaten gespeichert. Wenn Ihr S3 File Gateway Objekte entdeckt, die nicht vom S3 File Gateway gespeichert wurden, werden diesen Objekten standardmäßige Unix-Dateiberechtigungen 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.

Metadaten	Description
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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
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).

Beschränken Sie den Client-Zugriff für Ihre NFS-Dateifreigabe

Wir empfehlen, die Einstellungen für den NFS-Clientzugriff so zu bearbeiten, dass eine Liste bestimmter Client-IP-Adressen oder CIDR-Blockbereiche für NFS-Clients definiert wird, die eine Verbindung zu Ihrer NFS-Dateifreigabe herstellen dürfen. Wenn Sie den Zugriff nicht einschränken möchten, kann jeder Client in Ihrem Netzwerk in Ihre Dateifreigabe eingebunden werden.

Um den Client-Zugriff auf Ihre NFS-Dateifreigabe einzuschränken

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.

2. Wählen Sie im Navigationsbereich auf der linken Seite der Konsolenseite die Option Dateifreigaben und wählen Sie dann die Dateifreigabe-ID der NFS-Dateifreigabe aus, die Sie bearbeiten möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option Einstellungen für den Dateifreigabezugriff bearbeiten aus.

   Im Abschnitt Zugriffsobjekt wird eine Liste von IP-Adressen und CIDR-Blöcken angezeigt, die derzeit eine Verbindung zur NFS-Dateifreigabe herstellen dürfen. Wenn der Zugriff derzeit nicht eingeschränkt ist, wird unter Zulässige Clients ein Eintrag für den CIDR-Block 0.0.0.0/0 angezeigt, der angibt, dass alle möglichen IPv4 Adressen eine Verbindung herstellen dürfen.
4. Wählen Sie unter Zugelassene Clients rechts neben dem CIDR-Block 0.0.0.0/0 die Option Entfernen aus.
5. Wählen Sie Client hinzufügen und geben Sie dann eine IP-Adresse oder einen Adressbereich in CIDR-Notation für die Clients ein, die Sie zulassen möchten.
6. Wiederholen Sie den vorherigen Schritt, um nach Bedarf weitere IP-Adressen oder Bereiche hinzuzufügen. Wenn Sie einen Fehler machen oder den Zugriff widerrufen möchten, können Sie rechts neben der IP-Adresse oder dem Bereich, den Sie aus der Liste löschen möchten, die Option Entfernen auswählen.
7. Wählen Sie Änderungen speichern, wenn Sie fertig sind.

Aktualisieren des Amazon S3 S3-Bucket-Objekt-Caches

Während Ihr NFS- oder SMB-Client Dateisystemoperationen ausführt, führt Ihr Gateway ein Inventar der Objekte im Amazon S3 S3-Objekt-Cache, die mit Ihrer Dateifreigabe verknüpft sind. Ihr Gateway verwendet dieses zwischengespeicherte Inventar, um die Latenz und Häufigkeit von Amazon S3 S3-Anfragen zu reduzieren. Bei diesem Vorgang werden keine Dateien in den S3 File Gateway-Cache-Speicher importiert. Es aktualisiert nur das zwischengespeicherte Inventar, um Änderungen im Inventar der Objekte im Amazon S3 S3-Objekt-Cache widerzuspiegeln.

Um den S3-Bucket-Objekt-Cache für Ihre Dateifreigabe zu aktualisieren, wählen Sie aus der folgenden Liste die Methode aus, die am besten zu Ihrem Anwendungsfall passt, und führen Sie dann das entsprechende Verfahren unten durch.

> **Note**
>
> Unabhängig von der Methode, die Sie verwenden, wird ein Verzeichnis durch das erstmalige Auflisten initialisiert, sodass das Gateway die Metadateninhalte des Verzeichnisses aus Amazon S3 auflistet. Die Zeit, die für die Initialisierung eines Verzeichnisses benötigt wird, ist proportional zur Anzahl der Einträge in diesem Verzeichnis.

Themen

Konfigurieren Sie einen Zeitplan für die automatische Cache-Aktualisierung mithilfe der Storage Gateway Gateway-Konsole

Das folgende Verfahren konfiguriert einen Zeitplan für die automatische Cacheaktualisierung auf der Grundlage eines von Ihnen angegebenen Time To Live (TTL) -Werts. Bevor Sie einen TTL-basierten Cacheaktualisierungszeitplan konfigurieren, sollten Sie Folgendes berücksichtigen:

- TTL wird als die Zeitspanne seit der letzten Cacheaktualisierung für ein bestimmtes Verzeichnis gemessen.
- Eine TTL-basierte Cacheaktualisierung erfolgt nur, wenn nach Ablauf der angegebenen TTL-Periode auf ein bestimmtes Verzeichnis zugegriffen wird.
- Die Aktualisierung ist nicht rekursiv. Sie findet nur in den spezifischen Verzeichnissen statt, auf die zugegriffen wird.
- Für die Aktualisierung fallen Amazon S3-API-Kosten nur für Verzeichnisse an, die seit dem Ablauf der TTL nicht synchronisiert wurden.
  - Verzeichnisse werden nur synchronisiert, wenn auf sie über NFS- oder SMB-Aktivitäten zugegriffen wird.
  - Die Synchronisation erfolgt nicht häufiger als in der von Ihnen angegebenen TTL-Periode.

- Die Konfiguration einer TTL-basierten Cache-Aktualisierung wird nur empfohlen, wenn Sie den Inhalt Ihres Amazon S3 S3-Buckets häufig direkt außerhalb des Workflows zwischen dem Gateway und dem Amazon S3 S3-Bucket aktualisieren.
- NFS- und SMB-Operationen, die auf Verzeichnisse zugreifen, deren Ablauf abgelaufen ist, TTLs werden blockiert, während das Gateway den Inhalt des Verzeichnisses aktualisiert.

> **Note**
>
> Da die Cacheaktualisierung Verzeichniszugriffsvorgänge blockieren kann, empfehlen wir, den längsten TTL-Zeitraum zu konfigurieren, der für Ihre Bereitstellung praktikabel ist.

So konfigurieren Sie einen Zeitplan für die automatische Cache-Aktualisierung mit der Storage Gateway Gateway-Konsole

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Dateifreigaben.
3. Wählen Sie die Dateifreigabe aus, für die Sie den Aktualisierungszeitplan konfigurieren möchten.
4. Wählen Sie für Actions die Option Edit file share settings.
5. Aktivieren Sie für die automatische Cacheaktualisierung von S3 danach das Kontrollkästchen und legen Sie die Uhrzeit in Tagen, Stunden und Minuten fest, zu der der Cache der Dateifreigabe mithilfe von Time To Live (TTL) aktualisiert werden soll. TTL ist die Zeitspanne seit der letzten Aktualisierung, nach der der Zugriff auf das Verzeichnis dazu führen würde, dass das File Gateway zuerst den Inhalt dieses Verzeichnisses aus dem Amazon S3 S3-Bucket aktualisiert.
6. Wählen Sie Änderungen speichern aus.

Konfigurieren Sie einen Zeitplan für die automatische Cache-Aktualisierung AWS Lambda mithilfe einer CloudWatch Amazon-Regel

So konfigurieren Sie einen Zeitplan für die automatische Cache-Aktualisierung AWS Lambda mithilfe einer CloudWatch Amazon-Regel

1. Identifizieren Sie den S3-Bucket, der vom S3 File Gateway verwendet wird.

2. Vergewissern Sie sich, dass der Abschnitt Event leer ist. Er wird später automatisch aufgefüllt.
3. Erstellen Sie eine IAM-Rolle und lassen Sie Trust Relationship for `lambda.amazonaws.com` Lambda zu.
4. Verwenden Sie die folgende Richtlinie.

   JSON

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

5. 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-2:672406474878:share/
share-E51FBS9C'
    )
```

```
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. Wählen Sie für die Ausführungsrolle die IAM-Rolle aus, die Sie erstellt haben.
8. Optional: Fügen Sie einen Auslöser für Amazon S3 hinzu und wählen Sie das Ereignis ObjectCreatedoder aus ObjectRemoved.

> **Note**
>
> `RefreshCache`muss einen Prozess abschließen, bevor ein anderer gestartet wird. Wenn Sie viele Objekte in einem Bucket erstellen oder löschen, kann sich die Leistung verschlechtern. Daher raten wir davon ab, S3-Trigger zu verwenden. Verwenden Sie stattdessen die unten beschriebene CloudWatch Amazon-Regel.

9. Erstellen Sie eine CloudWatch Regel auf der CloudWatch Konsole und fügen Sie einen Zeitplan hinzu. Im Allgemeinen empfehlen wir einen festen Tarif von 30 Minuten. Bei großen S3-Buckets können Sie jedoch 1—2 Stunden verwenden.
10. Fügen Sie einen neuen Auslöser 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. Wählen Sie S3 PUT und passen Sie den Test an Ihre Anforderungen an.
13. Der Test sollte erfolgreich sein. Wenn nicht, ändern Sie das JSON an Ihre Anforderungen und testen Sie es erneut.
14. Öffnen Sie die Amazon S3 S3-Konsole und überprüfen Sie, ob das von Ihnen erstellte Ereignis und der ARN der Lambda-Funktion vorhanden sind.
15. Laden Sie ein Objekt mithilfe der Amazon S3-Konsole oder der in Ihren S3-Bucket hoch AWS CLI.

    Die CloudWatch Konsole generiert eine CloudWatch Ausgabe, die der folgenden ähnelt.

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
```

```
        u'bucket': {u'arn': u'arn:aws:s3:::amzn-s3-demo-bucket', u'name':
 u'MY-GATEWAY-NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}},
 u's3SchemaVersion': u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

Der Lambda-Aufruf gibt Ihnen eine Ausgabe, die der folgenden ähnelt.

```
{
    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'
        }
    }
}
```

Ihr auf Ihrem Client installiertes NFS-Laufwerk wird dieses Update widerspiegeln.

> **Note**
>
> Bei Caches, die das Erstellen oder 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 oder AWS CLI.
17. Sehen Sie sich die auf Ihrem Client installierte NFS-Freigabe an. Stellen Sie sicher, dass Ihr Objekt nicht mehr vorhanden ist (weil Ihr Cache aktualisiert wurde).
18. Überprüfe deine CloudWatch Logs, um das Protokoll deiner Löschung mit dem Ereignis `ObjectRemoved:Delete` zu sehen.

```
{
    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 lautet Ihr CloudWatch Protokollereignisu`'detail-type': u'Scheduled Event'`.

Führen Sie mit der Storage Gateway Gateway-Konsole eine manuelle Cache-Aktualisierung durch

So führen Sie eine manuelle Cache-Aktualisierung mit der Storage Gateway Gateway-Konsole durch

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Dateifreigaben und dann die Dateifreigabe aus, für die Sie die Aktualisierung durchführen möchten.
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.

Führen Sie eine manuelle Cache-Aktualisierung mithilfe der Storage Gateway Gateway-API durch

Das folgende Verfahren führt eine manuelle Cacheaktualisierung mithilfe der Storage Gateway Gateway-API durch. Bevor Sie eine API-basierte Cache-Aktualisierung durchführen, sollten Sie Folgendes beachten:

- Sie können eine rekursive oder eine nicht-rekursive Aktualisierung angeben.
- Eine rekursive Aktualisierung ist ressourcenintensiver und teurer.
- Die Aktualisierung verursacht Amazon S3-API-Kosten nur für Verzeichnisse, die Sie als Argumente in der Anfrage übergeben, und für untergeordnete Verzeichnisse, wenn Sie eine rekursive Aktualisierung angeben.
- Die Aktualisierung wird gleichzeitig mit anderen Vorgängen ausgeführt, während das Gateway verwendet wird.
  - NFS- und SMB-Operationen werden bei Aktualisierungen im Allgemeinen nicht blockiert, es sei denn, für das Verzeichnis, auf das der Vorgang zugreift, ist eine Aktualisierung aktiv.
  - Das Gateway kann nicht feststellen, ob der aktuelle Cache-Inhalt veraltet ist, und verwendet seinen aktuellen Inhalt unabhängig von der Aktualität für NFS- und SMB-Operationen.
  - Da bei einer Cacheaktualisierung virtuelle Gateway-Hardwareressourcen verwendet werden, kann die Gateway-Leistung während der Aktualisierung negativ beeinflusst werden.
- Die Durchführung einer API-basierten Cache-Aktualisierung wird nur empfohlen, wenn Sie den Inhalt Ihres Amazon S3 S3-Buckets direkt außerhalb des Workflows zwischen dem Gateway und dem Amazon S3 S3-Bucket aktualisieren.

> **Note**
>
> Wenn Sie die spezifischen Verzeichnisse kennen, in denen Sie Amazon S3 S3-Inhalte außerhalb des Gateway-Workflows aktualisieren, empfehlen wir, diese Verzeichnisse in Ihrer API-basierten Aktualisierungsanfrage anzugeben, um die Amazon S3 S3-API-Kosten und die Auswirkungen auf die Gateway-Leistung zu reduzieren.

So führen Sie eine manuelle Cache-Aktualisierung mithilfe der Storage Gateway Gateway-API durch

- Senden Sie eine HTTP-POST-Anforderung, um den `RefreshCache` Vorgang mit den gewünschten Parametern über die Storage Gateway Gateway-API aufzurufen. Weitere Informationen finden Sie RefreshCachein der AWS Storage Gateway API-Referenz.

  > **Note**
  >
  > Durch das Senden der `RefreshCache` Anfrage wird nur der Cache-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 abonnieren, um über eine CloudWatch Amazon-Veranstaltung benachrichtigt zu werden. Weitere Informationen finden Sie unter Über Dateioperationen benachrichtigt werden.

Verwenden von S3 Object Lock mit Amazon S3 File Gateway

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

Wenn Sie Amazon S3 Object Lock aktivieren, können Sie das Objekt trotzdem ändern. Beispielsweise kann es über eine Dateifreigabe auf einem S3 File Gateway in eine Dateifreigabe geschrieben, gelöscht oder umbenannt werden. Wenn Sie ein Objekt auf diese Weise ändern, platziert S3 File Gateway eine neue Version des Objekts, ohne dass sich dies auf die vorherige Version (d. h. das gesperrte Objekt) auswirkt.

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

Weitere Informationen zu Amazon S3 Object Lock finden Sie unter Sperren von Objekten mit S3 Object Lock im Amazon Simple Storage Service-Benutzerhandbuch.

Den Status der Dateifreigabe verstehen

Sie können den Status einer Dateifreigabe auf einen Blick überprüfen, indem Sie sich ihren Status ansehen. Wenn der Status anzeigt, dass die Dateifreigabe normal funktioniert, müssen Sie nichts unternehmen. Wenn der Status anzeigt, dass ein Problem vorliegt, können Sie untersuchen, ob möglicherweise Maßnahmen erforderlich sind.

Sie können den Status einer Dateifreigabe auf der Storage Gateway Gateway-Konsole in der Spalte Status anzeigen. Eine Dateifreigabe, die ordnungsgemäß funktioniert, zeigt den Status VERFÜGBAR an. Dies sollte in den meisten Fällen der Status sein.

In der folgenden Tabelle werden die Status von Dateifreigaben beschrieben, was sie bedeuten und ob möglicherweise Maßnahmen erforderlich sind.

Status	Bedeutung
VERFÜGBAR	Die Dateifreigabe ist ordnungsgemäß konfiguriert und verfügbar. Dies ist der Standardstatus für eine Dateifreigabe, die ordnungsgemäß funktioni ert.
WIRD ERSTELLT	Die Dateifreigabe wurde noch nicht vollständig erstellt und ist nicht einsatzbereit. Der Status CREATING ist vorübergehend. Es ist keine Aktion erforderlich. Wenn die Dateifreigabe in diesem Status hängen bleibt, liegt das wahrscheinlich daran, dass die Gateway-VM die Verbindung zu verloren hat AWS.
WIRD AKTUALISI ERT	Die Fileshare-Konfiguration wird gerade aktualisiert. Der Aktualisi erungsstatus ist vorübergehend. Es ist keine Aktion erforderlich. Wenn eine Dateifreigabe in diesem Status hängen bleibt, liegt das wahrschei nlich daran, dass die Gateway-VM die Verbindung zu verloren hat AWS.
WIRD GELÖSCHT	Die Dateifreigabe wird gelöscht. Die Dateifreigabe wird erst gelöscht, wenn alle Daten hochgeladen wurden AWS. Der Status DELETING ist vorübergehend, und es ist keine Aktion erforderlich.
FORCE_DELETING	Die Dateifreigabe wird gewaltsam gelöscht. Die Dateifreigabe wird sofort gelöscht und es werden keine Daten hochgeladen AWS. Der Status FORCE DELETING ist vorübergehend, und es ist keine Aktion erforderl ich.
NICHT VERFÜGBAR	Die Dateifreigabe befindet sich in einem fehlerhaften Status. Es ist eine Aktion erforderlich. Zu den möglichen Ursachen gehören Rollenric htlinienfehler oder die Zuordnung zu einem Amazon S3 S3-Bucket, der nicht existiert. Wenn das Problem, das den fehlerhaften Zustand

Status	Bedeutung
	verursacht hat, behoben ist, nimmt die Dateifreigabe wieder den Status VERFÜGBAR an.

Den Gateway-Status verstehen

Jedem Gateway in Ihrer AWS Storage Gateway Gateway-Bereitstellung ist ein Status zugeordnet, der Sie auf einen Blick über den Zustand des Gateways informiert. In den meisten Fällen gibt der Status an, dass das Gateway normal funktioniert und dass keine Maßnahmen Ihrerseits erforderlich sind. In einigen Fällen gibt der Status ein Problem an, das eventuell eine Aktion Ihrerseits erforderlich macht.

Sie können den Status für jedes Gateway in Ihrer Bereitstellung auf der Seite Gateways der Storage Gateway Gateway-Konsole sehen. Der Gateway-Status wird in der Spalte Status neben dem Namen des Gateways angezeigt. Ein Gateway, das normalerweise funktioniert, hat den Status`RUNNING`.

In der folgenden Tabelle finden Sie eine Beschreibung der einzelnen Gateway-Status und ob Sie auf der Grundlage des Status handeln sollten. Ein Gateway sollte die ganze Zeit oder die meiste Zeit, in der es verwendet wird, einen `RUNNING` Status haben.

Status	Bedeutung
`RUNNING`	Das Gateway ist ordnungsgemäß konfiguriert und kann verwendet werden.
`OFFLINE`	Ihr Gateway befindet sich möglicherweise aus einem oder mehreren der folgenden Gründe in einem `OFFLINE` Status: • Das Gateway kann die Storage Gateway-Dienstendpunkte nicht erreichen. • Das Gateway wurde unerwartet heruntergefahren. • Dem Gateway ist ein Cache-Laufwerk zugeordnet, das getrennt wurde, geändert wurde oder ausgefallen ist.

Verwaltung der Bandbreite für Ihr Amazon S3 File Gateway

Sie können den Upload-Durchsatz von Ihrem Gateway auf einschränken, AWS um die Menge der Netzwerkbandbreite zu kontrollieren, die das Gateway verwendet. Standardmäßig gibt es bei einem aktivierten Gateway keine Ratenlimits.

Sie können einen bandwidth-rate-limit Zeitplan mit dem AWS-Managementkonsole, einem AWS Software Development Kit (SDK) oder der AWS Storage Gateway API konfigurieren (siehe UpdateBandwidthRateLimitSchedulein der AWS Storage Gateway API-Referenz.). Mithilfe eines Zeitplans für Bandbreitenratenbeschränkungen können Sie Grenzwerte so konfigurieren, dass sie sich im Laufe des Tages oder der Woche automatisch ändern. Weitere Informationen finden Sie unter Den bandwidth-rate-limit Zeitplan für Ihr Gateway mithilfe der Storage Gateway Gateway-Konsole anzeigen und bearbeiten.

Sie können den Upload-Durchsatz Ihres Gateways anhand der `CloudBytesUploaded` Metrik auf der Registerkarte Überwachung in der Storage Gateway Gateway-Konsole oder in Amazon überwachen CloudWatch.

> **Note**
>
> Bandbreitenratenbeschränkungen gelten nur für Storage Gateway Gateway-Datei-Uploads. Andere Gateway-Operationen sind nicht betroffen.
> Bei der Begrenzung der Bandbreitenrate wird der Durchsatz aller hochgeladenen Dateien ausgeglichen, wobei der Durchschnitt über jede Sekunde berechnet wird. Es ist zwar möglich, dass Uploads die Bandbreitenratenbegrenzung für eine bestimmte Mikro- oder Millisekunde kurzzeitig überschreiten, dies führt jedoch in der Regel nicht zu großen Spitzen über längere Zeiträume.
> Die Konfiguration von Bandbreitenratenlimits und Zeitplänen wird derzeit für den Typ Amazon FSx File Gateway nicht unterstützt.

Themen

- Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem AWS Tools for Windows PowerShell

Den bandwidth-rate-limit Zeitplan für Ihr Gateway mithilfe der Storage Gateway Gateway-Konsole anzeigen und bearbeiten

In diesem Abschnitt wird beschrieben, wie Sie den Zeitplan für die Bandbreitenratenlimit für Ihr Gateway anzeigen und bearbeiten.

So können Sie den Zeitplan für das Bandbreitenlimit anzeigen und bearbeiten:

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im linken Navigationsbereich erst Gateways und anschließend das Gateway aus, das Sie verwalten möchten.
3. Wählen Sie für Aktionen die Option Bandbreitenraten-Limit bearbeiten aus.

   Der aktuelle bandwidth-rate-limit Zeitplan des Gateways wird auf der Seite Zeitplan für Bandbreitenratenlimit bearbeiten angezeigt. Standardmäßig hat ein neues Gateway keine definierten Bandbreitenbegrenzungen.
4. (Optional) Wählen Sie Neues Bandbreitenratenlimit hinzufügen aus, um dem Zeitplan ein neues konfigurierbares Intervall hinzuzufügen. Geben Sie für jedes hinzugefügte Intervall die folgenden Informationen ein:

   - Upload-Rate — Geben Sie das Limit für die Upload-Rate in Megabit pro Sekunde (Mbit/s) ein. Der Mindestwert ist 100 Mbit/s.
   - Wochentage — Wählen Sie den Tag oder die Tage in jeder Woche aus, an denen das Intervall gelten soll. Sie können das Intervall an Wochentagen (Montag bis Freitag), am Wochenende (Samstag und Sonntag), an jedem Wochentag oder an einem bestimmten Wochentag anwenden. Um das Bandbreitenlimit einheitlich und konstant an allen Tagen und zu jeder Zeit anzuwenden, wählen Sie „Kein Zeitplan“.
   - Startzeit — Geben Sie die Startzeit für das Bandbreitenintervall im Format HH:MM und den Zeitzonenversatz von UTC für Ihr Gateway ein.

> **Note**
>
> Ihr bandwidth-rate-limit Intervall beginnt am Anfang der Minute, die Sie hier angeben.

- Endzeit — Geben Sie die Endzeit für das Bandbreitenintervall im Format HH:MM und den Zeitzonenversatz von GMT für Ihr Gateway ein.

> **Important**
>
> Das bandwidth-rate-limit Intervall endet am Ende der hier angegebenen Minute. Um ein Intervall zu planen, das am Ende einer Stunde endet, geben Sie **59** ein.
> Um aufeinanderfolgende fortlaufende Intervalle zu planen, wobei der Übergang zu Beginn der Stunde ohne Unterbrechung zwischen den Intervallen erfolgt, geben Sie **59** für die Endminute des ersten Intervalls ein. Geben Sie **00** für die Startminute des nachfolgenden Intervalls ein.

5. (Optional) Wiederholen Sie den vorherigen Schritt nach Bedarf, bis Ihr bandwidth-rate-limit Zeitplan vollständig ist. Wenn Sie ein Intervall aus Ihrem Zeitplan löschen müssen, wählen Sie Entfernen.

> **Important**
>
> Bandwidth-rate-limitIntervalle dürfen sich nicht überschneiden. Die Startzeit eines Intervalls muss nach der Endzeit eines vorherigen Intervalls und vor der Startzeit eines nachfolgenden Intervalls liegen.

6. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem AWS SDK für Java

Indem Sie die Bandbreitenbegrenzungen programmgesteuert aktualisieren, können Sie diese Grenzwerte über einen bestimmten Zeitraum automatisch anpassen, z. B. mithilfe von geplanten Tasks. Im folgenden Beispiel wird gezeigt, wie Sie die Bandbreitenlimits eines Gateways mit AWS SDK für Java aktualisieren. 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: Aktualisierung der Gateway-Bandbreitenbegrenzungen mithilfe der AWS 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, Ihren Gateway-Amazon-Ressourcennamen (ARN) und das Upload-Limit angeben. Eine Liste der AWS -Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter Endpunkte und Kontingente für AWS Storage Gateway in der Allgemeine AWS-Referenz.

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

Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem AWS SDK für .NET

Indem Sie die Bandbreitenbegrenzungen programmgesteuert aktualisieren, können Sie diese Grenzwerte über einen bestimmten Zeitraum automatisch anpassen, z. B. mithilfe von geplanten Tasks. Das folgende Beispiel zeigt, wie die Bandbreitenbegrenzungen eines Gateways mithilfe des Software Development Kit (SDK) für.NET aktualisiert werden. AWS 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: Aktualisierung der Gateway-Bandbreitenbegrenzungen mithilfe von AWS 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, Ihren Gateway-Amazon-Ressourcennamen (ARN) und das Upload-Limit angeben. Eine Liste der AWS -Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter Endpunkte und Kontingente für AWS Storage Gateway in der Allgemeine AWS-Referenz.

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

Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem AWS Tools for Windows PowerShell

Indem Sie die Bandbreitenbegrenzungen programmgesteuert aktualisieren, können Sie diese Grenzwerte über einen bestimmten Zeitraum automatisch anpassen, z. B. mithilfe von geplanten Tasks. Im folgenden Beispiel wird gezeigt, wie Sie die Bandbreitenlimits eines Gateways mit AWS Tools for Windows PowerShell aktualisieren. Um den Beispielcode verwenden zu können, sollten Sie mit der Ausführung eines Skripts vertraut sein. PowerShell Weitere Informationen finden Sie unter Erste Schritte im AWS -Tools für PowerShell -Benutzerhandbuch.

Example: Aktualisierung der Gateway-Bandbreitenbegrenzungen mithilfe von AWS Tools for Windows PowerShell

Das folgende PowerShell Skriptbeispiel aktualisiert die Bandbreitenbegrenzungen eines Gateways. Um dieses Beispielskript verwenden zu können, müssen Sie Ihren Gateway-Amazon-Ressourcennamen (ARN) und das Upload-Limit 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)
```

Überwachen von Storage Gateway

In den Themen dieses Abschnitts wird beschrieben, wie ein Gateway mithilfe von Amazon überwacht wird CloudWatch, einschließlich der Überwachung des Cache-Speichers und anderer mit dem Gateway verbundener Ressourcen. Verwenden Sie die Storage-Gateway-Konsole, um Metriken und Alarme für Ihr Gateway anzuzeigen. Sie können beispielsweise die Anzahl der bei Lese- und Schreibvorgängen verwendeten Byte, die für Lese- und Schreibvorgänge aufgewendete Zeit und die Zeit, die zum Abrufen von Daten aus der AWS Cloud benötigt wird, anzeigen. Mit Metriken können Sie den Zustand des Gateways verfolgen und Alarme festlegen, sodass Sie benachrichtigt werden, falls für eine oder mehrere Metriken ein festgelegter Schwellenwert überschritten wird.

Storage Gateway stellt CloudWatch Metriken ohne zusätzliche Kosten bereit. Storage-Gateway-Metriken werden für einen Zeitraum von zwei Wochen aufgezeichnet. Mithilfe dieser Metriken können Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihrer Gateways verschaffen. Storage Gateway bietet auch CloudWatch Alarme, mit Ausnahme von hochauflösenden Alarmen, ohne zusätzliche Kosten. Weitere Informationen zur CloudWatch Preisgestaltung finden Sie unter CloudWatch Amazon-Preise. Weitere Informationen zu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Topics

- CloudWatch Alarme verstehen- Erfahren Sie grundlegende Informationen über CloudWatch Alarme, einschließlich Alarmstatus und empfohlener Konfigurationen.
- Erstellen Sie empfohlene CloudWatch Alarme- Erfahren Sie, wie Sie im Rahmen der ersten Einrichtung von File Gateway schnell und automatisch alle empfohlenen CloudWatch Alarme konfigurieren können.
- Erstellen Sie einen benutzerdefinierten CloudWatch Alarm- Erfahren Sie, wie Sie einen benutzerdefinierten CloudWatch Alarm erstellen können, um eine bestimmte Metrik anhand bestimmter Bewertungskriterien zu überwachen, um Alarmzustände auszulösen und Benachrichtigungen zu senden.
- Überwachung Ihres S3 File Gateway FSx - Erfahren Sie, wie Sie CloudWatch Logs und Audit-Logs einsehen können, und finden Sie Informationen zu den spezifischen Gateway- und Fileshare-Dateisystem-Metriken, die von Ihrem Gateway gemeldet werden.

CloudWatch Alarme verstehen

CloudWatch Alarme überwachen Informationen über Ihr Gateway auf der Grundlage von Metriken und Ausdrücken. Sie können CloudWatch Alarme für Ihr Gateway hinzufügen und deren Status in der Storage Gateway Gateway-Konsole anzeigen. Weitere Informationen zu den Metriken, die zur Überwachung von S3 File Gateway FSx File Gateway und Grundlegendes . Für jeden Alarm geben Sie Bedingungen an, die seinen ALARM-Status aktivieren. Die Alarmstatusanzeigen in der Storage-Gateway-Konsole leuchten rot, wenn der Status ALARM aktiv ist, sodass Sie den Status leichter proaktiv überwachen können. Sie können Alarme so konfigurieren, dass bei anhaltenden Zustandsänderungen automatisch Aktionen aufgerufen werden. Weitere Informationen zu CloudWatch Alarmen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

> **Note**
>
> Wenn Sie keine Zugriffsberechtigung haben CloudWatch, können Sie sich die Alarme nicht ansehen.

Für jedes aktivierte Gateway wird empfohlen, die folgenden CloudWatch-Alarme zu erstellen:

- Hohe E/A-Wartezeit: `IoWaitpercent` >= 20 für 3 Datenpunkte in 15 Minuten
- Cache-Prozent nicht korrekt: `CachePercentDirty` > 80 für 4 Datenpunkte innerhalb von 20 Minuten
- Dateien, die beim Hochladen fehlschlagen: `FilesFailingUpload` >= 1 für 1 Datenpunkt innerhalb von 5 Minuten
- Dateifreigaben nicht verfügbar: `FileSharesUnavailable` >= 1 für 1 Datenpunkt innerhalb von 5 Minuten
- Gesundheitsbenachrichtigungen: `HealthNotifications` >= 1 für 1 Datenpunkt innerhalb von 5 Minuten. Stellen Sie bei der Konfiguration dieses Alarms Fehlende Datenbehandlung auf notBreaching ein.

> **Note**
>
> Sie können einen Zustandsbenachrichtigungsalarm nur festlegen, wenn das Gateway eine vorherige Zustandsbenachrichtigung in CloudWatch hatte.

Für Gateways auf VMware Hostplattformen, die Teil eines VMware Hochverfügbarkeitsclusters sind, empfehlen wir außerdem diesen zusätzlichen Alarm: CloudWatch

- Verfügbarkeitsbenachrichtigungen: `AvailabilityNotifications` >= 1 für 1 Datenpunkt innerhalb von 5 Minuten. Stellen Sie bei der Konfiguration dieses Alarms Fehlende Datenbehandlung auf notBreaching ein.

In der folgenden Tabelle werden die Alarmzustände beschrieben CloudWatch .

Status	Description
OK	Die Metrik oder der Ausdruck liegt innerhalb des festgelegten Schwellenwerts.
Alarm	Die Metrik oder der Ausdruck liegt außerhalb des festgelegten Schwellenwerts.
Unzureichende Daten	Der Alarm wurde soeben gestartet; die Metrik ist nicht verfügbar oder es sind nicht genügend Daten verfügbar, damit die Metrik den Alarmstatus bestimmen kann.
Keine	Es werden keine Alarme für das Gateway erstellt. Informationen zum Erstellen eines neuen Alarms finden Sie unter Erstellen Sie einen benutzerdefinierten CloudWatch Alarm für Ihr Gateway.
Nicht verfügbar	Der Status des Alarms ist unbekannt. Wählen Sie Nicht verfügbar aus, um Fehlerinformationen auf der Registerkarte Überwachung anzuzeigen.

Empfohlene CloudWatch Alarme für Ihr Gateway erstellen

Wenn Sie mit der Storage Gateway-Konsole ein neues Gateway erstellen, können Sie festlegen, dass alle empfohlenen CloudWatch Alarme bei der Ersteinrichtung automatisch erstellt werden.

Weitere Informationen finden Sie unter Amazon S3 File Gateway konfigurieren. Wenn Sie empfohlene CloudWatch Alarme für ein vorhandenes Gateway hinzufügen oder aktualisieren möchten, nachdem Sie die erste Einrichtung bereits abgeschlossen haben, gehen Sie wie folgt vor.

Um empfohlene CloudWatch Alarme für ein vorhandenes Gateway hinzuzufügen oder zu aktualisieren

> **Note**
>
> Für diese Funktion sind CloudWatch Richtlinienberechtigungen erforderlich, die nicht automatisch als Teil der vorkonfigurierten Storage Gateway Gateway-Vollzugriffsrichtlinie gewährt werden. Stellen Sie sicher, dass Ihre Sicherheitsrichtlinie die folgenden Berechtigungen gewährt, bevor Sie versuchen, empfohlene CloudWatch Alarme zu erstellen:
>
> - `cloudwatch:PutMetricAlarm` – Alarme erstellen
> - `cloudwatch:DisableAlarmActions` – Alarmaktionen deaktivieren
> - `cloudwatch:EnableAlarmActions` – Alarmaktionen aktiveren
> - `cloudwatch:DeleteAlarms` - Alarme löschen

1. Öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause/.
2. Wählen Sie im Navigationsbereich auf der linken Seite die Option Gateways und dann das Gateway aus, für das Sie empfohlene CloudWatch Alarme erstellen möchten.
3. Wählen Sie auf der Detailseite für das Gateway die Registerkarte Überwachung aus.
4. Wählen Sie unter Alarme die Option Empfohlene Alarme erstellen aus. Die empfohlenen Alarme werden automatisch erstellt.

   Im Bereich Alarme sind alle CloudWatch Alarme für ein bestimmtes Gateway aufgeführt. Hier können Sie einen oder mehrere Alarme auswählen und löschen, Alarmaktionen aktivieren oder deaktivieren und neue Alarme erstellen.

Erstellen Sie einen benutzerdefinierten CloudWatch Alarm für Ihr Gateway

CloudWatch verwendet Amazon Simple Notification Service (Amazon SNS), um Alarmbenachrichtigungen zu senden, wenn sich der Status eines Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum und führt eine oder mehrere Aktionen durch, die vom Wert der Metrik im Vergleich zu einem festgelegten Schwellenwert in einer Reihe von Zeiträumen abhängt. Die Aktion ist eine Benachrichtigung, die an ein Amazon-SNS-Thema gesendet wird. Sie können ein Amazon SNS SNS-Thema erstellen, wenn Sie einen CloudWatch Alarm erstellen. Weitere Informationen finden Sie unter Was ist Amazon SNS? im Entwicklerhandbuch für Amazon Simple Notification Service.

So erstellen Sie einen CloudWatch Alarm in der Storage Gateway Gateway-Konsole

1. Öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause/.
2. Wählen Sie im Navigationsbereich Gateways und anschließend das Gateway aus, für das Sie einen Alarm erstellen möchten.
3. Wählen Sie auf der Seite mit Gateway-Details die Registerkarte Überwachung aus.
4. Wählen Sie unter Alarme die Option Alarm erstellen aus, um die CloudWatch Konsole zu öffnen.
5. Verwenden Sie die CloudWatch Konsole, um den gewünschten Alarmtyp zu erstellen. Sie können die folgenden Typen von Alarmen erstellen:

   - Statischer Schwellenwertalarm: Ein Alarm, der auf einem festgelegten Schwellenwert für eine ausgewählte Metrik basiert. Der Alarm geht in den ALARM-Status über, wenn die Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet.

     Informationen zum Erstellen eines statischen Schwellenwerts finden Sie unter Erstellen eines CloudWatch Alarms auf der Grundlage eines statischen Schwellenwerts im CloudWatch Amazon-Benutzerhandbuch.
   - Anomalieerkennungsalarm: Anomalieerkennung wertet Metrikdaten aus der Vergangenheit aus und erstellt ein Modell der erwarteten Werte. Sie legen einen Wert für den Schwellenwert für die Erkennung von Anomalien fest und CloudWatch verwenden diesen Schwellenwert zusammen mit dem Modell, um den „normalen“ Wertebereich für die Metrik zu bestimmen. Ein höherer Wert für den Schwellenwert erzeugt ein breiteres Band „normaler“ Werte. Sie können bestimmen, ob der Alarm ausgelöst werden soll, wenn der Metrikwert über der

Bandbreite erwarteter Werte liegt, wenn er darunter liegt oder wenn er die Bandbreite über- oder unterschreitet.

Informationen zum Erstellen eines Alarms bei der Erkennung von Anomalien finden Sie unter Erstellen eines CloudWatch Alarms auf der Grundlage der Anomalieerkennung im CloudWatch Amazon-Benutzerhandbuch.

- Alarm für mathematische Metrik-Ausdrücke: Ein Alarm, der auf einer oder mehreren Metriken basiert, die in einem mathematischen Ausdruck verwendet werden. Geben Sie den Ausdruck, den Schwellenwert und die Auswertungszeiträume an.

  Informationen zum Erstellen eines Alarms für metrische mathematische Ausdrücke finden Sie unter Erstellen eines CloudWatch Alarms auf der Grundlage eines metrischen mathematischen Ausdrucks im CloudWatch Amazon-Benutzerhandbuch.

- Zusammengesetzter Alarm: Ein Alarm, der seinen Alarmstatus bestimmt, indem er die Alarmstatus anderer Alarme beobachtet. Ein zusammengesetzter Alarm kann dazu beitragen, das Alarmrauschen zu reduzieren.

  Informationen zum Erstellen eines zusammengesetzten Alarms finden Sie unter Erstellen eines zusammengesetzten Alarms im CloudWatch Amazon-Benutzerhandbuch.

6. Nachdem Sie den Alarm in der CloudWatch Konsole erstellt haben, kehren Sie zur Storage Gateway Gateway-Konsole zurück. Sie können den Alarm anzeigen, indem Sie einen der folgenden Schritte ausführen:

   - Wählen Sie im Navigationsbereich erst Gateways und anschließend das Gateway aus, für das Sie Alarme erstellen möchten. Wählen Sie auf der Registerkarte Details unter Alarme die Option CloudWatch Alarme aus.
   - Wählen Sie im Navigationsbereich zunächst Gateways, dann das Gateway, für das Sie Alarme anzeigen möchten, und schließlich die Registerkarte Überwachung aus.

     Im Abschnitt Alarme sind alle CloudWatch Alarme für ein bestimmtes Gateway aufgeführt. Hier können Sie einen oder mehrere Alarme auswählen und löschen, Alarmaktionen aktivieren oder deaktivieren und neue Alarme erstellen.
   - Wählen Sie im Navigationsbereich Gateways und anschließend den Alarmstatus des Gateways aus, für den Sie Alarme anzeigen möchten.

Informationen zum Bearbeiten oder Löschen eines Alarms finden Sie unter CloudWatch Alarme bearbeiten oder löschen.

> **Note**
>
> Wenn Sie ein Gateway mit der Storage Gateway Gateway-Konsole löschen, werden auch alle mit dem Gateway verknüpften CloudWatch Alarme automatisch gelöscht.

Überwachung Ihres S3 File Gateway FSx

Sie können Ihr S3 File Gateway und die zugehörigen Ressourcen mithilfe AWS Storage Gateway von CloudWatch Amazon-Metriken und Audit-Logs überwachen. Sie können CloudWatch Ereignisse auch verwenden, um benachrichtigt zu werden, wenn Ihre Dateioperationen abgeschlossen sind.

Themen

Abrufen von S3 File Gateway FSx mit CloudWatch Protokollgruppen

Sie können Amazon CloudWatch Logs verwenden, um Informationen über den Zustand Ihres S3 File Gateways und verwandter Ressourcen zu erhalten. Sie können die Protokolle verwenden, um Ihr Gateway auf Fehler zu überwachen, auf die es stößt. Darüber hinaus können Sie CloudWatch Amazon-Abonnementfilter verwenden, um die Verarbeitung der Protokollinformationen in Echtzeit zu automatisieren. Weitere Informationen finden Sie unter Echtzeitverarbeitung von Protokolldaten mit Abonnements im CloudWatch Amazon-Benutzerhandbuch.

Sie können beispielsweise eine CloudWatch Protokollgruppe konfigurieren, um Ihr Gateway zu überwachen und benachrichtigt zu werden, wenn Ihr S3 File Gateway keine Dateien in einen Amazon S3 S3-Bucket hochladen kann. Sie können die Gruppe entweder bei der Aktivierung des Gateways oder nachdem Ihr Gateway aktiviert und betriebsbereit ist, konfigurieren. Hinweise zur Konfiguration einer CloudWatch Protokollgruppe bei der Aktivierung eines Gateways finden Sie unterKonfigurieren Ihres Amazon S3 File Gateways. Allgemeine Informationen zu CloudWatch Protokollgruppen finden Sie unter Working with Log Groups and Log Streams im CloudWatch Amazon-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für einen Fehler, der von einem S3 File Gateway gemeldet wurde.

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

Dieser Fehler bedeutet, dass das S3 File Gateway das Objekt `myFolder/myFile.text` nicht auf Amazon S3 hochladen kann, da es aus der Amazon S3 Standard-Speicherklasse entweder in die Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive umgestellt wurde.

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 trat dieser Fehler auf, als das Gateway versuchte, das angegebene Objekt auf Amazon S3 hochzuladen oder aus Amazon S3 zu lesen. In diesem Fall wurde das Objekt jedoch auf Amazon Glacier umgestellt. Der Wert von `"type"` kann ein beliebiger Fehler sein, auf den das S3 File Gateway stößt. Eine Liste möglicher Fehler finden Sie unter Fehlerbehebung: Probleme mit File Gateway.
- `"operation": "S3Upload"`gibt an, dass dieser Fehler aufgetreten ist, als das Gateway versuchte, dieses Objekt auf S3 hochzuladen.
- `"key": "myFolder/myFile.text"` gibt das Objekt an, das den Fehler verursacht hat.
- `gateway": "sgw-B1D123D4`gibt das S3 File Gateway an, bei dem dieser Fehler aufgetreten ist.
- `"timestamp": "1565740862516"`gibt den Zeitpunkt an, zu dem der Fehler aufgetreten ist.

Informationen zur Behebung von Fehlern, die möglicherweise von S3 File Gateway gemeldet werden, finden Sie unterFehlerbehebung: Probleme mit File Gateway.

Konfiguration einer CloudWatch Protokollgruppe nach der Aktivierung Ihres Gateways

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

So konfigurieren Sie eine CloudWatch Protokollgruppe für die Verwendung mit Ihrem S3 File Gateway FSx

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie die CloudWatch Protokollgruppe konfigurieren möchten.
3. Wählen Sie für Aktionen die Option Gateway-Informationen bearbeiten aus.
4. Wählen Sie unter Wählen Sie aus, wie die Protokollgruppe eingerichtet werden soll eine der folgenden Optionen:

   - Erstellen Sie eine neue Protokollgruppe, um eine neue CloudWatch Protokollgruppe zu erstellen.
   - Verwenden Sie eine vorhandene Protokollgruppe, um eine bereits vorhandene CloudWatch Protokollgruppe zu verwenden.

     Wählen Sie eine Protokollgruppe aus der Liste der vorhandenen Protokollgruppen aus.
   - Deaktivieren Sie die Protokollierung, wenn Sie Ihr Gateway nicht mithilfe von CloudWatch Protokollgruppen überwachen möchten.
5. Wählen Sie Änderungen speichern aus.
6. Gehen Sie wie folgt vor, um die Zustandsprotokolle für Ihr Gateway anzuzeigen:

   1. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie die CloudWatch Protokollgruppe konfiguriert haben.
   2. Wählen Sie die Registerkarte Details und dann unter Health Logs die Option CloudWatchLogs aus. Die Seite mit den Details zur Protokollgruppe wird in der CloudWatch Konsole geöffnet.

Verwenden von CloudWatch Amazon-Metriken

Sie können Überwachungsdaten für Ihr S3 File Gateway FSx entweder mithilfe der AWS-Managementkonsole oder der CloudWatch API abrufen. Die Konsole zeigt eine Reihe von

Diagrammen an, die auf den Rohdaten der CloudWatch API basieren. Die CloudWatch API kann auch über eines der CloudWatch API-Tools AWS SDKsoder Amazon verwendet werden. Je nach Anforderungen können Sie entweder die in der Konsole angezeigten oder die mit der API aufgerufenen Graphen verwenden.

Unabhängig davon, welche Methode Sie für die Arbeit mit Metriken verwenden, müssen Sie die folgenden Informationen angeben:

- Die zu verwendende Metrikdimension. Eine Dimension ist ein Name-Wert-Paar, mit dem Sie eine Metrik eindeutig identifizieren. `GatewayId` und `GatewayName` sind die Dimensionen für Storage Gateway. In der CloudWatch Konsole können Sie die `Gateway Metrics` Ansicht verwenden, um Gateway-spezifische Dimensionen auszuwählen. Weitere Informationen zu Abmessungen finden Sie unter Abmessungen im CloudWatch Amazon-Benutzerhandbuch.
- Der Metrikname, beispielsweise `ReadBytes`.

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

CloudWatch Amazon-Namespace	Dimension	Description
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Diese Dimensionen filtern nach Metrikdaten, die Aspekte des Gateways beschreiben. Sie können ein S3 File Gateway , mit dem Sie arbeiten möchten, identifizieren, indem Sie `GatewayId` sowohl die als auch die `GatewayName` Dimensionen 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:

- Verfügbare Metriken anzeigen
- Statistiken für eine Metrik abrufen
- Erstellen von CloudWatch -Alarmen

Über Dateioperationen benachrichtigt werden

Storage Gateway kann die folgenden CloudWatch Ereignisse auslösen, wenn Ihre Dateioperationen abgeschlossen sind:

- Sie können sich benachrichtigen lassen, wenn das Gateway das asynchrone Hochladen Ihrer Dateien von der Dateifreigabe zu Amazon S3 abgeschlossen hat. Verwenden Sie den `NotificationPolicy` Parameter, um eine Benachrichtigung zum Hochladen einer Datei anzufordern. Dadurch wird für jeden abgeschlossenen Datei-Upload auf Amazon S3 eine Benachrichtigung gesendet. Weitere Informationen finden Sie unter Sie erhalten eine Benachrichtigung über das Hochladen von Dateien.
- Sie können sich benachrichtigen lassen, wenn das Gateway das asynchrone Hochladen Ihres Arbeitsdateisatzes von der Dateifreigabe zu Amazon S3 abgeschlossen hat. Verwenden Sie den NotifyWhenUploadedAPI-Vorgang, um eine Benachrichtigung zum Hochladen eines funktionierenden Dateisatzes anzufordern. Dadurch wird eine Benachrichtigung gesendet, wenn alle Dateien im Arbeitsdateisatz auf Amazon S3 hochgeladen wurden. Weitere Informationen finden Sie unter Es wird eine Benachrichtigung zum Hochladen eines funktionierenden Dateisatzes angezeigt.
- Sie können eine Benachrichtigung erhalten, wenn ein Gateway die Aktualisierung des Caches für Ihren S3-Bucket abgeschlossen hat. Wenn Sie den RefreshCacheVorgang über die Storage Gateway Gateway-Konsole oder API aufrufen, abonnieren Sie die Benachrichtigung, wenn der Vorgang abgeschlossen ist. Weitere Informationen finden Sie unter Benachrichtigung zur Aktualisierung des Cache-Speichers erhalten.

Wenn der von Ihnen angeforderte Dateivorgang abgeschlossen ist, sendet Storage Gateway Ihnen eine Benachrichtigung über CloudWatch Ereignisse. Sie können CloudWatch Ereignisse so konfigurieren, dass die Benachrichtigung über Ereignisziele wie Amazon SNS, Amazon SQS oder eine AWS Lambda Funktion gesendet wird. Sie können beispielsweise ein Amazon SNS SNS-Ziel so konfigurieren, dass die Benachrichtigung an Amazon SNS SNS-Verbraucher gesendet wird, z. B. als E-Mail oder Textnachricht. Informationen zu CloudWatch Ereignissen finden Sie unter Was sind CloudWatch Ereignisse?

So richten Sie die Benachrichtigung über CloudWatch Ereignisse ein

1. Erstellen Sie ein Ziel, z. B. ein Amazon SNS SNS-Thema oder eine Lambda-Funktion, das aufgerufen werden soll, wenn das von Ihnen in Storage Gateway angeforderte Ereignis eintritt.
2. Erstellen Sie in der CloudWatch Events-Konsole eine Regel, um Ziele auf der Grundlage eines Ereignisses in Storage Gateway aufzurufen.
3. Erstellen Sie in der Regel ein Ereignismuster für den Ereignistyp. Die Benachrichtigung, die gesendet wird, 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 in der angegebenen AWS Region auslöst. 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"
   ]
}
```

Informationen zur Verwendung von CloudWatch Ereignisregeln finden Sie unter Erstellen einer CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird, im Amazon CloudWatch Events-Benutzerhandbuch.

Sie erhalten eine Benachrichtigung über das Hochladen von Dateien

Es gibt zwei Anwendungsfälle, in denen Sie die Benachrichtigung über das Hochladen von Dateien verwenden können:

- Um die Verarbeitung hochgeladener Dateien in der Cloud zu automatisieren, können Sie den `NotificationPolicy` Parameter aufrufen und eine Benachrichtigungs-ID abrufen. Die Benachrichtigung, die angezeigt wird, wenn die Dateien hochgeladen wurden, hat dieselbe

Benachrichtigungs-ID wie die Benachrichtigung, die von der API zurückgegeben wurde. Wenn Sie diese Benachrichtigungs-ID der Nachverfolgung der Liste der Dateien zuordnen, die Sie hochladen, können Sie die Verarbeitung der hochgeladenen Datei einleiten, AWS wenn das Ereignis mit derselben ID generiert wird.

- Für Anwendungsfälle zur Inhaltsverteilung können Sie zwei S3 File Gateways verwenden, die demselben Amazon S3-Bucket zugeordnet sind. Der Fileshare-Client für Gateway1 könnte neue Dateien auf Amazon S3 hochladen, und die Dateien werden von Fileshare-Clients auf Gateway2 gelesen. Die Dateien werden auf Amazon S3 hochgeladen, sind aber für Gateway2 nicht sichtbar, da es eine lokal zwischengespeicherte Version von Dateien in Amazon S3 verwendet. Um die Dateien in Gateway2 sichtbar zu machen, können Sie den `NotificationPolicy` Parameter verwenden, um eine Datei-Upload-Benachrichtigung von Gateway1 anzufordern, um Sie zu benachrichtigen, wenn die Upload-Datei abgeschlossen ist. Anschließend können Sie CloudWatch Ereignisse verwenden, um automatisch eine RefreshCacheAnfrage für die Dateifreigabe auf Gateway2 zu stellen. Wenn die RefreshCacheAnfrage abgeschlossen ist, ist die neue Datei in Gateway2 sichtbar.

Example Beispiel — Benachrichtigung beim Hochladen von Dateien

Das folgende Beispiel zeigt eine Benachrichtigung zum Hochladen von Dateien, die an Sie gesendet wird, CloudWatch wenn das Ereignis der von Ihnen erstellten Regel entspricht. Diese Benachrichtigung weist das JSON-Format auf. Sie können diese Benachrichtigung so konfigurieren, dass sie als Textnachricht an das Ziel übermittelt wird. Das `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": "amzn-s3-demo-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.
Quelle	Der AWS Dienst, der die Quelle der Anfrage und Benachrichtigung ist.
Konto	Die ID des AWS Kontos, von dem aus die Anfrage und die Benachrichtigung generiert wurden.
time	Wann die Anfrage zum Hochladen von Dateien auf Amazon S3 gestellt wurde.
Region	Die AWS Region, aus der die Anfrage und die Benachrichtigung gesendet wurden.
Ressourcen	Die Storage Gateway Gateway-Ressourcen, für die die Richtlinie gilt.
Objektgröße	Die Größe des Objekts in Byte.
Änderungszeit	Der Zeitpunkt, zu dem der Client die Datei geändert hat.
Objektschlüssel	Der Pfad zur Datei.

Feldnamen	Description
event-type	Die CloudWatch Ereignisse, die die Benachric htigung ausgelöst haben.
prefix	Der Präfixname des S3-Buckets.
bucket-name	Der Name des S3-Buckets.

Es wird eine Benachrichtigung zum Hochladen eines funktionierenden Dateisatzes angezeigt

Es gibt zwei Anwendungsfälle, in denen Sie die Benachrichtigung zum Hochladen eines funktionierenden Dateisatzes verwenden können:

- Um die Verarbeitung hochgeladener Dateien in der Cloud zu automatisieren, können Sie die `NotifyWhenUploaded` API aufrufen und eine Benachrichtigungs-ID abrufen. Die Benachrichtigung, die angezeigt wird, wenn die Arbeitsdateien hochgeladen wurden, hat dieselbe Benachrichtigungs-ID wie die Benachrichtigung, die von der API zurückgegeben wurde. Wenn Sie diese Benachrichtigungs-ID der Nachverfolgung der Liste der Dateien zuordnen, die Sie hochladen, können Sie die Verarbeitung der hochgeladenen Arbeitsdateien einleiten, AWS wenn das Ereignis mit derselben ID generiert wird.
- Für Anwendungsfälle zur Inhaltsverteilung können Sie zwei S3 File Gateways verwenden, die demselben Amazon S3-Bucket zugeordnet sind. Der Fileshare-Client für Gateway1 kann neue Dateien auf Amazon S3 hochladen, und die Dateien werden von Fileshare-Clients auf Gateway2 gelesen. Die Dateien werden auf Amazon S3 hochgeladen, sind aber für Gateway2 nicht sichtbar, da es eine lokal zwischengespeicherte Version von Dateien in S3 verwendet. Um die Dateien in Gateway2 sichtbar zu machen, verwenden Sie die NotifyWhenUploadedAPI-Operation, um eine Benachrichtigung über den Datei-Upload von Gateway1 anzufordern, um Sie zu benachrichtigen, wenn der Upload der Arbeitsdateien abgeschlossen ist. Anschließend können Sie mithilfe der CloudWatch Ereignisse automatisch eine RefreshCacheAnfrage für die Dateifreigabe auf Gateway2 stellen. Wenn die RefreshCacheAnfrage abgeschlossen ist, sind die neuen Dateien in Gateway2 sichtbar. Bei diesem Vorgang werden keine Dateien in den Gateway-Cache-Speicher importiert. Es aktualisiert nur das zwischengespeicherte Inventar, um Änderungen im Inventar der Objekte im S3-Bucket widerzuspiegeln.

Example Beispiel — Benachrichtigung zum Hochladen eines funktionierenden Dateisatzes

Das folgende Beispiel zeigt eine Benachrichtigung über das Hochladen eines funktionierenden Dateisatzes, die an Sie gesendet wird, CloudWatch 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. Das `detail-type` ist `Storage Gateway File Upload Event`.

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

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	Der AWS Dienst, der die Quelle der Anfrage und Benachrichtigung ist.

Feldnamen	Description
Konto	Die ID des AWS Kontos, von dem aus die Anfrage und die Benachrichtigung generiert wurden.
time	Wann die Anfrage zum Hochladen von Dateien auf Amazon S3 gestellt wurde.
Region	Die AWS Region, aus der die Anfrage und die Benachrichtigung gesendet wurden.
Ressourcen	Die Storage Gateway Gateway-Ressourcen, für die die Richtlinie gilt.
event-type	Die CloudWatch Ereignisse, 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.
request-received	Wann das Gateway die `NotifyWhe nUploaded` -Anforderung erhalten hat
Um diese potenziell sensiblen Informationen zu schützen, empfehlen wir dringend, die Protokoll e für alle Aufträge zu löschen, die den erreicht haben.	Als alle Dateien im Work-Set auf Amazon S3 hochgeladen wurden.

Benachrichtigung zur Aktualisierung des Cache-Speichers erhalten

Für den Anwendungsfall Aktualisierungs-Cache-Benachrichtigungen können Sie zwei S3-Datei-Gateways verwenden, 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 auf Amazon

S3 hochgeladen, aber sie werden 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. Es kann eine Weile dauern, bis große Dateien in Gateway2 angezeigt werden. Daher möchten Sie möglicherweise benachrichtigt werden, 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 — Cache-Benachrichtigung aktualisieren

Das folgende Beispiel zeigt eine Cache-Aktualisierungsbenachrichtigung, die an Sie gesendet wird, CloudWatch 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. Das `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 Ereignistyps, der die gesendete Benachrichtigung ausgelöst hat.
Quelle	Der AWS Dienst, der die Quelle der Anfrage und Benachrichtigung ist.
Konto	Die ID des AWS Kontos, von dem aus die Anfrage und die Benachrichtigung generiert wurden.
time	Zeitpunkt der Anforderung zum Aktualisieren der Dateien im Arbeitssatz
Region	Die AWS Region, aus der die Anfrage und die Benachrichtigung gesendet wurden.
Ressourcen	Die Storage Gateway Gateway-Ressourcen, für die die Richtlinie gilt.
event-type	Die CloudWatch Ereignisse, 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	als das Gateway die `RefreshCache` Anfrage erhalten hat und die Aktualisierung gestartet wurde.
Um diese potenziell sensiblen Informationen zu schützen, empfehlen wir dringend, die Protokoll	Wann die Aktualisierung des Arbeitssatzes abgeschlossen wurde

Feldnamen	Description
e für alle Aufträge zu löschen, die den erreicht haben.	
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 sich auf S3 File Gateways beziehen. Jedem Gateway ist eine Reihe von Metriken zugeordnet. Einige Gateway-spezifische Metriken haben denselben Namen wie bestimmte Metriken. file-share-specific Diese Metriken stellen dieselben Arten von Messungen dar, beziehen sich jedoch eher auf das Gateway als auf die Dateifreigabe.

Geben Sie immer an, ob Sie mit einem Gateway oder einer Dateifreigabe arbeiten möchten, wenn Sie mit einer bestimmten Metrik arbeiten. Insbesondere bei der Arbeit mit Gateway-Metriken müssen Sie die `Gateway Name` für das Gateway angeben, dessen Metrikdaten Sie anzeigen möchten. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Metriken.

> **Note**
>
> Einige Metriken geben nur dann Datenpunkte zurück, wenn während des letzten Überwachungszeitraums neue Daten generiert wurden.

In der folgenden Tabelle werden die Metriken beschrieben, mit denen Sie Informationen über Ihre S3 File Gateways abrufen können.

Metrik	Description
`AuditNotifications`	Diese Metrik gibt die Anzahl der ausgegebenen Audit-Logs an. Einheiten: Anzahl

Metrik	Description
`AvailabilityNotifications`	Diese Metrik gibt die Anzahl der verfügbar keitsbezogenen Zustandsbenachrichtigungen an, die im Berichtszeitraum vom Gateway generiert wurden. Einheiten: Anzahl
`CacheFileSize`	Diese Metrik verfolgt die Größe der Dateien im Gateway-Cache. Verwenden Sie diese Metrik zusammen mit der `Average` Statistik, um die durchschn ittliche Größe einer Datei im Gateway-Cache zu messen. Verwenden Sie diese Metrik zusammen mit der `Max` Statistik, um die maximale Größe einer Datei im Gateway-C ache zu messen. Einheiten: Byte
`CacheFree`	Diese Metrik gibt die Anzahl der verfügbaren Byte im Gateway-Cache an. Einheiten: Byte
`CacheHitPercent`	Prozentsatz der Anwendungslesevorgänge vom Gateway, die über den Cache bedient werden. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Wenn keine Anwendungslesevorgänge vom Gateway aus erfolgen, meldet diese Metrik 100 Prozent. Einheiten: Prozent

Metrik	Description
`CachePercentDirty`	Der Gesamtprozentsatz des Gateway-Cache, auf den keine Persistenz angewendet wurde. AWS Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Verwenden Sie diese Metrik zusammen mit der `Sum` Statistik. Idealerweise sollte diese Kennzahl niedrig bleiben. Einheiten: Prozent
`CachePercentUsed`	Der Prozentsatz des Datencaches, der für das gesamte Gateway verwendet wird. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheiten: Prozent
`CacheUsed`	Diese Metrik gibt die Anzahl der verwendeten Byte im Gateway-Cache an. Einheiten: Byte
`CloudBytesDownloaded`	Die Gesamtzahl der Byte, von denen das Gateway AWS im Berichtszeitraum heruntergeladen hat. 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
`CloudBytesUploaded`	Die Gesamtzahl der Byte, auf die das Gateway AWS während des Berichtszeitraums Uploads ausgeführt hat. Verwenden Sie diese Metrik zusammen mit der `Sum` Statistik, um den Durchsatz zu messen, und mit der `Samples` Statistik, um input/output Operationen pro Sekunde (IOPS) zu messen. Einheiten: Byte
`FilesFailingUpload`	Diese Metrik verfolgt die Anzahl der Dateien, in die der Upload fehlschlägt. AWS Aus diesen Dateien werden Statusmeldungen generiert , die weitere Informationen zu dem Problem enthalten. Verwenden Sie diese Metrik zusammen mit der `Sum` Statistik, um die Anzahl der Dateien anzuzeigen, in die derzeit kein Upload möglich ist. AWS Einheiten: Anzahl
`FileSharesUnavailable`	Diese Metrik gibt die Anzahl der Dateifreigaben auf diesen Gateways an, die sich im Status Nicht verfügbar befinden. Wenn diese Metrik meldet, dass Dateifrei gaben nicht verfügbar sind, liegt wahrscheinlich ein Problem mit dem Gateway vor, das Ihren Arbeitsablauf stören kann. Es wird empfohlen , einen Alarm auszulösen, 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 Integritä tsbenachrichtigungen an, die von diesem Gateway im Berichtszeitraum generiert wurden. Einheiten: Anzahl
IndexEvictions	Diese Metrik gibt die Anzahl der Dateien an, deren Metadaten aus dem zwischengespeicher ten Index der Dateimetadaten entfernt wurden, um Platz für neue Einträge zu schaffen. Das Gateway verwaltet diesen Metadatenindex, der bei Bedarf aus der AWS Cloud gefüllt wird. Einheiten: Anzahl
IndexFetches	Diese Metrik gibt die Anzahl der Dateien an, für die Metadaten abgerufen wurden. Das Gateway verwaltet einen zwischengespeicher ten Index von Dateimetadaten, der bei Bedarf aus der AWS Cloud gefüllt wird. Einheiten: Anzahl
IoWaitPercent	Diese Metrik gibt an, wie lange die CPU in Prozent auf eine Antwort von der lokalen Festplatte wartet. Einheiten: Prozent
MemTotalBytes	Diese Metrik gibt die Gesamtmenge des Speichers auf dem Gateway an. Einheiten: Byte

Metrik	Description
`MemUsedBytes`	Diese Metrik gibt die Menge des verwendeten Speichers auf dem Gateway an. Einheiten: Byte
`NfsSessions`	Diese Metrik gibt die Anzahl der NFS-Sitzungen an, die auf dem Gateway aktiv sind. Einheiten: Anzahl
`RootDiskFreeBytes`	Diese Metrik gibt die Anzahl der verfügbaren Byte auf der Stammfestplatte des Gateways an. Wenn diese Metrik meldet, dass weniger als 20 GB frei sind, sollten Sie die Größe der Root-Festplatte erhöhen. Um die Größe der Stammfestplatte zu erhöhen, können Sie die Größe der vorhandenen Stammfestplatte auf der VM erhöhen. Wenn die VM neu gestartet wird, erkennt das Gateway die vergrößerte Größe auf der Root-Festplatte. Einheiten: Byte
`S3GetObjectRequestTime`	Diese Metrik gibt an, wie viel Zeit das Gateway benötigt, um S3-Anfragen zum Abrufen von Objekten abzuschließen. Einheiten: Millisekunden
`S3PutObjectRequestTime`	Diese Metrik gibt an, wie viel Zeit das Gateway benötigt, um S3-Put-Objektanforderungen abzuschließen. Einheiten: Millisekunden

Metrik	Description
S3UploadPartRequestTime	Diese Metrik gibt an, wie viel Zeit das Gateway benötigt, um S3-Upload-Teilanfragen abzuschli eßen. Einheiten: Millisekunden
SmbV1Sessions	Diese Metrik gibt die Anzahl der SMBv1 Sitzungen an, die auf dem Gateway aktiv sind. Einheiten: Anzahl
SmbV2Sessions	Diese Metrik gibt die Anzahl der SMBv2 Sitzungen an, die auf dem Gateway aktiv sind. Einheiten: Anzahl
SmbV3Sessions	Diese Metrik gibt die Anzahl der SMBv3 Sitzungen an, die auf dem Gateway aktiv sind. Einheiten: Anzahl
TotalCacheSize	Diese Metrik gibt die Gesamtgröße des Caches an. Einheiten: Byte
UserCpuPercent	Diese Metrik gibt den Prozentsatz der Zeit an, die für die Gateway-Verarbeitung aufgewendet wird. Einheiten: Prozent

Metriken zur Dateifreigabe verstehen

Im Folgenden finden Sie Informationen zu den Storage Gateway Gateway-Metriken, die Dateifreigaben abdecken. 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 CloudWatch Amazon-Metriken.

> **Note**
>
> Einige Metriken geben nur dann Datenpunkte zurück, wenn während des letzten Überwachungszeitraums neue Daten generiert wurden.

In der folgenden Tabelle werden die Storage Gateway Gateway-Metriken beschrieben, mit denen Sie Informationen über Ihre Dateifreigaben abrufen können.

Metrik	Description
`CacheHitPercent`	Prozentsatz der Anwendungslesevorgänge aus den Dateifreigaben, die über den Cache bereitgestellt werden. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Wenn keine Anwendungslesevorgänge von der Dateifreigabe aus durchgeführt werden, gibt diese Metrik 100 Prozent an. Einheiten: Prozent
`CachePercentDirty`	Der Beitrag der Dateifreigabe zum Gesamtant eil des Gateway-Caches, der nicht dauerhaft gespeichert wurde. AWS Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Verwenden Sie diese Metrik zusammen mit der `Sum` Statistik.

Metrik	Description
	Idealerweise sollte diese Kennzahl niedrig bleiben. **Note** Verwenden Sie die `CachePercentDirty` Metrik des Gateways, um den Gesamtprozentsatz des Gateway-Caches anzuzeigen, der noch nicht dauerhaft gespeichert wurde. AWS Einheiten: Prozent
`CachePercentUsed`	Der Prozentsatz des Datencaches, der für das gesamte Gateway verwendet wird. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Diese Fileshare-spezifische Metrik meldet denselben Wert wie die entsprechende Gateway-spezifische Metrik. Einheiten: Prozent
`CloudBytesUploaded`	Die Gesamtzahl der Byte, in die das Gateway während des Berichtszeitraums Uploads ausgeführt hat. AWS 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
`CloudBytesDownloaded`	Die Gesamtzahl der Byte, von denen das Gateway AWS im Berichtszeitraum heruntergeladen hat. Verwenden Sie diese Metrik zusammen mit der `Sum` Statistik, um den Durchsatz zu messen, und mit der `Samples` Statistik, um input/output Operationen pro Sekunde (IOPS) zu messen. Einheiten: Byte
`FilesFailingUpload`	Diese Metrik verfolgt die Anzahl der Dateien, in die der Upload fehlschlägt. AWS Aus diesen Dateien werden Statusmeldungen generiert, die weitere Informationen zu dem Problem enthalten. Verwenden Sie diese Metrik zusammen mit der `Sum` Statistik, um die Anzahl der Dateien anzuzeigen, in die derzeit kein Upload möglich ist. AWS Einheiten: Anzahl
`ReadBytes`	Die Gesamtzahl in Byte, die in Ihren On-Premises-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

Grundlegendes zu S3 File Gateway

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

Operationen

In der folgenden Tabelle werden die Vorgänge zur Prüfung des Dateizugriffs auf Protokolldateien von S3 File beschrieben. FSx

Vorgangsname	Definition
Daten lesen	Lesen Sie den Inhalt einer Datei.
Daten schreiben	Ändert den Inhalt einer Datei.
Create	Eine neue Datei oder einen neuen Ordner erstellen.
Umbenennen	Eine vorhandene Datei oder einen vorhanden en Ordner umbenennen.
Delete	Eine Datei oder einen Ordner löschen.

Vorgangsname	Definition
Schreibattribute	Aktualisieren Sie Datei- oder Ordner-Metadaten (ACLs, Besitzer, Gruppe, Berechtigungen).

Attribute

In der folgenden Tabelle werden die Zugriffsattribute für Audit-Logdateien von S3 File Gateway 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)	Die ID der Gruppe des Benutzers, der auf das Objekt zugreift.
`clientUid` (Nur NFS)	Die ID 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 Erfolge werden protokolliert (Fehler werden protokolliert, mit Ausnahme von Fehlern, die auf verweigerte Berechtigungen zurückzuf ühren sind).
`timestamp`	Der Zeitpunkt, zu dem der Vorgang basierend auf dem Betriebssystemzeitstempel des Gateways ausgeführt wurde.

Attribut	Definition
`version`	Die Version des Auditprotokollformats.

Pro Vorgang protokollierte Attribute

In der folgenden Tabelle werden die Attribute des S3 File Gateway-Audit-Logs beschrieben, die bei jedem Dateizugriffsvorgang protokolliert wurden.

	Daten lesen	Daten schreiben	Erstellen von Ordnern	Datei erstellen	Datei/Ordner umbenennen	Datei/Ordner löschen	Attribute schreiben (ACL ändern — nur SMB)	Attribute schreiben (chown)	Schreiber Sie Attribute (chmod)	Attribute schreiben (chgrp)
`access`			X	X					X	
`accoun` main (r 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
`client` (nur NFS)	X	X	X	X	X	X		X	X	X
`ctime`			X	X						

	Daten lesen	Daten schreiben	Erstellen von Ordnern	Datei erstellen	Datei/Ordner umbenennen	Datei/Ordner löschen	Attribute schreiben (ACL ändern — nur SMB)	Attribute schreiben (chown)	Schreiber Sie Attribute (chmod)	Attribute schreiben (chgrp)
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		
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

	Daten lesen	Daten schreiben	Erstellen von Ordnern	Datei erstellen	Datei/Ordner umbenennen	Datei/Ordner löschen	Attribute schreiben (ACL ändern — nur SMB)	Attribute schreiben (chown)	Schreiber Sie Attribute (chmod)	Attribute schreiben (chgrp)
`source ress`	X	X	X	X	X	X	X	X	X	X
`status`	X	X	X	X	X	X	X	X	X	X
`timest`	X	X	X	X	X	X	X	X	X	X
`versic`	X	X	X	X	X	X	X	X	X	X

Erstellen Sie einen Cache-Bericht für Ihr S3 File Gateway

S3 File Gateway kann einen Bericht mit den Metadaten für Dateien generieren, die sich derzeit im lokalen Upload-Cache für eine bestimmte Dateifreigabe befinden. Sie können Filter und zusätzliche Kriterien anwenden, die bestimmen, welche spezifischen Typen von zwischengespeicherten Dateien im Bericht erscheinen. Sie können diesen Bericht verwenden, um Gateway-Probleme zu identifizieren und zu lösen. Wenn Sie beispielsweise Dateien haben, die nicht von Ihrem Gateway zu Amazon S3 hochgeladen werden können, können Sie einen Bericht erstellen, der die spezifischen Dateien auflistet, die nicht hochgeladen werden konnten, sowie die Gründe für den Upload-Fehler. Der Bericht ist eine CSV-Datei mit einer Liste von Dateien, die den von Ihnen angegebenen Filterparametern entsprechen. Die Ausgabedatei wird als Amazon S3 S3-Objekt an einem Bucket-Speicherort gespeichert, den Sie bei der Konfiguration des Berichts angeben. Informationen zum Erstellen eines Cache-Berichts mithilfe der AWS Storage Gateway API finden Sie StartCacheReportin der Storage Gateway API-Referenz. Gehen Sie wie folgt vor, um einen Cache-Bericht in der Storage Gateway Gateway-Konsole zu erstellen.

Voraussetzungen

- Ihr Gateway muss über `s3:PutObject` `s3:AbortMultipartUpload` Berechtigungen für den Amazon S3 S3-Bucket verfügen, in dem Sie den Cache-Bericht speichern möchten.

- Derzeit können keine anderen Cache-Berichte für die Dateifreigabe bearbeitet werden.
- Es müssen weniger als 10 Cacheberichte für die Dateifreigabe vorhanden sein.
- Das Gateway muss online und verbunden sein AWS.
- Die Gateway-Root-Festplatte muss über mindestens 20 GB freien Speicherplatz verfügen.

So erstellen Sie einen Cache-Bericht mit der Storage Gateway Gateway-Konsole

1. Öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause/.
2. Wählen Sie im Navigationsbereich auf der linken Seite die Option Dateifreigaben und dann die Dateifreigabe aus, für die Sie einen Cache-Bericht erstellen möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option Cache-Bericht erstellen aus.
4. Geben Sie für den Amazon S3-Standort den Amazon S3 S3-Bucket und das Präfix des Speicherorts ein, an dem Sie das CSV-Dateiobjekt für den vollständigen Cache-Bericht in Amazon S3 speichern möchten. Um den Bucket und das Präfix aus Ihrem vorhandenen Amazon S3 S3-Speicher auszuwählen, wählen Sie Browse S3.
5. Gehen Sie für die IAM-Rolle wie folgt vor, um eine IAM-Rolle anzugeben, die Ihnen File Gateway-Berechtigungen zum Generieren und Speichern Ihres Cache-Berichts gewährt:

   - Um eine bestehende IAM-Rolle anzugeben, wählen Sie eine Rolle aus der Dropdownliste aus.
   - Um eine neue IAM-Rolle manuell zu erstellen, wählen Sie Create a role und erstellen Sie dann die neue Rolle mithilfe der IAM-Konsole.

> **Note**
>
> Die von Ihnen angegebene IAM-Rolle muss über die folgenden Berechtigungen verfügen, um Objekte zum Amazon-S3-Speicherort des Berichts-Buckets zu schreiben und mehrteilige Uploads zum Berichts-Bucket zu stoppen:
>
> - `s3:PutObject`
> - `s3:AbortMultipartUpload`
>
> Die Rolle muss es dem `storagegateway.amazonaws.com` Service auch ermöglichen, die Rolle mithilfe der `sts:AssumeRole` Aktion anzunehmen.

6. Führen Sie für den Berichtsfilter einen der folgenden Schritte aus, um zu bestimmen, welche Dateien in den Cache-Bericht aufgenommen werden sollen:

   - Um alle zwischengespeicherten Dateien einzubeziehen, die derzeit nicht auf Amazon S3 hochgeladen werden können, wählen Sie Alle Dateien, die nicht hochgeladen werden können.
   - Um nur die Dateien einzubeziehen, bei denen der Upload zu Amazon S3 aus einem bestimmten Grund fehlschlägt, wählen Sie Nur bestimmte Gründe für Upload-Fehler. Wählen Sie dann unter Gründe für Fehler einen oder mehrere der folgenden Gründe aus:
     - Unzugängliche Speicherklasse — Das Gateway kann nicht auf die Amazon S3 S3-Speicherklasse zugreifen, in der das Objekt gespeichert ist. Weitere Informationen finden Sie unter Fehler: InaccessibleStorageClass.
     - Ungültiger Objektstatus — Der Status der Datei auf dem Gateway entspricht nicht dem Status in Amazon S3. Weitere Informationen finden Sie unter Fehler: InvalidObjectState.
     - Objekt fehlt — Das Objekt wurde in Amazon S3 gelöscht oder verschoben. Weitere Informationen finden Sie unter Fehler: ObjectMissing.
     - S3-Zugriff verweigert — Die IAM-Rolle für den Amazon S3 S3-Bucket-Zugriff erlaubt dem Gateway nicht, den Upload-Vorgang durchzuführen. Weitere Informationen finden Sie unter Fehler: S3 AccessDenied.

   > **Note**
   >
   > Das Flag Files Fail Upload wird alle 24 Stunden und beim Neustart des Gateways zurückgesetzt. Wenn in diesem Bericht die Dateien nach dem Zurücksetzen, aber bevor sie erneut gekennzeichnet werden, erfasst werden, werden sie nicht als Dateien, die nicht hochgeladen wurden, gemeldet.

7. Für Verwenden Sie einen VPC-Endpunkt, um eine Verbindung zu S3 herzustellen? , führen Sie einen der folgenden Schritte aus, um anzugeben, wie Ihr Gateway eine Verbindung zum Amazon S3 S3-Bucket herstellen soll:

   - Um eine direkte Verbindung herzustellen, ohne Amazon VPC zu verwenden, wählen Sie Direkt mit dem Bucket verbinden.
   - Um eine Liste vorhandener Amazon VPC-Endpunkte zu durchsuchen, wählen Sie einen VPC-Endpunkt auswählen und geben Sie dann einen Endpunkt aus der angezeigten VPC-Endpunkt-Dropdownliste an.

- Um einen vorhandenen Amazon VPC-Endpunkt anhand seines DNS-Namens anzugeben, wählen Sie Geben Sie einen VPC-Endpunkt-DNS-Namen ein und geben Sie dann den DNS-Namen in das angezeigte Feld VPC-Endpunkt-DNS-Name ein.

> **Note**
>
> Wenn Ihre Dateifreigabe einen VPC-Endpunkt verwendet, um für den normalen Betrieb eine Verbindung zu Amazon S3 herzustellen, empfehlen wir, bei der Konfiguration Ihres Cache-Berichts dieselbe VPC zu verwenden. Die Erstellung eines Cache-Berichts schlägt fehl, wenn das Gateway aus irgendeinem Grund, einschließlich einer ungültigen VPC-Konfiguration, keine Verbindung zum Amazon S3 S3-Bucket herstellen kann.

8. (Optional) Wählen Sie unter Tags — optional die Option Neues Tag hinzufügen aus und geben Sie dann einen Schlüssel und einen Wert für Ihren Cache-Bericht ein.

   Ein Tag ist ein Schlüssel-Wert-Paar, bei dem Groß- und Kleinschreibung beachtet wird und Ihnen hilft, Ihre Storage Gateway Gateway-Ressourcen zu kategorisieren. Das Hinzufügen von Tags kann das Filtern und Suchen nach Ihrem Cache-Bericht vereinfachen. Sie können diesen Schritt wiederholen, um bis zu 50 Tags hinzuzufügen.

9. Wählen Sie Bericht erstellen, wenn Sie fertig sind.

   Storage Gateway beginnt mit der Generierung des Berichts. Sie können den Fortschritt überprüfen und den Status auf der Registerkarte Cache-Berichte auf der Detailseite für die Dateifreigabe einsehen.

Cache-Berichte für Ihr S3 File Gateway anzeigen und verwalten

In Cacheberichten werden Dateien aufgeführt, die sich derzeit im lokalen Cache für eine bestimmte Dateifreigabe befinden. Dabei werden die von Ihnen angegebenen Filter und Kriterien berücksichtigt. Mit der AWS Storage Gateway API oder der Storage Gateway Gateway-Konsole können Sie eine Liste vorhandener Cache-Berichte für eine bestimmte Dateifreigabe anzeigen, den Berichtsfortschritt und -status überprüfen und Berichte löschen, die Sie nicht mehr benötigen.

Informationen zur Verwaltung von Cache-Berichten mithilfe der API finden Sie in den folgenden Abschnitten in der Storage Gateway API-Referenz:

- ListCacheReports

- DescribeCacheReport
- CancelCacheReport
- DeleteCacheReport

Gehen Sie wie folgt vor, um Cache-Berichte in der Storage Gateway Gateway-Konsole zu verwalten.

So verwalten Sie Cache-Berichte mit der Storage Gateway Gateway-Konsole

1. Öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause/.
2. Wählen Sie im Navigationsbereich auf der linken Seite die Option Dateifreigaben und dann die Dateifreigabe aus, für die Sie Cache-Berichte verwalten möchten.
3. Wählen Sie auf der Detailseite für die Dateifreigabe die Registerkarte Cache-Berichte aus. Diese Registerkarte listet die vorhandenen Cache-Berichte für die Dateifreigabe auf und bietet Informationen über Status, Fortschritt und den Objektpfad, unter dem die Berichtsdatei in Amazon S3 gespeichert ist.
4. Führen Sie eine der folgenden Aktionen aus:

   - Um zusätzliche Details für einen bestimmten Bericht anzuzeigen, z. B. den Berichts-ARN und die zugehörigen Tags, wählen Sie einen Bericht aus der Spalte Berichts-ID aus.
   - Um anzugeben, dass mehrere Berichte gleichzeitig verwaltet werden sollen, wählen Sie die Berichte mithilfe der Checkbox-Spalte aus.
5. Um einen oder mehrere Berichte zu verwalten, wählen Sie im Dropdownmenü Aktionen eine der folgenden Optionen aus:

   - Cache-Bericht löschen — Dadurch wird der Datensatz des Cache-Berichts aus der Storage Gateway Gateway-Datenbank gelöscht. Löschen Sie Datensätze für veraltete Cache-Berichte, um Platz für neue Berichte zu schaffen. Jede Dateifreigabe kann bis zu 10 vorhandene Cache-Berichte gleichzeitig enthalten.

     > **Note**
     >
     > Wenn Sie den Cache-Berichtsdatensatz mit diesem Verfahren löschen, wird das Berichtsdateiobjekt nicht aus Amazon S3 gelöscht.

   - Bericht stornieren — Dadurch wird ein Bericht storniert, der gerade bearbeitet wird. Stornieren Sie einen in Bearbeitung befindlichen Bericht, wenn Sie bei der Berichtskonfiguration einen

Fehler gemacht haben oder wenn die Fertigstellung des Berichts ungewöhnlich lange dauert. Bestätigen Sie die Stornierung, wenn Sie dazu aufgefordert werden.

> **Note**
>
> Die Bearbeitungszeiten können je nach Anzahl der Dateien im Cache erheblich variieren. In der Regel werden die meisten Berichte innerhalb von 5 Minuten abgeschlossen.

Die Storage Gateway Gateway-Konsole zeigt eine Meldung mit dem Ergebnis der Stornierungs- oder Löschaktion an.

Grundlegendes zu den Informationen in den Cache-Berichten von S3 File Gateway

In Cacheberichten werden Dateien aufgeführt, die sich derzeit im lokalen Cache für eine bestimmte Dateifreigabe befinden. Dabei werden die von Ihnen angegebenen Filter und Kriterien berücksichtigt. Jeder Cachebericht enthält die folgenden Informationen:

- Bucket — Der Amazon S3 S3-Bucket oder Access Point, der mit der Dateifreigabe verknüpft ist.
- S3 ObjectKey — Das Amazon S3 S3-Objekt, das die Daten und Metadaten für diese Datei speichert. Dieses Objekt enthält die neuesten Daten, die auf S3 hochgeladen wurden, aber es könnten Daten fehlen, die nicht auf S3 hochgeladen werden können.
- FilePath— Der Dateipfad für den Dateieintrag im Gateway-Cache. Hier finden Sie die Datei, wenn Sie die Dateifreigabe mounten und durchsuchen.
- RenamedTo— Der neue Pfad einer umbenannten Datei. Wenn Sie eine Datei auf Ihrer Dateifreigabe umbenennen, muss das Gateway sowohl den alten als auch den neuen Speicherort der Datei verfolgen. In diesem Feld wird angezeigt, wohin die Datei verschoben wurde, sodass Sie Vorgänge beim Umbenennen von Dateien nachverfolgen können — auch wenn eine Datei mehrfach umbenannt wurde. Diese Informationen sind besonders nützlich, wenn Sie verstehen möchten, wie Dateien in Ihrer Dateifreigabe Objekten in Ihrem Amazon S3 S3-Bucket entsprechen.

  Das folgende Beispiel zeigt die Cache-Berichtseinträge für ein komplexes Szenario, bei dem eine Datei direkt in Amazon S3 überschrieben und gleichzeitig über File Gateway umbenannt wird. In diesem Szenario lädt das Gateway die Datei `A.txt` auf S3 hoch und entfernt dann

den Dateiinhalt, um Platz im lokalen Cache zu schaffen. Das zugehörige S3-Objekt wird dann direkt in S3 überschrieben — nicht durch eine vom Gateway ausgeführte Aktion —, was zu einer Diskrepanz zwischen dem S3-Objekt und den Erwartungen `InvalidObjectState` des Gateways führt. Gleichzeitig wurde die Datei in „Über das Gateway“ umbenannt. `A.txt` `B.txt`

Bucket	S3 ObjectK	FilePat	Renam	Typ	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplc	Upload or	SizeInE es	IsWholeFi leInCache
Muster er-iad	A.txt	/B.txt		FILE	TRUE	FALSE	FALSE	TRUE	Invalid(jectSta	4	FALSE
Beispie Bucket Iad	A.txt	/A.txt	/B.txt	FILE	TRUE	FALSE	TRUE	FALSE		4	FALSE

- Typ — Gibt an, ob der Eintrag für ein `FILE` oder `DIRECTORY` ist.
- IsDirty— `TRUE` Meldet, ob es irgendwelche Änderungen an der Datei gibt, die nicht auf Amazon S3 hochgeladen wurden. Dazu gehören Änderungen an Metadaten wie dem Dateinamen und den read/write Berechtigungen, auch wenn sich die Daten der Datei nicht geändert haben.
- IsDataDirty— `TRUE` Meldet, ob es Änderungen an den Dateidaten gibt, die nicht auf Amazon S3 hochgeladen wurden.
- IsDeleted— `TRUE` Meldet, ob die Datei auf dem Gateway gelöscht wurde. Wenn eine Datei als gelöscht markiert ist, wird sie immer als verschmutzt markiert.
- IsFailingToUpload— `TRUE` Meldet, wenn beim Hochladen der Datei auf Amazon S3 ein Problem auftritt. Dieser Status wird alle 24 Stunden zurückgesetzt, sodass das Gateway den Upload erneut versuchen und überprüfen kann, ob das Problem behoben wurde. Das Gateway lehnt alle neuen Schreibvorgänge für eine Datei ab, die nicht hochgeladen werden kann. Wenn das Gateway nicht die gesamte Datei im Cache hat, lehnt es auch Lesevorgänge ab.
- UploadError— Der Fehler, der verhindert, dass die Datei auf Amazon S3 hochgeladen wird. Weitere Informationen und empfohlene Schritte zur Behebung dieser Fehler finden Sie unter Fehlerbehebung: Probleme mit File Gateway.
- SizeInBytes— Die Gesamtgröße der Datei.
- IsWholeFileInCache— `TRUE` Meldet, ob alle Daten der Datei derzeit im Gateway-Cache gespeichert sind. Wenn dies für eine Datei, die nicht auf Amazon S3 hochgeladen werden kann, WAHR ist, lässt das Gateway das Lesen der Datei zu.

Wartung Ihres Gateways

Wartung Ihres Amazon S3 File Gateway umfasst allgemeine Wartungsarbeiten, um die Leistung Ihres Gateways zu optimieren. Diese Aufgaben sind für alle Gateway-Typen gleich.

Dieser Abschnitt enthält die folgenden Themen, in denen Konzepte und Verfahren zur Wartung Ihres beschrieben werden:

Topics

- Verwaltung von Gateway-Updates— Erfahren Sie, wie Sie Wartungsupdates ein- oder ausschalten und den Zeitplan für das Wartungsfenster für Ihr File Gateway ändern können.
- Durchführung von Wartungsaufgaben über die lokale Konsole— Erfahren Sie, wie Sie Wartungsaufgaben mit der lokalen Gateway-Konsole ausführen.
- Ihre Gateway-VM wird heruntergefahren— Erfahren Sie, was zu tun ist, wenn Sie Ihre virtuelle Gateway-Maschine zu Wartungszwecken herunterfahren oder neu starten müssen, z. B. wenn Sie einen Patch auf Ihren Hypervisor anwenden.
- Ersetzen Sie Ihre vorhandenen S3 File Gateway mit einer neuen Instanz— Erfahren Sie, wie Sie Ihr S3 File Gateway durch eine neue Instanz ersetzen können, wenn Sie die Leistung verbessern oder auf eine Benachrichtigung zur Migration des Gateways reagieren möchten.
- Löschen Sie Ihr Gateway und entfernen Sie die zugehörigen Ressourcen— Erfahren Sie, wie Sie Ihr Gateway mithilfe der AWS Storage Gateway Konsole löschen und die zugehörigen Ressourcen bereinigen, um zu vermeiden, dass deren weitere Nutzung in Rechnung gestellt wird.

Verwaltung von Gateway-Updates

Storage Gateway besteht aus einer Managed Cloud Services-Komponente und einer Gateway-Appliance-Komponente, die Sie entweder lokal oder auf einer Amazon EC2 EC2-Instance in der AWS Cloud bereitstellen. Beide Komponenten werden regelmäßig aktualisiert. In den Themen in diesem Abschnitt wird der Rhythmus dieser Updates beschrieben, wie sie angewendet werden und wie Sie die Einstellungen für Updates auf den Gateways in Ihrer Bereitstellung konfigurieren.

> **Important**
>
> Sie sollten die Storage Gateway Gateway-Appliance wie eine verwaltete virtuelle Maschine behandeln und nicht versuchen, auf ihre Installation oder ihren Inhalt zuzugreifen oder sie in

irgendeiner Weise zu ändern. Der Versuch, Softwarepakete mit anderen Methoden als dem normalen AWS Gateway-Aktualisierungsmechanismus (z. B. SSM- oder Hypervisor-Tools) zu installieren oder zu aktualisieren, kann zu Fehlfunktionen des Gateways führen.
Storage Gateway patcht die Appliance automatisch und regelmäßig, um Sicherheit und Stabilität zu gewährleisten. Storage Gateway Gateway-Appliances verwenden Amazon Linux als Basisbetriebssystem. Sie können den Status der erkannten Common Vulnerabilities and Exposures (CVE) -Probleme im Amazon Linux Security Center überprüfen. CVE-Patches werden automatisch innerhalb von 30 Tagen nach ihrer Veröffentlichung installiert, wie im Amazon Linux Security Center angegeben. Patches werden während Ihres Gateway-Wartungsplans installiert, sofern Ihr Gateway online ist.
Storage Gateway unterstützt die manuelle Aktualisierung eines Amazon EC2 EC2-Gateways mithilfe von Cloud-Init-Direktiven nicht. Wenn Sie diese Methode verwenden, um ein Gateway zu aktualisieren, können Interoperabilitätsprobleme auftreten, die Sie daran hindern, die Gateway-Appliance zu aktivieren oder zu verwenden.

Aktualisierungshäufigkeit und erwartetes Verhalten

AWSaktualisiert die Cloud-Services-Komponente nach Bedarf, ohne dass die bereitgestellten Gateways unterbrochen werden. Ihre bereitgestellten Gateway-Appliances erhalten die folgenden Arten von Updates:

- Wartung — Regelmäßige Updates, die Betriebssystem- und Software-Upgrades, Korrekturen zur Verbesserung der Stabilität, Leistung und Sicherheit sowie Zugriff auf neue Funktionen beinhalten können.
- Dringend — Wichtige Updates, die erforderliche Korrekturen für Probleme beinhalten, die sich unmittelbar auf die Sicherheit, Leistung oder Haltbarkeit Ihres Gateways auswirken. Dringende Updates können jederzeit außerhalb des normalen Rhythmus der monatlichen Wartungs- und Funktionsupdates veröffentlicht werden.

Alle Updates sind kumulativ und aktualisieren Gateways auf die aktuelle Version, wenn sie angewendet werden. Informationen zu den spezifischen Änderungen, die in den einzelnen Updates enthalten sind, finden Sie in den Versionshinweisen für die Gateway-Appliance-Software.

Alle Gateway-Geräte-Updates können zu einer kurzen Betriebsunterbrechung führen. Der VM-Host des Gateways muss während der Updates nicht neu gestartet werden, aber das Gateway ist für kurze Zeit nicht verfügbar, solange das Gateway-Gerät aktualisiert und neu gestartet wird.

Wenn Sie Ihr Gateway bereitstellen und aktivieren, wird ein standardmäßiger Zeitplan für das Wartungsfenster festgelegt. Sie können den Zeitplan für das Wartungsfenster jederzeit ändern. Sie können Wartungsupdates auch deaktivieren, wir empfehlen jedoch, sie aktiviert zu lassen.

> **Note**
>
> Dringende Updates werden gemäß dem Zeitplan für das Wartungsfenster installiert, auch wenn die regulären Wartungsupdates deaktiviert sind.

Bevor ein Update auf Ihr Gateway angewendet wird, AWS benachrichtigt Sie mit einer Meldung auf der Storage Gateway Gateway-Konsole und IhremAWS Health Dashboard. Weitere Informationen finden Sie unter AWS Health Dashboard. Informationen zum Ändern der E-Mail-Adresse, an die Benachrichtigungen über Softwareupdates gesendet werden, finden Sie unter Aktualisieren der alternativen Kontakte für Ihr AWS Konto im Referenzhandbuch zur AWS Kontoverwaltung.

Wenn Updates verfügbar sind, wird auf der Registerkarte „Gateway-Details“ eine Wartungsmeldung angezeigt. Auf der Registerkarte Details können Sie auch das Datum und die Uhrzeit der Installation des letzten erfolgreichen Updates sehen.

Schalten Sie Wartungsupdates ein oder aus

Wenn Wartungs-Updates eingeschaltet sind, wendet Ihr Gateway diese Updates automatisch gemäß dem konfigurierten Zeitplan für das Wartungsfenster an. Weitere Informationen finden Sie unter Ändern des Zeitplans für das Gateway-Wartungsfenster Ändern des Zeitplans .

Wenn Wartungsupdates deaktiviert sind, wendet das Gateway diese Updates nicht automatisch an. Sie können sie jedoch jederzeit manuell über die Storage Gateway Gateway-Konsole, API oder CLI anwenden. Dringende Updates werden manchmal unabhängig von dieser Einstellung während des konfigurierten Wartungsfensters installiert.

> **Note**
>
> Das folgende Verfahren beschreibt, wie Gateway-Updates mithilfe der Storage Gateway Gateway-Konsole ein- oder ausgeschaltet werden. Informationen zum programmgesteuerten Ändern dieser Einstellung mithilfe der API finden Sie UpdateMaintenanceStartTimein der Storage Gateway API-Referenz.

So schalten Sie Wartungsupdates mit der Storage Gateway Gateway-Konsole ein oder aus:

1. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie Wartungsupdates konfigurieren möchten.
3. Wählen Sie Aktionen und dann Wartungseinstellungen bearbeiten aus.
4. Wählen Sie für Wartungsupdates „Ein“ oder „Aus“.
5. Wählen Sie Änderungen speichern, wenn Sie fertig sind.

Sie können die aktualisierte Einstellung auf der Registerkarte Details für das ausgewählte Gateway in der Storage Gateway Gateway-Konsole überprüfen.

Ändern Sie den Zeitplan für das Gateway-Wartungsfenster

Wenn Wartungsupdates aktiviert sind, wendet Ihr Gateway diese Updates automatisch gemäß dem Zeitplan für das Wartungsfenster an. Dringende Updates werden manchmal während des konfigurierten Wartungsfensters installiert, unabhängig von der Einstellung für Wartungsupdates.

> **Note**
>
> Das folgende Verfahren beschreibt, wie Sie den Zeitplan für das Wartungsfenster mithilfe der Storage Gateway Gateway-Konsole ändern. Informationen zum programmgesteuerten Ändern dieser Einstellung mithilfe der API finden Sie UpdateMaintenanceStartTimein der Storage Gateway API-Referenz.

So ändern Sie den Zeitplan für das Wartungsfenster mit der Storage Gateway Gateway-Konsole:

1. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie Wartungsupdates konfigurieren möchten.
3. Wählen Sie Aktionen und dann Wartungseinstellungen bearbeiten aus.
4. Gehen Sie unter Startzeit des Wartungsfensters wie folgt vor:

a. Wählen Sie unter Zeitplan die Option Wöchentlich oder Monatlich aus, um die Häufigkeit des Wartungsfensters festzulegen.

b. Wenn Sie Wöchentlich wählen, ändern Sie die Werte für Wochentag und Uhrzeit, um den bestimmten Zeitpunkt innerhalb jeder Woche festzulegen, an dem das Wartungsfenster beginnt.

   Wenn Sie Monatlich wählen, ändern Sie die Werte für Tag des Monats und Uhrzeit, um den bestimmten Zeitpunkt in jedem Monat festzulegen, an dem das Wartungsfenster beginnt.

> **Note**
>
> Der Höchstwert, der für den Tag des Monats festgelegt werden kann, ist 28. Es ist nicht möglich, den Wartungsplan so einzustellen, dass er an den Tagen 29 bis 31 beginnt.
> Wenn Sie bei der Konfiguration dieser Einstellung eine Fehlermeldung erhalten, kann dies bedeuten, dass Ihre Gateway-Software veraltet ist. Erwägen Sie, Ihr Gateway zunächst manuell zu aktualisieren und dann erneut zu versuchen, den Zeitplan für das Wartungsfenster zu konfigurieren.

5. Wählen Sie Änderungen speichern, wenn Sie fertig sind.

Sie können die aktualisierten Einstellungen auf der Registerkarte Details für das ausgewählte Gateway in der Storage Gateway Gateway-Konsole überprüfen.

Wenden Sie ein Update manuell an

Wenn ein Softwareupdate für Ihr Gateway verfügbar ist, können Sie es manuell installieren, indem Sie wie folgt vorgehen. Bei diesem manuellen Aktualisierungsvorgang wird der Zeitplan für das Wartungsfenster ignoriert und das Update wird sofort angewendet, auch wenn die Wartungsupdates ausgeschaltet sind.

> **Note**
>
> Das folgende Verfahren beschreibt, wie Sie ein Update mithilfe der Storage Gateway Gateway-Konsole manuell anwenden. Informationen zum programmgesteuerten Ausführen

dieser Aktion mithilfe der API finden Sie UpdateGatewaySoftwareNowin der Storage Gateway API-Referenz.

Um ein Gateway-Softwareupdate manuell mit der Storage Gateway Gateway-Konsole anzuwenden:

1. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, das Sie aktualisieren möchten.

   Wenn ein Update verfügbar ist, zeigt die Konsole auf der Registerkarte Gateway-Details ein blaues Benachrichtigungsbanner an, das eine Option zum Anwenden des Updates enthält.
3. Wählen Sie Update jetzt anwenden, um das Gateway sofort zu aktualisieren.

> **Note**
>
> Dieser Vorgang führt zu einer vorübergehenden Unterbrechung der Gateway-Funktionalität während der Installation des Updates. Während dieser Zeit wird der Gateway-Status in der Storage Gateway Gateway-Konsole als OFFLINE angezeigt. Nach Abschluss der Installation des Updates nimmt das Gateway den normalen Betrieb wieder auf und sein Status ändert sich zu RUNNING.

Sie können überprüfen, ob die Gateway-Software auf die neueste Version aktualisiert wurde, indem Sie die Registerkarte Details für das ausgewählte Gateway in der Storage Gateway Gateway-Konsole überprüfen.

Durchführung von Wartungsaufgaben über die lokale Konsole

Dieser Abschnitt enthält die folgenden Themen, die Informationen zur Durchführung von Wartungsaufgaben mithilfe der lokalen Konsole der Gateway-Appliance enthalten. Sie können diese Aufgaben ausführen, indem Sie über die lokale virtuelle Maschine oder Amazon EC2 EC2-Instance, die Ihre Gateway-Appliance hostet, auf die lokale Konsole zugreifen. Die meisten Aufgaben sind auf den verschiedenen Host-Plattformen gleich, es gibt jedoch auch einige Unterschiede.

Topics

- Zugriff auf die lokale Gateway-Konsole- Erfahren Sie, wie Sie sich bei der lokalen Konsole für ein lokales Gateway anmelden, das auf einer Linux Kernel-based Virtual Machine (KVM), VMware ESXi oder Microsoft Hyper-V Manager-Plattform gehostet wird.
- Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine- Erfahren Sie, wie Sie mit der lokalen Konsole grundlegende Einrichtungsaufgaben und erweiterte Konfigurationsaufgaben für ein lokales Gateway ausführen, z. B. einen HTTP-Proxy konfigurieren, den Status der Systemressourcen anzeigen oder Terminalbefehle ausführen.
- Aufgaben auf der lokalen Amazon EC2 EC2-Gateway-Konsole ausführen- Erfahren Sie, wie Sie sich bei der lokalen Konsole anmelden, um grundlegende Einrichtungsaufgaben und erweiterte Konfigurationsaufgaben für ein Amazon EC2 EC2-Gateway durchzuführen, z. B. einen HTTP-Proxy zu konfigurieren, den Status der Systemressourcen anzuzeigen oder Terminalbefehle auszuführen.

Zugriff auf die lokale Gateway-Konsole

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-based Virtual Machine (KVM), VMware ESXi und Microsoft Hyper-V Manager.

Themen

- Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
- Zugreifen auf die lokale Konsole mit VMware ESXi
- Greifen Sie mit Microsoft auf die lokale Gateway-Konsole zu Hyper-V

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
```

Der Befehl gibt eine Liste von VMs mit jeweils ID -, Namen - und Statusinformationen zurück. Notieren Sie sich `Id` die virtuelle Maschine, für die Sie die lokale Gateway-Konsole starten möchten.

2. Verwenden Sie den folgenden Befehl, um auf die lokale Konsole zuzugreifen.

```
# virsh console Id
```

*Id*Ersetzen Sie es durch die ID der VM, die Sie im vorherigen Schritt notiert haben.

Die lokale Konsole des AWS Appliance-Gateways fordert Sie auf, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich bei der lokalen Gateway-Konsole anzumelden. Weitere Informationen finden Sie unter Bei der lokalen File Gateway-Konsole anmelden Bei der lokalen anmelden.

Nachdem Sie sich angemeldet haben, wird das Menü „AWSGeräteaktivierung — Konfiguration“ angezeigt. Sie können aus den Menüoptionen auswählen, um Gateway-Konfigurationsaufgaben auszuführen. Weitere Informationen finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine .

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 die Gateway-VM eingeschaltet ist.

> **Note**
>
> Wenn Ihre Gateway-VM eingeschaltet ist, erscheint ein grünes Pfeilsymbol zusammen mit dem VM-Symbol im VM-Browserfenster auf der linken Seite des Anwendungsfensters. Wenn Ihre Gateway-VM nicht eingeschaltet ist, können Sie sie einschalten, indem Sie in der Werkzeugleiste oben im Anwendungsfenster auf das grüne Einschaltsymbol klicken.

3. Wählen Sie im Hauptinformationsbereich auf der rechten Seite des Anwendungsfensters die Registerkarte Konsole.

   Nach einigen Augenblicken werden Sie von der lokalen Konsole des AWS Appliance-Gateways aufgefordert, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

   > **Note**
   >
   > Drücken Sie Ctrl+Alt (Strg+Alt), um den Mauszeiger aus dem Konsolenfenster freizugeben.

4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich an der lokalen Gateway-Konsole anzumelden. Weitere Informationen finden Sie unter Bei der lokalen File Gateway-Konsole anmelden Bei der lokalen anmelden.

   Nachdem Sie sich angemeldet haben, wird das Menü „AWSGeräteaktivierung — Konfiguration“ angezeigt. Sie können aus den Menüoptionen auswählen, um Gateway-Konfigurationsaufgaben auszuführen. Weitere Informationen finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine .

Greifen Sie mit Microsoft auf die lokale Gateway-Konsole zu Hyper-V

Um auf die lokale Konsole Ihres Gateways zuzugreifen (Microsoft Hyper-V)

1. Wählen Sie Ihre Gateway-Appliance-VM im Bereich Virtuelle Maschinen auf der linken Seite des Microsoft Hyper-V Manager-Anwendungsfensters aus.
2. Stellen Sie sicher, dass das Gateway aktiviert ist.

   > **Note**
   >
   > Wenn Ihre Gateway-VM eingeschaltet `Running` ist, wird dies in der Statusspalte für die VM im Bereich Virtuelle Maschinen auf der linken Seite des Anwendungsfensters angezeigt. Wenn Ihre Gateway-VM nicht eingeschaltet ist, können Sie sie einschalten, indem Sie im Bereich Aktionen auf der rechten Seite des Anwendungsfensters auf Start klicken.

3. Wählen Sie im Bedienfeld „Aktionen“ die Option „Connect“.

   Das Fenster Virtual Machine Connection (Verbindung der virtuellen Maschine) wird angezeigt. Wenn ein Authentifizierungsfenster angezeigt wird, geben Sie die Anmeldeinformationen ein, die Sie vom Hypervisor-Administrator erhalten haben.

   Nach einigen Augenblicken werden Sie von der lokalen Konsole des AWS Appliance-Gateways aufgefordert, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich an der lokalen Gateway-Konsole anzumelden. Weitere Informationen finden Sie unter Bei der lokalen File Gateway-Konsole anmelden Bei der lokalen anmelden.

   Nachdem Sie sich angemeldet haben, wird das Menü „AWSGeräteaktivierung — Konfiguration“ angezeigt. Sie können aus den Menüoptionen auswählen, um Gateway-Konfigurationsaufgaben auszuführen. Weitere Informationen finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine .

Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine

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

Topics

- Melden Sie sich bei der lokalen File Gateway-Konsole an- Erfahren Sie, wie Sie sich an der lokalen Konsole anmelden, wo Sie die Gateway-Netzwerkeinstellungen konfigurieren und das Standardkennwort ändern können.
- Konfigurieren eines HTTP-Proxys- Erfahren Sie, wie Sie Storage Gateway so konfigurieren, dass der gesamte AWS Endpunktdatenverkehr über einen Proxyserver geleitet wird.
- Konfiguration Ihrer Gateway-Netzwerkeinstellungen- Erfahren Sie, wie Sie Ihr Gateway für die Verwendung von DHCP oder einer statischen IP-Adresse konfigurieren.
- Testen der Netzwerkkonnektivität Ihres Gateways- Erfahren Sie, wie Sie die lokale Gateway-Konsole verwenden, um die Netzwerkkonnektivität zu testen.
- Anzeigen des Gateway-Systemressourcen-Status- Erfahren Sie, wie Sie die virtuellen CPU-Kerne, die Größe des Root-Volumes und den Arbeitsspeicher Ihres Gateways überprüfen können.

- Konfiguration eines NTP-Servers (Network Time Protocol) für Ihr Gateway- Erfahren Sie, wie Sie Network Time Protocol (NTP) -Serverkonfigurationen anzeigen und bearbeiten und die Uhrzeit auf Ihrem Gateway mit Ihrem Hypervisor-Host synchronisieren.
- Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole- Erfahren Sie, wie Sie lokale Konsolenbefehle ausführen, um Aufgaben wie das Speichern von Routing-Tabellen, das Herstellen einer Verbindung zu Support usw. auszuführen.

Melden Sie sich bei der lokalen File Gateway-Konsole an

Sobald Sie sich an die VM anmelden können, wird der Anmeldebildschirm angezeigt. Wenn Sie sich zum ersten Mal an der lokalen Konsole der VM anmelden, verwenden Sie die temporären Anmeldeinformationen, um sich anzumelden. Mit diesen temporären Anmeldeinformationen haben Sie Zugriff auf Menüs, in denen Sie die Gateway-Netzwerkeinstellungen konfigurieren und das Passwort von der lokalen Konsole aus ändern können. Der ursprüngliche Benutzername lautet `admin` und das temporäre Passwort lautet`password`. Sie müssen das Passwort bei der ersten Anmeldung ändern.

Um das temporäre Passwort zu ändern

1. Geben Sie im Hauptmenü AWSGeräteaktivierung — Konfiguration die entsprechende Zahl für die Gateway-Konsole ein.
2. Führen Sie den Befehl `passwd` aus. Weitere Informationen zum Ausführen des Befehls finden Sie unter Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole.

Einstellen des Kennworts für die lokale Konsole von der Storage Gateway Gateway-Konsole aus

Sie können das Passwort der lokalen Konsole auch über die webbasierte Storage Gateway Gateway-Konsole verwalten. Alle erfolgreichen Kennwortaktualisierungen, die mit der webbasierten Konsole vorgenommen wurden, setzen das von der lokalen Konsole der Gateway-VM verwendete Passwort außer Kraft, einschließlich des temporären Passworts, falls Sie sich noch nie lokal angemeldet haben. Wenn das Gateway derzeit nicht über das Netzwerk erreichbar ist, schlägt die Kennwortaktualisierung fehl.

So legen Sie das Passwort für die lokale Konsole auf der Storage-Gateway-Konsole fest

1. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.

2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie ein neues Passwort einrichten 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).

   Ihr neues Passwort ersetzt das aktuelle Passwort. Der Storage Gateway Gateway-Dienst speichert, speichert oder protokolliert das Passwort nicht, sondern überträgt es stattdessen sicher über einen verschlüsselten Kanal an die VM, wo es sicher gespeichert wird.

   > **Note**
   >
   > Das Passwort kann aus einem beliebigen Zeichen auf der Tastatur bestehen und 1—512 Zeichen lang sein.

Konfigurieren eines HTTP-Proxys

File Gateways unterstützen die Konfiguration eines HTTP-Proxys.

> **Note**
>
> Die einzige Proxykonfiguration, die File Gateways unterstützen, ist 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 den gesamten AWS Endpunktdatenverkehr über Ihren Proxyserver weiter. Die Kommunikation zwischen dem Gateway und den Endpunkten ist verschlüsselt, auch 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 zur Anmeldung an der Hyper-V lokalen Microsoft-Konsole finden Sie unterGreifen Sie mit Microsoft auf die lokale Gateway-Konsole zu Hyper-V.
- Weitere Informationen zur Anmeldung an der lokalen Konsole für die Linux Kernel-Based Virtual Machine (KVM) finden Sie unterZugreifen auf die lokale Konsole des Gateways mit Linux KVM.

2. Geben Sie im Hauptmenü AWS-Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um HTTP-Proxy aktivieren auszuwählen.
3. Geben Sie im Menü AWSAppliance-Aktivierung HTTP-Proxy-Konfiguration die entsprechende Zahl für die Aufgabe ein, die Sie ausführen möchten:

   - Konfigurieren eines HTTP-Proxy konfigurieren – Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
   - Anzeigen der aktuellen HTTP-Proxy-Konfiguration – Wenn kein HTTP-Proxy konfiguriert ist, wird die Nachricht `HTTP Proxy not configured` angezeigt. Ist ein HTTP-Proxy konfiguriert, werden der Hostname und Port des Proxys angezeigt.
   - Entfernen einer HTTP-Proxy-Konfiguration – Die Nachricht `HTTP Proxy Configuration Removed` wird angezeigt.

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

Konfiguration 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 zur Anmeldung an der Hyper-V lokalen Microsoft-Konsole finden Sie unterGreifen Sie mit Microsoft auf die lokale Gateway-Konsole zu 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. Geben Sie im Hauptmenü AWSGeräteaktivierung — Konfiguration die entsprechende Zahl ein, um Netzwerkkonfiguration auszuwählen.
3. Führen Sie im Menü Netzwerkkonfiguration eine der folgenden Aufgaben aus:

Zur Ausführung dieser Aufgabe	Vorgehensweise
Abrufen von Informationen zum Netzwerkadapter	Geben Sie die entsprechende Zahl ein, um Adapter beschreiben auszuwählen. Eine Liste mit Adapternamen wird angezeigt, und Sie werden aufgefordert, einen Adapternamen einzugeben, z. B. **`eth0`** 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 die hier aufgeführten Adapternamen, wenn Sie eine statische IP-Adresse

Zur Ausführung dieser Aufgabe	Vorgehensweise
	konfigurieren oder wenn Sie den Standarda dapter Ihres Gateways festlegen.
Konfigurieren Sie das DHCP-Routing	Geben Sie die entsprechende Zahl ein, um DHCP konfigurieren auszuwählen. Sie werden aufgefordert, die Netzwerkschnittste lle für die Verwendung von DHCP zu konfiguri eren.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren einer statischen IP-Adresse für Ihr Gateway	Geben Sie die entsprechende Zahl ein, um Statische IP-Adresse konfigurieren auszuwählen. 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 in der Storage-Gateway-Konsole beenden und neu starten, damit die Einstellungen wirksam werden. Weitere Informationen finden Sie unter Ihre Gateway-VM wird heruntergefahren.

Zur Ausführung dieser Aufgabe	Vorgehensweise
	Wenn Ihr Gateway mehr als eine Netzwerks chnittstelle verwendet, müssen Sie alle aktiven Schnittstellen so einrichten, dass sie DHCP oder statische IP-Adressen verwenden. 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 aktivieren, 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.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren eines Hostnamens für Ihr Gateway	Geben Sie die entsprechende Zahl ein, um Hostname konfigurieren auszuwählen. Sie werden aufgefordert, auszuwählen, ob das Gateway einen von Ihnen angegebenen statischen Hostnamen verwenden oder einen Namen automatisch über DCHP oder rDNS beziehen soll. Wenn Sie Statisch auswählen, werden Sie aufgefordert, einen statischen Hostnamen anzugeben, z. B. `testgateway.example.com` Geben Sie einy, um die Konfiguration anzuwenden. **Note** Wenn Sie einen statischen Hostnamen für Ihr Gateway konfigurieren, stellen Sie sicher, dass sich der angegebene Hostname in der Domäne befindet, zu der das Gateway gehört. Sie müssen außerdem einen A-Eintrag in Ihrem DNS-System erstellen, der die IP-Adresse des Gateways auf seinen statischen Hostnamen verweist.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Sehen Sie sich die Hostnamen-Konfiguration Ihres Gateways an	Geben Sie die entsprechende Zahl ein, um Hostnamen-Konfiguration anzeigen auszuwählen. Der Hostname, der Erfassungsmodus, die Domäne und der Active Directory-Bereich Ihres Gateways werden angezeigt.
Zurücksetzen der Netzwerkkonfiguration Ihres Gateways auf DHCP	Geben Sie die entsprechende Zahl ein, um Alles auf DHCP zurücksetzen auszuwählen. Alle Netzwerkschnittstellen sind für die Verwendung von DHCP eingerichtet. **Important** Wenn Ihr Gateway bereits aktiviert wurde, müssen Sie es in der Storage-Gateway-Konsole beenden und neu starten, damit die Einstellungen wirksam werden. Weitere Informationen finden Sie unter Ihre Gateway-VM wird heruntergefahren.
Einrichten des Standard-Routing-Adapters Ihres Gateways	Geben Sie die entsprechende Zahl ein, um Standardadapter festlegen auszuwählen. Die verfügbaren Adapter für Ihr Gateway werden angezeigt, und Sie werden aufgefordert, einen der Adapter auszuwählen, z. B. **`eth0`**

Zur Ausführung dieser Aufgabe	Vorgehensweise
Bearbeiten der DNS-Konfiguration Ihres Gateways	Geben Sie die entsprechende Zahl ein, um DNS-Konfiguration bearbeiten auszuwählen. 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 die entsprechende Zahl ein, um DNS-Konfiguration anzeigen auszuwählen. Die verfügbaren Adapter des primären und sekundären DNS-Servers werden angezeigt. **Note** Bei einigen Versionen des VMware-Hypervisor können Sie die Adapterkonfiguration in diesem Menü bearbeiten.
Anzeigen von Routing-Tabellen	Geben Sie die entsprechende Zahl ein, um Routen anzeigen auszuwählen. 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.

Um die Netzwerkkonnektivität Ihres Gateways zu testen

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 zur Anmeldung an der Hyper-V lokalen Microsoft-Konsole finden Sie unterGreifen Sie mit Microsoft auf die lokale Gateway-Konsole zu 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. Geben Sie im Hauptmenü AWS-Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um Netzwerkkonnektivität testen auszuwählen.

   Wenn Ihr Gateway bereits aktiviert wurde, beginnt der Konnektivitätstest sofort. Für Gateways, die noch nicht aktiviert wurden, müssen Sie den Endpunkttyp AWS-Region wie in den folgenden Schritten beschrieben angeben.
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 öffentlichen Endpunkttyp ausgewählt haben, geben Sie die entsprechende Zahl ein, um den Endpunkttyp auszuwählenAWS-Region, den Sie testen möchten. Unterstützte AWS-Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage GatewayEndpunkte und Kontingente in der. Allgemeine AWS-Referenz

Im Verlauf des Tests zeigt jeder Endpunkt entweder [PASSED] oder [FAILED] an, womit der Status der Verbindung wie folgt angegeben wird:

Fehlermeldung	Description
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über Netzwerkkonnektivität.
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway hat keine Netzwerkkonnektivität.

Anzeigen des Gateway-Systemressourcen-Status

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 zur Anmeldung an der Hyper-V lokalen Microsoft-Konsole finden Sie unterGreifen Sie mit Microsoft auf die lokale Gateway-Konsole zu 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. Geben Sie im Hauptmenü AWS-Appliance-Aktivierung – Konfiguration) die entsprechende Zahl ein, um Systemressourcenprüfung anzeigen auszuwählen.

   Für jede Ressource wird [OK], [WARNING] oder [FAIL] angezeigt, was den Status der Ressource wie folgt angibt:

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

Fehlermeldung	Description
	Beschreibung der Ergebnisse der Ressource nprüfung an.

Die Konsole zeigt die Anzahl der Fehler und Warnungen neben der Menüoption für die Ressourcenprüfung an.

Konfiguration eines NTP-Servers (Network Time Protocol) 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 zur Anmeldung an der Hyper-V lokalen Microsoft-Konsole finden Sie unterGreifen Sie mit Microsoft auf die lokale Gateway-Konsole zu 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. Geben Sie im Hauptmenü AWSGeräteaktivierung — Konfiguration die entsprechende Zahl ein, um System Time Management auszuwählen.
3. Geben Sie im Menü System Time Management die entsprechende Ziffer ein, um eine der folgenden Aufgaben auszuführen.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Zeigen Sie Ihre VM-Zeit an und synchroni sieren Sie sie mit der NTP-Serverzeit.	Geben Sie die entsprechende Zahl ein, um Systemzeit anzeigen und synchronisieren auszuwählen. Die aktuelle Zeit der VM wird angezeigt. Ihr File Gateway ermittelt den Zeitunterschied zu

Zur Ausführung dieser Aufgabe	Vorgehensweise
	Ihrer Gateway-VM, und Ihre NTP-Serverzeit fordert Sie auf, die VM-Zeit mit der NTP-Zeit zu synchronisieren. 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 Sie die VM-Zeit mit der VMware Host-Zeit. Bei einem auf Microsoft Hyper-V bereitges tellten Gateway sollten Sie regelmäßig die Uhrzeit Ihrer VM überprüfen. Weitere Informati onen finden Sie unter Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Host-Zeit. Bei einem Gateway, das auf KVM bereitges tellt wird, können Sie die VM-Zeit mithilfe der `virsh`-Befehlszeilenschnittstelle für KVM überprüfen und synchronisieren.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Bearbeiten Ihrer NTP-Serverkonfiguration	Geben Sie die entsprechende Zahl ein, um NTP-Konfiguration bearbeiten auszuwählen. Sie werden zur Angabe eines bevorzugten und eines sekundären NTP-Servers aufgefordert.
Anzeigen Ihrer NTP-Serverkonfiguration	Geben Sie die entsprechende Zahl ein, um NTP-Konfiguration anzeigen auszuwählen. Ihre NTP-Serverkonfiguration wird angezeigt.

Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole

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 Routingtabellen, das Herstellen einer Verbindung zu Support usw. ausführen.

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 zur Anmeldung an der Hyper-V lokalen Microsoft-Konsole finden Sie unterGreifen Sie mit Microsoft auf die lokale Gateway-Konsole zu 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. Geben Sie im Hauptmenü AWS-Geräteaktivierung – Konfiguration die entsprechende Zahl ein, um Gateway-Konsole auszuwählen.
3. Geben Sie in der Eingabeaufforderung der Gateway-Konsole **h** ein.

   Die Konsole zeigt das Menü VERFÜGBARE BEFEHLE mit den verfügbaren Befehlen an:

Befehl	Funktion
dig	Sammeln Sie die Ausgaben von dig für die DNS-Fehlerbehebung.
exit	Kehren Sie zum Konfigurationsmenü zurück.
h	Zeigen Sie die Liste der verfügbaren Befehle an.
ifconfig	Netzwerkschnittstellen anzeigen oder konfigurieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren. Anweisungen finden Sie unter Konfiguration Ihrer Gateway-Netzwerkeinstellungen.
ip	Routing, Geräte und Tunnel anzeigen/manipulieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren. Anweisungen finden Sie unter Konfiguration Ihrer Gateway-Netzwerkeinstellungen.

Befehl	Funktion
iptables	Verwaltungstool für IPv4-Paketfilterung und NAT.
IP6-Tabellen	Administrationstool für IPv6-Paketfilterung und NAT.
ncport	Testen Sie die Konnektivität zu einem bestimmten TCP-Port in einem Netzwerk.
nping	Sammeln Sie die Ausgaben von nping zur Netzwerkfehlerbehebung.
open-support-channel	Connect zum AWS Support her. Anweisungen zum Aktivieren des AWS Support-Zugriffs finden Sie unter Sie möchten, dass der AWS Support Ihnen bei der Fehlerbehebung Ihres EC2-Gateways hilft .
passwd	Aktualisieren Sie die Authentifizierungstoken.
save-iptables	IP-Tabellen speichern.
save-routing-table	Speichern Sie den neu hinzugefügten Eintrag in der Routingtabelle.
tcptraceroute	Erfassen Sie die Traceroute-Ausgabe des TCP-Datenverkehrs zu einem Ziel.

Befehl	Funktion
sslcheck	Gibt die Ausgabe mit dem Zertifikatsaussteller zurück **Note** Storage Gateway verwendet die Überprüfung durch den Zertifikatsaussteller und unterstützt keine SSL-Inspektion. Wenn dieser Befehl einen anderen Aussteller als aws-appliance@amazon.com zurückgibt, ist es wahrscheinlich, dass eine Anwendung eine SSL-Inspektion durchführt. In diesem Fall empfehlen wir, die SSL-Inspektion für die Storage Gateway Gateway-Appliance zu umgehen.

4. Geben Sie an der Eingabeaufforderung der Gateway-Konsole den entsprechenden Befehl für die Funktion ein, die Sie verwenden möchten, und folgen Sie den Anweisungen.

Um mehr über einen Befehl zu erfahren, geben Sie *command name* in der Befehlszeile **man** + ein.

Aufgaben auf der lokalen Amazon EC2 EC2-Gateway-Konsole ausführen

Für einige Wartungsaufgaben müssen Sie sich bei der lokalen Konsole anmelden, wenn ein Gateway auf einer Amazon-EC2-Instance ausgeführt wird. In diesem Abschnitt wird beschrieben, wie Sie sich bei der lokalen Konsole anmelden und Wartungsaufgaben ausführen.

Topics

- Melden Sie sich bei Ihrer lokalen Amazon EC2-Gateway-Konsole an- Erfahren Sie, wie Sie Ihre Amazon EC2 EC2-Instance mithilfe eines Secure Shell (SSH) -Clients mit der lokalen Gateway-Konsole verbinden und sich dort anmelden.

- Routing Ihres auf Amazon EC2 bereitgestellten Gateways über einen HTTP-Proxy- Erfahren Sie, wie Sie einen Socket Secure Version 5 (SOCKS5) -Proxy zwischen AWS und einem auf einer Amazon EC2 EC2-Instance bereitgestellten Gateway konfigurieren.
- Testen der Netzwerkkonnektivität Ihres Gateways- Erfahren Sie, wie Sie die lokale Gateway-Konsole verwenden, um die Netzwerkkonnektivität zwischen Ihrem Gateway und verschiedenen Netzwerkressourcen zu testen.
- Anzeigen des Gateway-Systemressourcen-Status- Erfahren Sie, wie Sie die lokale Gateway-Konsole verwenden, um die virtuellen CPU-Kerne, die Größe des Root-Volumes und den Arbeitsspeicher Ihres Gateways zu überprüfen.
- Ausführen von Storage Gateway Gateway-Befehlen auf der lokalen Konsole für ein Amazon EC2 EC2-Gateway- Erfahren Sie, wie Sie lokale Konsolenbefehle ausführen, um Aufgaben wie das Speichern von Routing-Tabellen, das Herstellen einer Verbindung zu Support usw. auszuführen.
- Konfiguration Ihrer Amazon EC2 EC2-Gateway-Netzwerkeinstellungen- Erfahren Sie, wie Sie die lokale Konsole verwenden, um Netzwerkeinstellungen wie DNS und Hostname für ein Gateway auf einer Amazon EC2 EC2-Instance anzuzeigen und zu konfigurieren.

Melden Sie sich bei Ihrer lokalen Amazon EC2-Gateway-Konsole an

Sie melden sich mit einem Secure Shell (SSH) -Client bei der lokalen Gateway-Konsole auf einer Amazon EC2 EC2-Instance an. Ausführliche Informationen finden Sie unter Connect to your Instance im Amazon EC2 EC2-Benutzerhandbuch. Für diese Art des Verbindungsaufbaus benötigen Sie das SSH-Schlüsselpaar, das Sie beim Starten Ihrer Instance angegeben haben. Informationen zu Amazon EC2 EC2-Schlüsselpaaren finden Sie unter Amazon EC2 EC2-Schlüsselpaare im Amazon EC2 EC2-Benutzerhandbuch.

So melden Sie sich bei der lokalen Konsole des Gateways an

1. Stellen Sie über SSH Connect zur Amazon EC2 EC2-Instance her und melden Sie sich als Admin-Benutzer an.
2. Nachdem Sie sich angemeldet haben, wird das Hauptmenü AWSAppliance-Aktivierung — Konfiguration angezeigt, von dem aus Sie verschiedene Aufgaben ausführen können.

Für weitere Informationen zu dieser Aufgabe	Siehe folgendes Thema
Konfigurieren eines HTTP-Proxys für Ihr Gateway	Routing Ihres auf Amazon EC2 bereitgestellten Gateways über einen HTTP-Proxy
Konfigurieren von Netzwerkeinstellungen für Ihr Gateway	Konfiguration Ihrer Amazon EC2 EC2-Gateway-Netzwerkeinstellungen
Testen der Netzwerkverbindung	Testen der Netzwerkkonnektivität Ihres Gateways
Anzeigen einer Systemressourcenprüfung	Anzeigen des Gateway-Systemressourcen-Status.
Ausführen von Storage-Gateway-Konsolenbefehlen	Ausführen von Storage Gateway Gateway-Befehlen auf der lokalen Konsole für ein Amazon EC2 EC2-Gateway

Wenn Sie das Gateway beenden möchten, geben Sie **0** ein.

Zum Beenden der Konfigurationssitzung geben Sie **X** ein.

Routing Ihres auf Amazon EC2 bereitgestellten Gateways über einen HTTP-Proxy

Storage Gateway unterstützt die Konfiguration einer Socket Secure-Proxy Version 5 (SOCKS5) zwischen dem auf Amazon EC2 und AWS bereitgestellten Gateway.

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 den gesamten AWS Endpunktdatenverkehr über Ihren Proxyserver weiter. Die Kommunikation zwischen dem Gateway und den Endpunkten ist verschlüsselt, auch 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. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2-Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS-Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um HTTP-Proxy aktivieren auszuwählen.
3. Geben Sie im Menü AWSAppliance-Aktivierung HTTP-Proxy-Konfiguration die entsprechende Zahl für die Aufgabe ein, die Sie ausführen möchten:

   - Konfigurieren eines HTTP-Proxy konfigurieren – Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
   - Anzeigen der aktuellen HTTP-Proxy-Konfiguration – Wenn kein HTTP-Proxy konfiguriert ist, wird die Nachricht `HTTP Proxy not configured` angezeigt. Ist ein HTTP-Proxy konfiguriert, werden der Hostname und Port des Proxys angezeigt.
   - Entfernen einer HTTP-Proxy-Konfiguration – Die Nachricht `HTTP Proxy Configuration Removed` 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 Konnektivität Ihres Gateways

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2-Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS-Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um Netzwerkkonnektivität testen auszuwählen.

   Wenn Ihr Gateway bereits aktiviert wurde, beginnt der Konnektivitätstest sofort. Für Gateways, die noch nicht aktiviert wurden, müssen Sie den Endpunkttyp AWS-Region wie in den folgenden Schritten beschrieben angeben.
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 öffentlichen Endpunkttyp ausgewählt haben, geben Sie die entsprechende Zahl ein, um den Endpunkttyp auszuwählenAWS-Region, den Sie testen möchten. Unterstützte AWS-Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage Gateway verwenden

können, finden Sie unter AWS Storage GatewayEndpunkte und Kontingente in der. Allgemeine AWS-Referenz

Im Verlauf des Tests zeigt jeder Endpunkt entweder [PASSED] oder [FAILED] an, womit der Status der Verbindung wie folgt angegeben wird:

Fehlermeldung	Description
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über Netzwerkkonnektivität.
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway hat keine Netzwerkkonnektivität.

Anzeigen des Gateway-Systemressourcen-Status

Wenn Ihr File Gateway startet, überprüft es seine virtuellen CPU-Kerne, die Größe des Root-Volumes und den Arbeitsspeicher. Anschließend wird festgestellt, ob die verfügbaren Systemressourcen ausreichen, damit Ihr Gateway ordnungsgemäß funktioniert. Sie können die Ergebnisse der Überprüfung der Systemressourcen mithilfe der lokalen Gateway-Konsole anzeigen.

So zeigen Sie den Status einer Systemressourcenprüfung an

1. Melden Sie sich bei der lokalen Konsole auf Ihrem Amazon EC2 File Gateway an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2-Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS-Geräteaktivierung – Konfiguration) die entsprechende Zahl ein, um Systemressourcenprüfung anzeigen auszuwählen.

   Die lokale Gateway-Konsole zeigt [OK], [WARNUNG] oder [FAIL] an, um den Status der Ressource wie folgt anzuzeigen:

Fehlermeldung	Description
[OK]	Die Ressource hat die Systemressourcenprüfung bestanden.

Fehlermeldung	Description
[WARNING] ([WARNUNG])	Die Ressource erfüllt nicht die empfohlen en Anforderungen, aber Ihr Gateway kann weiterhin funktionieren. Auf der lokalen Gateway-Konsole wird eine Meldung angezeigt , in der die Ergebnisse der Ressourcenprüfung beschrieben werden.
[FAIL] ([FEHLGESCHLAGEN])	Die Ressource erfüllt nicht die Mindestan forderungen. Das Gateways funktioniert möglicherweise nicht ordnungsgemäß. Die lokale Gateway-Konsole zeigt eine Meldung an, die die Ergebnisse der Ressourcenprüfung beschreibt.

Auf der lokalen Konsole wird auch die Anzahl der Fehler und Warnungen neben der Menüoption „Ressourcenprüfung“ angezeigt.

Ausführen von Storage Gateway Gateway-Befehlen auf der lokalen Konsole für ein Amazon EC2 EC2-Gateway

Die AWS Storage Gateway Konsole bietet eine sichere Umgebung für die Konfiguration und Diagnose von Problemen mit Ihrem Gateway. Mithilfe der Konsolenbefehle können Sie Wartungsaufgaben wie das Speichern von Routingtabellen oder das Herstellen einer Verbindung zu Support ausführen.

So führen Sie eine Konfiguration oder einen Diagnosebefehl aus

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2-Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS-Geräteaktivierung – Konfiguration die entsprechende Zahl ein, um Gateway-Konsole auszuwählen.
3. Geben Sie in der Eingabeaufforderung der Gateway-Konsole **h** ein.

   Die Konsole zeigt das Menü VERFÜGBARE BEFEHLE mit den verfügbaren Befehlen an:

Befehl	Funktion
dig	Sammeln Sie die Ausgaben von dig für die DNS-Fehlerbehebung.
exit	Kehren Sie zum Konfigurationsmenü zurück.
h	Zeigen Sie die Liste der verfügbaren Befehle an.
ifconfig	Netzwerkschnittstellen anzeigen oder konfigurieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren. Anweisungen finden Sie unter Konfiguration Ihrer Gateway-Netzwerkeinstellungen.
ip	Routing, Geräte und Tunnel anzeigen/manipulieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren. Anweisungen finden Sie unter Konfiguration Ihrer Gateway-Netzwerkeinstellungen.

Befehl	Funktion
iptables	Verwaltungstool für IPv4-Paketfilterung und NAT.
IP6-Tabellen	Administrationstool für IPv6-Paketfilterung und NAT.
ncport	Testen Sie die Konnektivität zu einem bestimmten TCP-Port in einem Netzwerk.
nping	Sammeln Sie die Ausgaben von nping zur Netzwerkfehlerbehebung.
open-support-channel	Connect zum AWS Support her.
save-iptables	IP-Tabellen speichern.
save-routing-table	Speichern Sie den neu hinzugefügten Eintrag in der Routingtabelle.
tcptraceroute	Erfassen Sie die Traceroute-Ausgabe des TCP-Datenverkehrs zu einem Ziel.

4. Geben Sie an der Eingabeaufforderung der Gateway-Konsole den entsprechenden Befehl für die Funktion ein, die Sie verwenden möchten, und folgen Sie den Anweisungen.

Um mehr über einen Befehl zu erfahren, geben Sie *command name* in der Befehlszeile **man** + ein.

Konfiguration Ihrer Amazon EC2 EC2-Gateway-Netzwerkeinstellungen

Sie können die Netzwerkeinstellungen für Ihr Amazon EC2 File Gateway mithilfe der lokalen Gateway-Konsole anzeigen und konfigurieren.

Um Ihre Netzwerkeinstellungen zu konfigurieren

1. Melden Sie sich bei der lokalen Konsole auf Ihrem Amazon EC2 File Gateway an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2-Gateway-Konsole an.

2. Geben Sie im Hauptmenü AWSAppliance-Aktivierung — Konfiguration die entsprechende Zahl ein, um Netzwerkkonfiguration auszuwählen.
3. Geben Sie im Menü AWSGeräteaktivierung — Netzwerkkonfiguration die entsprechende Zahl für die Aufgabe ein, die Sie ausführen möchten:

   - DNS-Konfiguration bearbeiten — Die lokale Gateway-Konsole zeigt die verfügbaren Adapter für den primären und sekundären DNS-Server an. Die Konsole fordert Sie dann auf, die neue IP-Adresse anzugeben.
   - DNS-Konfiguration anzeigen — Die lokale Gateway-Konsole zeigt die verfügbaren Adapter für den primären und sekundären DNS-Server an.
   - Hostname konfigurieren — Die lokale Gateway-Konsole fordert Sie auf, auszuwählen, ob das Gateway einen von Ihnen angegebenen statischen Hostnamen verwenden soll oder ob es automatisch einen Hostnamen über DCHP oder RDNS bezieht.

     > **Note**
     >
     > Wenn Sie einen statischen Hostnamen für Ihr Gateway konfigurieren möchten, müssen Sie in Ihrem DNS-System einen A-Eintrag erstellen, der die IP-Adresse des Gateways auf seinen statischen Hostnamen verweist.

   - Hostnamen-Konfiguration anzeigen — Die lokale Gateway-Konsole zeigt Hostname, Erfassungsmodus, Domain und Active Directory-Bereich für Ihr Amazon EC2 File Gateway an.

Ihre Gateway-VM wird heruntergefahren

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. Sie fahren lokale Gateway-VMs über Ihre Hypervisor-Schnittstelle und Amazon EC2 EC2-Instances mithilfe der Amazon EC2 EC2-Konsole herunter.

> **Important**
>
> Wenn Sie flüchtigen Speicher verwenden und Ihr Amazon-EC2-Gateway anhalten und starten, ist das Gateway dauerhaft offline. Dies geschieht, weil der physische Speicherdatenträger ersetzt wird. Für dieses Problem gibt es keine Lösung. Die einzige

Lösung besteht darin, das Gateway zu löschen und ein neues auf einer neuen EC2-Instance zu aktivieren.

Ersetzen Sie Ihre vorhandenen S3 File Gateway mit einer neuen Instanz

> **Note**
>
> Wenn Sie eine Migration von Storage Gateway AL2 zu AL2023 durchführen, stellen Sie vor Beginn sicher, dass Sie alle Punkte der Pre-migration Checkliste in der Storage-Gateway-Migrationskampagne von AL2 zu AL2023 abgeschlossen haben.

Sie können ein vorhandenes S3 File Gateway durch eine neue Instanz ersetzen, wenn Ihre Daten- und Leistungsanforderungen steigen oder wenn Sie eine AWS Benachrichtigung zur Migration Ihres Gateways erhalten. Möglicherweise müssen Sie dies tun, wenn Sie Ihr Gateway auf eine bessere Host-Plattform oder neuere Amazon EC2 EC2-Instances verschieben oder die zugrunde liegende Serverhardware aktualisieren möchten.

Es gibt zwei Methoden, um ein vorhandenes S3 File Gateway zu ersetzen. In der folgenden Tabelle werden die Vor- und Nachteile der einzelnen Methoden beschrieben. Wählen Sie anhand dieser Informationen die Methode aus, die für Ihre Gateway-Umgebung am besten geeignet ist, und lesen Sie dann die Verfahrensschritte im entsprechenden Abschnitt weiter unten.

> **Note**
>
> Wenn Sie sich bei Ihrer neuen lokalen Storage Gateway Gateway-Konsole anmelden müssen, um eine der beiden Methoden auszuführen, lautet der ursprüngliche Benutzername admin und das temporäre Passwort password.

> **Important**
>
> Verwenden Sie diese Anweisungen nur für die Migration von Gateway-Appliances, auf denen Version 1.x ausgeführt wird. Sie können sie nicht zur Migration von Gateway-Appliances verwenden, auf denen niedrigere Versionen ausgeführt werden.

	Methode 1: Migrieren Sie die Cache-Festplatte und die Gateway-ID zur Ersatzinstanz*	Methode 2: Ersatzinstanz mit leerer Cache-Festplatte und neuer Gateway-ID
Festplattendaten zwischens peichern	Daten auf der Cache-Fes tplatte bleiben erhalten. Diese Methode ist nützlich, wenn Ihr Gateway über eine große Cache-Festplatte verfügt oder wenn Ihre Anwendungen empfindlich auf Verzögeru ngen reagieren, die durch Lesevorgänge außerhalb des Cache verursacht werden.	Daten im Cache werden aus der AWS Cloud herunterg eladen. Diese Methode ist optimal für schreibin tensive Workloads, wenn Ihre Anwendungen die Verzögerung tolerieren können, die durch Lesevorgä nge außerhalb des Cache verursacht wird.
Ausfallzeit	Ihr Gateway wird während des Migrationsprozesses für 1-2 Stunden offline sein.	Fileshares sind immer verfügbar, allerdings kommt es bei Kunden zu kurzen Cutover-Ausfallzeiten, wenn sie während der Umstellun g auf die neue Instanz von einer Dateifreigabe zu einer anderen wechseln. **Note** Das gleichzeitige Schreiben von zwei Dateifreigaben in einen Amazon S3 S3-Bucket wird nicht unterstützt. Daher müssen alle Clients gleichzeitig und nicht schrittweise von einer Freigabe zur anderen

	Methode 1: Migrieren Sie die Cache-Festplatte und die Gateway-ID zur Ersatzinstanz*	Methode 2: Ersatzinstanz mit leerer Cache-Festplatte und neuer Gateway-ID
		neu zugeordnet 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.

	Methode 1: Migrieren Sie die Cache-Festplatte und die Gateway-ID zur Ersatzinstanz*	Methode 2: Ersatzinstanz mit leerer Cache-Festplatte und neuer Gateway-ID
Auswirkungen auf die Kosten	Durch die Aufbewahrung zwischengespeicherter Daten entfällt die Notwendigkeit erneuter Downloads, sodass keine zusätzlichen S3-Kosten anfallen.	Bei dieser Methode können zusätzliche Kosten anfallen, insbesondere wenn ein Datenabruf aus S3 erforderl ich ist. Dieser Ansatz kann auch zu erheblichen Kosten für den Abruf von S3-Daten führen, wenn die von S3-Buckets unterstützten Dateifrei gaben Speicherklassen wie S3 Intelligent-Tiering, S3, S3 Standard-IA One oder Objekte nutzen, die über Zone-IA S3-Lebenszyklusrichtlinien auf GLACIER übertragen wurden. Wenn bei SMB-Dateifreigaben die Root-ACL für die Dateifrei gabe konfiguriert ist, muss sie erneut auf das migrierte Gateway angewendet werden. Durch diese Aktion wird die Einstellung rekursiv auf alle Objekte innerhalb der Dateifrei gabe angewendet, was einige Kosten mit sich bringt.

> **Note**
>
> Die Migration kann nur zwischen Gateways desselben Typs durchgeführt werden. Sie können beispielsweise keine Einstellungen oder Daten von einem FSx File Gateway zu einem S3 File Gateway migrieren.

Methode 1: Migrieren Sie die Cache-Festplatte und die Gateway-ID zur Ersatzinstanz

Um deine zu migrieren S3 File GatewayCache-Festplatte und Gateway-ID für eine Ersatzinstanz:

1. Beenden Sie alle Anwendungen, die auf das bestehende S3 File Gateway schreiben.
2. Gehen Sie wie folgt vor, um das Gateway auf die neueste Version zu aktualisieren

   a. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.

   b. Wählen Sie im Navigationsbereich Gateways und dann das alte S3 File Gateway aus, das Sie migrieren möchten.

   c. Klicken Sie auf Jetzt aktualisieren, falls verfügbar. Wenn nicht, ist Ihr Gateway bereits auf der neuesten Version.
3. Stellen Sie sicher, dass die `CachePercentDirty` Metrik auf der Registerkarte Überwachung für das bestehende S3 File Gateway lautet`0`.
4. Fahren Sie das vorhandene S3 File Gateway herunter, indem Sie die virtuelle Host-Maschine (VM) mithilfe ihrer Hypervisor-Steuerelemente ausschalten.

   Weitere Informationen zum Herunterfahren einer Amazon EC2 EC2-Instance finden Sie unter Beenden und Starten Ihrer Instance im Amazon EC2 EC2-Benutzerhandbuch.

   Weitere Informationen zum Herunterfahren einer KVM, VMware oder VM finden Sie in Ihrer Hyper-V Hypervisor-Dokumentation.
5. Trennen Sie alle Festplatten, einschließlich der Root-Festplatte und der Cache-Festplatten, von der alten Gateway-VM.

> **Note**
>
> Notieren Sie sich die Volume-ID der Stammfestplatte sowie die Gateway-ID, die dieser Stammfestplatte zugeordnet ist. In einem späteren Schritt müssen Sie diese Festplatte vom neuen Storage Gateway Gateway-Hypervisor trennen.

Wenn Sie eine Amazon EC2 EC2-Instance als VM für Ihr S3 File Gateway verwenden, finden Sie weitere Informationen unter Trennen eines Amazon EBS-Volumes von einer Windows-Instance oder Trennen eines Amazon EBS-Volumes von einer Linux-Instance im Amazon EC2 EC2-Benutzerhandbuch.

Informationen zum Trennen von Festplatten von einer KVM, VMware oder Hyper-V VM finden Sie in der Dokumentation zu Ihrem Hypervisor.

6. Erstellen Sie eine neue AWS Storage Gateway Hypervisor-VM-Instanz, aktivieren Sie sie jedoch nicht als Gateway. In einem späteren Schritt nimmt diese neue VM die Identität des alten Gateways an.

   Weitere Informationen zum Erstellen einer neuen Storage Gateway Gateway-Hypervisor-VM finden Sie unter Auswahl einer Hostplattform und Herunterladen der VM.

   > **Note**
   >
   > Fügen Sie keine Cache-Festplatten für die neue VM hinzu. Diese VM verwendet dieselben Cache-Festplatten, die von der alten VM verwendet wurden.

   > **Note**
   >
   > Schließen Sie nach dem Herunterladen der VM den Konsolenassistenten. Fahren Sie zu diesem Zeitpunkt nicht mit der Aktivierung fort.

7. 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 weitere Informationen unter Netzwerkparameter konfigurieren.

Wenn Ihre Gateway-VM einen Socket Secure Version 5 (SOCKS5) -Proxy verwenden muss, um eine Verbindung zum Internet herzustellen, finden Sie weitere Informationen unter Routing Ihres auf EC2 bereitgestellten Gateways über einen HTTP-Proxy.

> **Note**
>
> Sie können dieselbe statische IP-Adresse oder denselben Hostnamen aus der alten Gateway-VM wiederverwenden, um eine Neukonfiguration von NFS- oder SMB-Clients zu vermeiden.

8. Starten Sie die neue Storage Gateway Gateway-VM.
9. Hängen Sie alle Festplatten, die Sie von der alten Gateway-VM getrennt haben, an die neue Gateway-VM an. Dazu gehören die Root-Festplatte und die Cache-Festplatte (n) des alten Gateways. Trennen Sie nicht die eigene Stammfestplatte der neuen Gateway-VM.

   > **Note**
   >
   > Für eine erfolgreiche Migration müssen alle Festplatten unverändert bleiben. Das Ändern der Festplattengröße oder anderer Werte führt zu Inkonsistenzen in den Metadaten, die eine erfolgreiche Migration verhindern.

10. Initiieren Sie den Gateway-Migrationsprozess, indem Sie entweder eine Verbindung zur lokalen Konsole der neuen Gateway-VM herstellen oder Webanfragen an die IP-Adresse der neuen Gateway-VM stellen (unten beschrieben).

    a. Um die lokale Konsole zu verwenden, wählen Sie die Option Migrate Gateway und geben Sie Ihre bestehende Gateway-ID ein, wenn Sie dazu aufgefordert werden. Sie werden aufgefordert, zuvor angewendete Einstellungen auf dem alten Gateway auf das neue Gateway zu kopieren. Sie können wählen, ob Sie sie anwenden oder später manuell konfigurieren möchten. Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole.

    b. Alternativ können Sie den Gateway-Migrationsprozess einleiten, indem Sie mit einer URL, die das folgende Format verwendet, eine Verbindung zur neuen VM herstellen.

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

Sie können dieselbe IP-Adresse, die Sie für die alte Gateway-VM verwendet haben, für die neue Gateway-VM wiederverwenden. Ihre URL sollte ähnlich wie das folgende Beispiel aussehen.

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

Verwenden Sie diese URL in einem Browser oder über die Befehlszeile mit `curl`, um den Migrationsprozess zu starten.

Wenn der Gateway-Migrationsprozess erfolgreich abgeschlossen wurde, wird eine Meldung angezeigt, die die erfolgreiche Migration bestätigt.

11. Warten Sie, bis der Gateway-Status in der AWS Storage Gateway Konsole als Wird ausgeführt angezeigt wird. Je nach verfügbarer Bandbreite kann dies bis zu 10 Minuten dauern.
12. Stoppen Sie die neue Storage Gateway Gateway-VM.
13. Trennen Sie die Stammfestplatte des alten Gateways, deren Volume-ID Sie zuvor notiert haben, vom neuen Gateway.
14. Starten Sie die neue Storage Gateway Gateway-VM.
15. Wenn Ihr Gateway mit einer Active Directory-Domäne verbunden war, treten Sie der Domäne erneut bei. Anweisungen finden Sie unter Verwenden von Active Directory zur Benutzerauthentifizierung.

    > **Note**
    >
    > Sie müssen diesen Schritt auch dann abschließen, wenn der Status von S3 File Gateway angezeigt wird.

16. Wenn Ihr Gateway die SMB Guest Access-Authentifizierungsmethode verwendet hat, muss das Passwort erneut eingegeben werden. Anweisungen finden Sie unter Gastzugriff auf Ihre Dateifreigabe bereitstellen.
17. Vergewissern Sie sich, dass Ihre Shares unter der IP-Adresse der neuen Gateway-VM verfügbar sind, und löschen Sie dann die alte Gateway-VM.

> **Warning**
>
> Wenn ein Gateway gelöscht worden ist, gibt es keine Möglichkeit, es wiederherzustellen.

Weitere Informationen zum Löschen einer Amazon EC2 EC2-Instance finden Sie unter Terminate your Instance im Amazon EC2 EC2-Benutzerhandbuch. Weitere Informationen zum Löschen einer KVM, VMware oder Hyper-V VM finden Sie in der Dokumentation zu Ihrem Hypervisor.

Methode 2: Ersatzinstanz mit leerer Cache-Festplatte und neuer Gateway-ID

Um einen Ersatz einzurichten S3 File Gateway Instanz mit leerer Cache-Festplatte und neuer Gateway-ID:

1. Stoppen Sie alle Anwendungen, die auf das bestehende S3 File Gateway () schreiben. Stellen Sie sicher, dass die `CachePercentDirty` Metrik auf der Registerkarte Überwachung `0` korrekt ist, bevor Sie Dateifreigaben auf dem neuen Gateway einrichten.
2. Verwenden Sie AWS Command Line Interface (AWS CLI), um die Konfigurationsinformationen über Ihr vorhandenes S3 File Gateway und Dateifreigaben zu sammeln und zu speichern. Gehen Sie dazu wie folgt vor:

   a. Speichern Sie die Gateway-Konfigurationsinformationen für das S3 File 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, seine Netzwerkschnittstellen, die konfigurierte Zeitzone und seinen Status (ob das Gateway läuft).

   b. Speichern Sie die Server Message Block (SMB) -Einstellungen des S3 File Gateway Gateway.

```
aws storagegateway describe-smb-settings --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, ob das Gastkennwort festgelegt ist, und die Art der Sicherheitsstrategie.

c. Speichern Sie Dateifreigabeinformationen für jede SMB- und Network File System (NFS) - Dateifreigabe des S3 File Gateway File Gateway:

- 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 über die SMB-Dateifreigabe enthält, wie z. B. Namen, Speicherklasse, Status, IAM-Rolle, Amazon Resource Name (ARN), eine Liste von Clients, die auf das S3 File Gateway zugreifen dürfen, und den Pfad, den der SMB-Client zur Identifizierung des Bereitstellungspunkts verwendet.

- 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 über die NFS-Dateifreigabe enthält, z. B. ihren Namen, ihre Speicherklasse, ihren Status, den ARN der IAM-Rolle, eine Liste von Clients, die auf das S3 File Gateway zugreifen dürfen, und den Pfad, den der NFS-Client zur Identifizierung des Bereitstellungspunkts verwendet.

3. Erstellen Sie ein neues S3 File Gateway mit den gleichen Einstellungen und der gleichen Konfiguration wie das alte Gateway. Falls erforderlich, beziehen Sie sich auf die Informationen, die Sie in Schritt 2 gespeichert haben.
4. Erstellen Sie neue Dateifreigaben für das neue Gateway mit denselben Einstellungen und derselben Konfiguration wie die Dateifreigaben, die auf dem alten Gateway konfiguriert wurden. Schlagen Sie gegebenenfalls in den Informationen nach, die Sie in Schritt 2 gespeichert haben.

> **Note**
>
> Sie können jetzt Dateifreigabekonfigurationen zwischen Gateways kopieren. Weitere Informationen finden Sie unter Kopieren einer Dateifreigabe.

5. Vergewissern Sie sich, dass Ihr neues Gateway ordnungsgemäß funktioniert, und remap/cut übertragen Sie dann Ihre Clients von den alten Dateifreigaben auf die neuen Dateifreigaben, und zwar so, wie es für Ihre Umgebung am besten geeignet ist.
6. Vergewissern Sie sich, dass Ihr neues Gateway ordnungsgemäß funktioniert, und löschen Sie dann das alte Gateway aus der Storage Gateway Gateway-Konsole.

> **Important**
>
> Bevor Sie ein S3 File Gateway löschen, stellen Sie sicher, dass derzeit keine Anwendungen in den Cache dieses Gateways schreiben. Wenn Sie ein Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten.

> **Warning**
>
> Wenn ein Gateway gelöscht worden ist, gibt es keine Möglichkeit, es wiederherzustellen.

7. Löschen Sie die alte Gateway-VM oder Amazon EC2 EC2-Instance.

Löschen Sie Ihr Gateway und entfernen Sie die zugehörigen 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 Management Console angezeigt und seine werden 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 wird, führen Sie jedoch spezifische Anweisungen zum Entfernen zugehöriger Ressourcen aus.

Sie können ein Gateway mithilfe der Storage-Gateway-Konsole oder programmgesteuert löschen. Im Folgenden finden Sie Informationen zum Löschen eines Gateways mit der Storage-Gateway-Konsole. Informationen zum programmgesteuerten Löschen eines Gateways finden Sie unter AWS Storage Gateway API-Referenz..

Löschen eines Gateways mithilfe der Storage-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 wird, 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-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. Um die VM zu entfernen, verwenden Sie den VMware vSphere-Client, Microsoft Hyper-V Manager oder den Linux Kernel-based Virtual Machine (KVM) -Client, um eine Verbindung zum 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-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie Gateways und anschließend ein oder mehrere Gateways zum Löschen aus.
3. Wählen Sie für Aktionen die Option Gateway löschen aus. Das Bestätigungsdialogfeld wird angezeigt.

> **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.

4. Vergewissern Sie sich, dass Sie die angegebenen Gateways löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen aus.
5. (Optional) Wenn Sie Feedback zu Ihrem gelöschten Gateway geben möchten, füllen Sie das Feedback-Dialogfeld aus und wählen Sie dann Absenden. Wählen Sie andernfalls Überspringen aus.

> **Important**
>
> Sie zahlen keine Softwaregebühren mehr, nachdem Sie ein Gateway gelöscht haben, aber Ressourcen wie Amazon S3 S3-Bucket und Amazon EC2 EC2-Instances bleiben bestehen. Sie können die Amazon EC2 EC2-Gateway-Instance entfernen, nachdem das File-Gateway entfernt wurde. Wenn Sie die mit den Dateifreigaben verknüpften Daten in Amazon S3 S3-Buckets nicht benötigen, können Sie Ihre Amazon S3 S3-Buckets entfernen. Anweisungen finden Sie unter Löschen Ihres Buckets.

Leistung und Optimierung

In diesem Abschnitt werden Anleitungen und bewährte Methoden zur Optimierung der File Gateway-Leistung beschrieben.

Themen

Grundlegende Hinweise zur Leistung für S3 File Gateway FSx

In diesem Abschnitt finden Sie Anleitungen zur Bereitstellung von Hardware für Ihre S3 File Gateway-VM. Die in der Tabelle aufgeführten Instanzkonfigurationen 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.

> **Note**
>
> Wir raten davon ab, flüchtigen Speicher zu verwenden. Weitere Informationen zur Verwendung des flüchtigen Speichers finden Sie unter Verwendung von kurzlebigem Speicher mit EC2-Gateways.
>
> Wenn Sie für Amazon EC2 EC2-Instances mehr als 5 Millionen Objekte in Ihrem S3-Bucket haben und ein SSD-Volume für allgemeine Zwecke verwenden, ist für eine akzeptable Leistung Ihres Gateways beim Start ein EBS-Root-Volume von mindestens 350 GiB erforderlich. Weitere Informationen zum Erhöhen der Volume-Größe finden Sie unter Ändern eines EBS-Volumes mit Elastic Volumes (Konsole).
>
> Die empfohlene Größenbeschränkung für einzelne Verzeichnisse in den , die Sie mit File Gateway verbinden, beträgt 10.000 Dateien pro Verzeichnis. Sie können File Gateway mit Verzeichnissen verwenden, die mehr als 10.000 Dateien enthalten, aber die Leistung kann beeinträchtigt werden.

In den folgenden Tabellen handelt es sich bei Cache-Treffer-Lesevorgängen um Lesevorgänge aus den Dateifreigaben, die über den Cache bereitgestellt werden. Cache-Fehllesevorgänge sind Lesevorgänge aus den Dateifreigaben, die von Amazon S3 bereitgestellt werden.

Die folgenden Tabellen zeigen Beispielkonfigurationen für S3 File Gateway.

Leistung von S3 File Gateway auf Linux-Clients

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz beim Cache-Treffer	Durchsatz bei fehlendem Lesen im Cache
Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPS Cache-Festplatte: 512 GiB Cache, io1, 1.500 bereitgestellte IOPS Mindestnetzwerkleistung: 10 Gbit/s CPU: 16 vCPU | RAM: 32 GB Das NFS-Protokoll wird für Linux empfohlen	NFSv3 - 1 Thread	110 MiB/sec (0,92 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	310 MiB/sec (2,6 Gbit/s)
	NFSv3 - 8 Fäden	160 MiB/sec (1,3 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	335 MiB/sec (2,8 Gbit/s)
	NFSv4 - 1 Faden	130 MiB/sec (1,1 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	295 MiB/sec (2,5 Gbit/s)
	NFSv4 - 8 Fäden	160 MiB/sec (1,3 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	335 MiB/sec (2,8 Gbit/s)
	SMBV3 - 1 Faden	115 MiB/sec (1,0 Gbit/s)	325 MiB/sec (2,7 Gbit/s)	255 MiB/sec (2,1 Gbit/s)
	SMBV3 - 8 Fäden	190 MiB/sec (1,6 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	335 MiB/sec (2,8 Gbit/s)
Storage Gateway-Hardware-Appliance	NFSv3 - 1 Faden	265 MiB/sec (2,2 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	310 MiB/sec (2,6 Gbit/s)
	NFSv3 - 8 Fäden	385 MiB/sec (3,1 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	335 MiB/sec (2,8 Gbit/s)

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz beim Cache-Treffer	Durchsatz bei fehlendem Lesen im Cache
Mindestnetzwerkleistung: 10 Gbit/s	NFSv4 - 1 Faden	310 MiB/sec (2,6 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	295 MiB/sec (2,5 Gbit/s)
	NFSv4 - 8 Fäden	385 MiB/sec (3,1 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	335 MiB/sec (2,8 Gbit/s)
	SMBV3 - 1 Faden	275 MiB/sec (2,4 Gbit/s)	325 MiB/sec (2,7 Gbit/s)	255 MiB/sec (2,1 Gbit/s)
	SMBV3 - 8 Fäden	455 MiB/sec (3,8 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	335 MiB/sec (2,8 Gbit/s)
Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPS Cache-Festplatte: 4 x 2 TB NVME-Cache-Festplatten Mindestnetzwerkleistung: 10 Gbit/s PROZESSOR: 32 vCPU | Arbeitsspeicher: 244 GB Das NFS-Protokoll wird für Linux empfohlen	NFSv3 - 1 Thread	300 MiB/sec (2,5 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	325 MiB/sec (2,7 Gbit/s)
	NFSv3 - 8 Fäden	585 MiB/sec (4,9 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	580 MiB/sec (4,8 Gbit/s)
	NFSv4 - 1 Faden	355 MiB/sec (3,0 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	340 MiB/sec (2,9 Gbit/s)
	NFSv4 - 8 Fäden	575 MiB/sec (4,8 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	575 MiB/sec (4,8 Gbit/s)
	SMBV3 - 1 Faden	230 MiB/sec (1,9 Gbit/s)	325 MiB/sec (2,7 Gbit/s)	245 MiB/sec (2,0 Gbit/s)
	SMBV3 - 8 Fäden	585 MiB/sec (4,9 Gbit/s)	590 MiB/sec (4,9 Gbit/s)	580 MiB/sec (4,8 Gbit/s)

Leistung von File Gateway auf Windows-Clients

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz beim Cache-Treffer	Durchsatz bei fehlendem Lesen im Cache
Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPS Cache-Festplatte: 512 GiB Cache, io1, 1.500 bereitgestellte IOPS Mindestnetzwerkleistung: 10 Gbit/s CPU: 16 vCPU | RAM: 32 GB Das SMB-Protokoll wird für Windows empfohlen	SMBV3 - 1 Thread	150 MiB/sec (1,3 Gbit/s)	180 MiB/sec (1,5 Gbit/s)	20 MiB/sec (0,2 Gbit/s)
	SMBV3 - 8 Fäden	190 MiB/sec (1,6 Gbit/s)	335 MiB/sec (2,8 Gbit/s)	195 MiB/sec (1,6 Gbit/s)
	NFSv3 - 1 Faden	95 MiB/sec (0,8 Gbit/s)	130 MiB/sec (1,1 Gbit/s)	20 MiB/sec (0,2 Gbit/s)
	NFSv3 - 8 Fäden	190 MiB/sec (1,6 Gbit/s)	330 MiB/sec (2,8 Gbit/s)	190 MiB/sec (1,6 Gbit/s)
Storage Gateway-Hardware-Appliance Mindestnetzwerkleistung: 10 Gbit/s	SMBV3 - 1 Faden	230 MiB/sec (1,9 Gbit/s)	255 MiB/sec (2,1 Gbit/s)	20 MiB/sec (0,2 Gbit/s)
	SMBV3 - 8 Fäden	835 MiB/sec (7,0 Gbit/s)	475 MiB/sec (4,0 Gbit/s)	195 MiB/sec (1,6 Gbit/s)
	NFSv3 - 1 Faden	135 MiB/sec (1,1 Gbit/s)	185 MiB/sec (1,6 Gbit/s)	20 MiB/sec (0,2 Gbit/s)
	NFSv3 - 8 Fäden	545 MiB/sec (4,6 Gbit/s)	470 MiB/sec (4,0 Gbit/s)	190 MiB/sec (1,6 Gbit/s)

Beispielkonfigurationen	Protocol (Protokoll)	Schreibdurchsatz (Dateigrößen 1 GB)	Lesedurchsatz beim Cache-Treffer	Durchsatz bei fehlendem Lesen im Cache
Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPS Cache-Festplatte: 4 x 2 TB NVME-Cache-Festplatten Mindestnetzwerkleistung: 10 Gbit/s PROZESSOR: 32 vCPU | Arbeitsspeicher: 244 GB Das SMB-Protokoll wird für Windows empfohlen	SMBV3 - 1 Thread	230 MiB/sec (1,9 Gbit/s)	265 MiB/sec (2,2 Gbit/s)	30 MiB/sec (0,3 Gbit/s)
	SMBV3 - 8 Fäden	835 MiB/sec (7,0 Gbit/s)	780 MiB/sec (6,5 Gbit/s)	250 MiB/sec (2,1 Gbit/s)
	NFSv3 - 1 Faden	135 MiB/sec (1.1). Gbit/s)	220 MiB/sec (1,8 Gbit/s)	30 MiB/sec (0,3 Gbit/s)
	NFSv3 - 8 Fäden	545 MiB/sec (4,6 Gbit/s)	570 MiB/sec (4,8 Gbit/s)	240 MiB/sec (2,0 Gbit/s)

> **Note**
>
> Die Leistung hängt von der Konfiguration Ihrer Hostplattform und der Netzwerkbandbreite ab. Die Schreibdurchsatzleistung nimmt mit der Dateigröße ab, wobei der höchste erreichbare Durchsatz für kleine Dateien (weniger als 32 MiB) bei 16 Dateien pro Sekunde liegt.

Hinweise zur Leistung von Gateways mit mehreren Dateifreigaben

Amazon S3 File Gateway unterstützt das Anhängen von bis zu 50 Dateifreigaben an eine einzelne Storage Gateway Gateway-Appliance. Durch das Hinzufügen mehrerer Dateifreigaben pro Gateway

können Sie mehr Benutzer und Workloads unterstützen und gleichzeitig weniger Gateways und virtuelle Hardwareressourcen verwalten. Neben anderen Faktoren kann sich die Anzahl der von einem Gateway verwalteten Dateifreigaben auf die Leistung dieses Gateways auswirken. In diesem Abschnitt wird beschrieben, wie sich die Gateway-Leistung je nach Anzahl der angehängten Dateifreigaben voraussichtlich ändern wird, und es werden virtuelle Hardwarekonfigurationen empfohlen, um die Leistung für Gateways zu optimieren, die mehrere Shares verwalten.

Im Allgemeinen kann die Erhöhung der Anzahl der Dateifreigaben, die von einem einzelnen Storage Gateway verwaltet werden, die folgenden Konsequenzen haben:

- Für den Neustart des Gateways ist mehr Zeit erforderlich.
- Bessere Nutzung virtueller Hardwareressourcen wie vCPU und RAM.
- Verminderte Leistung bei Daten- und Metadatenoperationen, wenn die virtuellen Hardwareressourcen überlastet sind.

In der folgenden Tabelle sind empfohlene virtuelle Hardwarekonfigurationen für Gateways aufgeführt, die mehrere Dateifreigaben verwalten:

Dateifreigaben pro Gateway	Empfohlene Gateway-Kapazitätseinstellung	Empfohlene vCPU-Kerne	Empfohlener Arbeitsspeicher	Empfohlene Größe der Root-Festplatte			
1-10	Small	4 (EC2-Instance-Typ m4.xlarge oder höher)	16 GiB	80 GiB			
10-20	Mittel	8 (EC2-Instance-Typ m4.2xlarg	32 GiB	160 GiB			

Dateifreigaben pro Gateway	Empfohlene Gateway-Kapazitätseinstellung	Empfohlene vCPU-Kerne	Empfohlener Arbeitsspeicher	Empfohlene Größe der Root-Festplatte			
		e oder höher)					
20+	Large (Groß)	16 (EC2-Instance-Typ m4.4xlarge oder höher)	64 GiB	240 GiB			

Zusätzlich zu den oben empfohlenen virtuellen Hardwarekonfigurationen empfehlen wir die folgenden bewährten Methoden für die Konfiguration und Wartung von Storage Gateway Gateway-Geräten, die mehrere Dateifreigaben verwalten:

- Beachten Sie, dass das Verhältnis zwischen der Anzahl der Dateifreigaben und der Nachfrage nach der virtuellen Hardware des Gateways nicht unbedingt linear ist. Einige Dateifreigaben erzeugen möglicherweise einen höheren Durchsatz und damit einen höheren Hardwarebedarf als andere. Die Empfehlungen in der obigen Tabelle basieren auf maximalen Hardwarekapazitäten und verschiedenen Durchsatzraten für Dateifreigaben.
- Wenn Sie feststellen, dass das Hinzufügen mehrerer Dateifreigaben zu einem einzelnen Gateway die Leistung beeinträchtigt, sollten Sie erwägen, die aktivsten Dateifreigaben auf andere Gateways zu verschieben. Insbesondere, wenn eine Dateifreigabe für eine very-high-throughput Anwendung verwendet wird, sollten Sie erwägen, ein separates Gateway für diese Dateifreigabe einzurichten.
- Es wird nicht empfohlen, ein Gateway für mehrere Anwendungen mit hohem Durchsatz und ein anderes für mehrere Anwendungen mit niedrigem Durchsatz zu konfigurieren. Versuchen Sie stattdessen, Dateifreigaben mit hohem und niedrigem Durchsatz gleichmäßig auf die Gateways zu verteilen, um die Hardwaresättigung auszugleichen. Verwenden Sie die `WriteBytes` Metriken

`ReadBytes` und, um den Durchsatz Ihrer Dateifreigaben zu messen. Weitere Informationen finden Sie unter Grundlegendes zu Metriken zur Dateifreigabe.

Maximierung des S3 File Gateway-Durchsatzes

In den folgenden Abschnitten werden bewährte Methoden zur Maximierung des Durchsatzes zwischen Ihren NFS- und SMB-Clients, S3 File Gateway und Amazon S3 beschrieben. Die in den einzelnen Abschnitten enthaltenen Anleitungen tragen schrittweise zur Verbesserung des Gesamtdurchsatzes bei. Obwohl keine dieser Empfehlungen erforderlich ist und sie nicht voneinander abhängig sind, wurden sie auf logische Weise ausgewählt und angeordnet, sodass sie zum Testen und Optimieren von S3 File Gateway-Implementierungen Support verwendet werden. Denken Sie beim Implementieren und Testen dieser Vorschläge daran, dass jede S3 File Gateway-Bereitstellung einzigartig ist, sodass Ihre Ergebnisse variieren können.

S3 File Gateway bietet eine Dateischnittstelle zum Speichern und Abrufen von Amazon S3 S3-Objekten mithilfe der branchenüblichen NFS- oder SMB-Dateiprotokolle mit einer systemeigenen 1:1 -Zuordnung zwischen Datei und Objekt. Sie stellen S3 File Gateway als virtuelle Maschine entweder lokal in Ihrer VMware Microsoft Hyper-V- oder Linux-KVM-Umgebung oder in der AWS Cloud als Amazon EC2 EC2-Instanz bereit. S3 File Gateway ist nicht als vollständiger NAS-Ersatz für Unternehmen konzipiert. S3 File Gateway emuliert ein Dateisystem, aber es ist kein Dateisystem. Die Verwendung von Amazon S3 als dauerhaftem Back-End-Speicher erzeugt zusätzlichen Overhead bei jedem I/O Vorgang, sodass die Bewertung der Leistung von S3 File Gateway mit einem vorhandenen NAS oder Dateiserver kein gleichwertiger Vergleich ist.

Stellen Sie Ihr Gateway am selben Standort wie Ihre Kunden bereit

Wir empfehlen, Ihre virtuelle S3 File Gateway-Appliance an einem physischen Standort mit möglichst geringer Netzwerklatenz zwischen ihr und Ihren NFS- oder SMB-Clients bereitzustellen. Beachten Sie bei der Auswahl eines Standorts für Ihr Gateway Folgendes:

- Eine geringere Netzwerklatenz bis zum Gateway kann dazu beitragen, die Leistung von NFS- oder SMB-Clients zu verbessern.
- S3 File Gateway ist so konzipiert, dass es eine höhere Netzwerklatenz zwischen dem Gateway und Amazon S3 toleriert als zwischen dem Gateway und den Clients.
- Für S3 File Gateway-Instances, die in Amazon EC2 bereitgestellt werden, empfehlen wir, das Gateway und die NFS- oder SMB-Clients in derselben Platzierungsgruppe zu belassen. Weitere

Informationen finden Sie unter Platzierungsgruppen für Ihre Amazon EC2 EC2-Instances im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Reduzieren Sie Engpässe, die durch langsame Festplatten verursacht werden

Wir empfehlen, die `IoWaitPercent` CloudWatch Metrik zu überwachen, um Leistungsengpässe zu identifizieren, die auf langsame Speicherfestplatten auf Ihrem S3 File Gateway zurückzuführen sein können. Wenn Sie versuchen, festplattenbedingte Leistungsprobleme zu optimieren, sollten Sie Folgendes berücksichtigen:

- `IoWaitPercent`gibt an, wie lange die CPU in Prozent auf eine Antwort von den Root- oder Cache-Festplatten wartet.
- Wenn der Wert höher als 5-10% `IoWaitPercent` ist, deutet dies in der Regel auf einen Gateway-Leistungsengpass hin, der durch Festplatten mit schlechter Leistung verursacht wird. Diese Metrik sollte so nahe wie möglich bei 0% liegen — was bedeutet, dass das Gateway nie auf die Festplatte wartet —, was zur Optimierung der CPU-Ressourcen beiträgt.
- Sie können dies `IoWaitPercent` auf der Registerkarte Überwachung der Storage Gateway Gateway-Konsole überprüfen oder empfohlene CloudWatch Alarme so konfigurieren, dass Sie automatisch benachrichtigt werden, wenn die Metrik einen bestimmten Schwellenwert überschreitet. Weitere Informationen finden Sie unter Empfohlene CloudWatch Alarme für Ihr Gateway erstellen.
- Zur Minimierung empfehlen wir, für die Root- und Cache-Festplatten Ihres Gateways entweder eine SSD NVMe oder eine SSD zu verwenden`IoWaitPercent`.

Passen Sie die Ressourcenzuweisung der virtuellen Maschine für CPU-, RAM- und Cache-Festplatten an

Wenn Sie versuchen, den Durchsatz für Ihr S3 File Gateway zu optimieren, ist es wichtig, der Gateway-VM ausreichend Ressourcen zuzuweisen, einschließlich CPU-, RAM- und Cache-Festplatten. Die Mindestanforderungen an virtuelle Ressourcen von 4 CPUs, 16 GB RAM und 150 GB Cache-Speicher sind in der Regel nur für kleinere Workloads geeignet. Bei der Zuweisung virtueller Ressourcen für größere Workloads empfehlen wir Folgendes:

- Erhöhen Sie die zugewiesene Anzahl auf 16 CPUs bis 48, abhängig von der typischen CPU-Auslastung, die von Ihrem S3 File Gateway generiert wird. Sie können die CPU-Auslastung mithilfe der `UserCpuPercent` Metrik überwachen. Weitere Informationen finden Sie unter Grundlegendes zu Gateway-Metriken.
- Erhöhen Sie den zugewiesenen Arbeitsspeicher auf 32 bis 64 GB.

> **Note**
>
> S3 File Gateway kann nicht mehr als 64 GB RAM verwenden.

- Verwenden Sie NVMe oder SSD für Root-Festplatten und Cache-Festplatten, und passen Sie die Größe Ihrer Cache-Festplatten so an, dass sie dem Datenbestand entsprechen, den Sie in das Gateway schreiben möchten. Weitere Informationen finden Sie unter Best Practices zur Cache-Dimensionierung von S3 File Gateway auf dem offiziellen Amazon Web Services YouTube Services-Kanal.
- Fügen Sie dem Gateway mindestens 4 virtuelle Cache-Festplatten hinzu, anstatt eine einzige große Festplatte zu verwenden. Mehrere virtuelle Laufwerke können die Leistung verbessern, selbst wenn sie dieselbe zugrunde liegende physische Festplatte verwenden. Die Verbesserungen sind jedoch in der Regel größer, wenn sich die virtuellen Laufwerke auf verschiedenen zugrunde liegenden physischen Festplatten befinden.

  Wenn Sie beispielsweise 12 TB Cache bereitstellen möchten, können Sie eine der folgenden Konfigurationen verwenden:

  - 4 x 3 TB Cache-Festplatten
  - 8 x 1,5 TB Cache-Festplatten
  - 12 x 1-TB-Cache-Festplatten

  Zusätzlich zur Leistung ermöglicht dies im Laufe der Zeit eine effizientere Verwaltung der virtuellen Maschine. Wenn sich Ihre Arbeitslast ändert, können Sie die Anzahl der Cache-Festplatten und Ihre gesamte Cachekapazität schrittweise erhöhen und gleichzeitig die ursprüngliche Größe jedes einzelnen virtuellen Laufwerks beibehalten, um die Gateway-Integrität zu wahren.

  Weitere Informationen finden Sie unter Festlegung der Größe des lokalen Festplattenspeichers.

Beachten Sie bei der Bereitstellung von S3 File Gateway als Amazon EC2 EC2-Instance Folgendes:

- Der von Ihnen gewählte Instance-Typ kann sich erheblich auf die Gateway-Leistung auswirken. Amazon EC2 bietet umfassende Flexibilität bei der Anpassung der Ressourcenzuweisung für Ihre S3 File Gateway-Instance.
- Die empfohlenen Amazon EC2 EC2-Instance-Typen für S3 File Gateway finden Sie unter Anforderungen für Amazon EC2 EC2-Instance-Typen.
- Sie können den Amazon EC2 EC2-Instance-Typ ändern, der ein aktives S3 File Gateway hostet. Auf diese Weise können Sie die Amazon EC2 EC2-Hardwaregenerierung und die Ressourcenzuweisung einfach anpassen, um ein ideales price-to-performance Verhältnis zu finden. Gehen Sie in der Amazon EC2 EC2-Konsole wie folgt vor, um den Instance-Typ zu ändern:

  1. Stoppen Sie die Amazon EC2 EC2-Instance.
  2. Ändern Sie den Amazon EC2 EC2-Instance-Typ.
  3. Schalten Sie die Amazon EC2 EC2-Instance ein.

  > **Note**
  >
  > Durch das Stoppen einer Instance, die ein S3 File Gateway hostet, wird der Dateifreigabezugriff vorübergehend unterbrochen. Stellen Sie sicher, dass Sie bei Bedarf ein Wartungsfenster einplanen.

- Das price-to-performance Verhältnis einer Amazon EC2 EC2-Instance bezieht sich darauf, wie viel Rechenleistung Sie für den Preis erhalten, den Sie zahlen. In der Regel bieten Amazon EC2 EC2-Instances der neueren Generation das beste price-to-performance Verhältnis mit neuerer Hardware und verbesserter Leistung zu relativ geringeren Kosten im Vergleich zu älteren Generationen. Faktoren wie Instance-Typ, Region und Nutzungsmuster wirken sich auf dieses Verhältnis aus. Daher ist es wichtig, die richtige Instance für Ihren spezifischen Workload auszuwählen, um die Kosteneffizienz zu optimieren.

Passen Sie die SMB-Sicherheitsstufe an

Das SMBv3 Protokoll ermöglicht sowohl SMB-Signaturen als auch SMB-Verschlüsselung, was einige Kompromisse in Bezug auf Leistung und Sicherheit mit sich bringt. Um den Durchsatz zu optimieren, können Sie die SMB-Sicherheitsstufe Ihres Gateways anpassen, um festzulegen, welche dieser Sicherheitsfunktionen für Client-Verbindungen durchgesetzt werden. Weitere Informationen finden Sie unter Einstellen einer Sicherheitsstufe für Ihr Gateway.

Beachten Sie bei der Anpassung der SMB-Sicherheitsstufe Folgendes:

- Die Standardsicherheitsstufe für S3 File Gateway ist Enforce encryption. Diese Einstellung erzwingt sowohl die Verschlüsselung als auch die Signierung für SMB-Clientverbindungen zu Gateway-Dateifreigaben, was bedeutet, dass der gesamte Datenverkehr vom Client zum Gateway verschlüsselt wird. Diese Einstellung wirkt sich nicht auf den Datenverkehr vom Gateway zum aus AWS, der immer verschlüsselt ist.

  Das Gateway begrenzt jede verschlüsselte Client-Verbindung auf eine einzelne vCPU. Wenn Sie beispielsweise nur einen verschlüsselten Client haben, ist dieser Client auf nur 1 vCPU beschränkt, auch wenn dem Gateway 4 oder mehr v zugewiesen CPUs sind. Aus diesem Grund liegt der Durchsatz für verschlüsselte Verbindungen von einem einzelnen Client zum S3 File Gateway in der Regel zwischen 40 und 60 MB/s.
- Wenn Ihre Sicherheitsanforderungen eine entspanntere Haltung zulassen, können Sie die Sicherheitsstufe auf „Vom Kunden ausgehandelt“ ändern. Dadurch wird die SMB-Verschlüsselung deaktiviert und nur die SMB-Signatur erzwungen. Mit dieser Einstellung können Client-Verbindungen zum Gateway mehrere V verwendenCPUs, was in der Regel zu einer erhöhten Durchsatzleistung führt.

> **Note**
>
> Nachdem Sie die SMB-Sicherheitsstufe für Ihr S3 File Gateway geändert haben, müssen Sie warten, bis sich der Dateifreigabestatus in der Storage Gateway Gateway-Konsole von Aktuell auf Verfügbar ändert, und dann Ihre SMB-Clients trennen und erneut verbinden, damit die neue Einstellung wirksam wird.

Verwenden Sie mehrere Threads und Clients, um Schreibvorgänge zu parallelisieren

Es ist schwierig, mit einem S3 File Gateway, das jeweils nur einen NFS- oder SMB-Client verwendet, um jeweils eine Datei zu schreiben, eine maximale Durchsatzleistung zu erreichen, da sequentielles Schreiben von einem einzelnen Client aus ein Single-Thread-Vorgang ist. Stattdessen empfehlen wir, mehrere Threads von jedem NFS- oder SMB-Client zu verwenden, um mehrere Dateien parallel zu schreiben, und mehrere NFS- oder SMB-Clients gleichzeitig auf Ihrem S3 File Gateway zu verwenden, um den Gateway-Durchsatz zu maximieren.

Die Verwendung mehrerer Threads kann die Leistung erheblich verbessern. Die Verwendung von mehr Threads erfordert jedoch mehr Systemressourcen, was sich negativ auf die Leistung

auswirken kann, wenn das Gateway nicht so dimensioniert ist, dass es der erhöhten Last gerecht wird. In einer typischen Bereitstellung können Sie mit einer besseren Durchsatzleistung rechnen, wenn Sie mehr Threads und Clients hinzufügen, bis Sie die maximalen Hardware- und Bandbreitenbeschränkungen für Ihr Gateway erreicht haben. Wir empfehlen, mit verschiedenen Thread-Zahlen zu experimentieren, um das optimale Gleichgewicht zwischen Geschwindigkeit und Systemressourcennutzung für Ihre spezifische Hardware- und Netzwerkkonfiguration zu finden.

Beachten Sie die folgenden Informationen zu gängigen Tools, mit denen Sie Ihre Thread- und Client-Konfiguration testen können:

- Sie können die Schreibleistung mehrerer Threads testen, indem Sie Tools wie Robocopy verwenden, um eine Reihe von Dateien auf eine Dateifreigabe auf Ihrem Gateway zu kopieren. Standardmäßig verwendet Robocopy beim Kopieren von Dateien 8 Threads, Sie können jedoch bis zu 128 Threads angeben.

  Um mehrere Threads mit Robocopy zu verwenden, fügen Sie Ihrem Befehl den `/MT:n` Schalter hinzu, der die Anzahl der Threads angibt, die Sie verwenden möchten. n Beispiel:

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

  Dieser Befehl verwendet 64 Threads für den Kopiervorgang.

  > **Note**
  >
  > Es wird nicht empfohlen, Windows Explorer zum Ziehen und Ablegen von Dateien zu verwenden, wenn Sie den maximalen Durchsatz testen, da diese Methode auf einen einzelnen Thread beschränkt ist und die Dateien sequentiell kopiert.

  Weitere Informationen finden Sie unter Robocopy auf der Microsoft Learn-Website.

- Sie können Tests auch mit gängigen Speicher-Benchmarking-Tools wie DISKSPD oder FIO durchführen. Diese Tools bieten Optionen, mit denen Sie die Anzahl der Threads, die I/O-Tiefe und andere Parameter an Ihre spezifischen Workload-Anforderungen anpassen können.

  DiskSpd ermöglicht es Ihnen, die Anzahl der Threads mithilfe des `-t` Parameters zu steuern. Beispiel:

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

Dieser Beispielbefehl macht Folgendes:

- Erzeugt eine 10-GB-Testdatei () `-c1G`
- Läuft 300 Sekunden lang () `-d300`
- Führt einen I/O Zufallstest mit 50% Lesevorgängen und 50% Schreibvorgängen durch (`-r -w50`)
- Verwendet 64 Threads (`-t64`)
- Setzt die Warteschlangentiefe auf 32 pro Thread (`-o32`)
- Verwendet eine Blockgröße von 1 MB () `-b1M`
- Deaktiviert das Hardware- und Software-Caching () `-h -L`

Weitere Informationen finden Sie unter Verwenden von DISKSPD zum Testen der Workload-Speicherleistung auf der Microsoft Learn-Website.

- FIO verwendet den `numjobs` Parameter, um die Anzahl der parallel Threads zu steuern. Beispiel:

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

Dieser Beispielbefehl macht Folgendes:

- Führt einen I/O Zufallstest durch (`--rw=randrw`)
- Führt 70% Lese- und 30% Schreibvorgänge durch (`--rwmixread=70`)
- Verwendet eine Blockgröße von 1 MB () `--bs=1M`
- Setzt die I/O Tiefe auf 64 () `--iodepth=64`
- Testet mit einer 10-GB-Datei (`--size=10G`)
- Läuft 5 Minuten (`--runtime=300`)
- Erzeugt 64 parallel Jobs (Threads) (`--numjobs=64`)
- Verwendet eine asynchrone I/O Engine () `--ioengine=libaio`
- Gruppiert Ergebnisse zur einfacheren Analyse () `--group_reporting`

Weitere Informationen finden Sie in der Manpage fio Linux.

-

Schalten Sie die automatische Cache-Aktualisierung aus

Die automatische Cache-Aktualisierungsfunktion ermöglicht es Ihrem S3 File Gateway, seine Metadaten automatisch zu aktualisieren. Dies kann dazu beitragen, alle Änderungen zu erfassen, die Benutzer oder Anwendungen an Ihrem Dateisatz vornehmen, indem sie direkt in den Amazon S3 S3-Bucket schreiben und nicht über das Gateway. Weitere Informationen finden Sie unter Aktualisieren des Amazon S3 S3-Bucket-Objekt-Caches.

Um den Gateway-Durchsatz zu optimieren, empfehlen wir, diese Funktion in Bereitstellungen zu deaktivieren, in denen alle Lese- und Schreibvorgänge in den Amazon S3 S3-Bucket über Ihr S3 File Gateway ausgeführt werden.

Beachten Sie bei der Konfiguration der automatischen Cache-Aktualisierung Folgendes:

- Wenn Sie die automatische Cache-Aktualisierung verwenden müssen, weil Benutzer oder Anwendungen in Ihrer Bereitstellung gelegentlich direkt in Amazon S3 schreiben, empfehlen wir, das längstmögliche Zeitintervall zwischen den Aktualisierungen zu konfigurieren, das für Ihre Geschäftsanforderungen immer noch praktikabel ist. Ein längeres Cache-Aktualisierungsintervall trägt dazu bei, die Anzahl der Metadatenoperationen zu reduzieren, die das Gateway beim Durchsuchen von Verzeichnissen oder beim Ändern von Dateien ausführen muss.

  Beispiel: Stellen Sie die automatische Cache-Aktualisierung auf 24 Stunden statt auf 5 Minuten ein, wenn dies für Ihre Arbeitslast tolerierbar ist.
- Das Mindestzeitintervall beträgt 5 Minuten. Das maximale Intervall beträgt 30 Tage.
- Wenn Sie sich dafür entscheiden, ein sehr kurzes Cache-Aktualisierungsintervall festzulegen, empfehlen wir, das Durchsuchen von Verzeichnissen für Ihre NFS- und SMB-Clients zu testen. Die Zeit, die zum Aktualisieren des Gateway-Cache benötigt wird, kann je nach Anzahl der Dateien und Unterverzeichnisse in Ihrem Amazon S3-Bucket erheblich länger dauern.

Erhöhen Sie die Anzahl der Amazon S3 S3-Uploader-Threads

Standardmäßig öffnet S3 File Gateway 8 Threads für den Amazon S3 S3-Datenupload, was ausreichend Upload-Kapazität für die meisten typischen Bereitstellungen bietet. Es ist jedoch möglich, dass ein Gateway Daten von NFS- und SMB-Clients mit einer höheren Geschwindigkeit empfängt, als es mit der standardmäßigen 8-Thread-Kapazität auf Amazon S3 hochladen kann, was dazu führen kann, dass der lokale Cache sein Speicherlimit erreicht.

Unter bestimmten Umständen Support kann die Anzahl der Amazon S3 S3-Upload-Thread-Pools für Ihr Gateway von 8 auf 40 erhöht werden, sodass mehr Daten parallel hochgeladen werden können. Abhängig von der Bandbreite und anderen Faktoren, die für Ihre Bereitstellung spezifisch sind, kann dies die Upload-Leistung erheblich steigern und dazu beitragen, den zur Unterstützung Ihrer Arbeitslast benötigten Cache-Speicher zu reduzieren.

Wir empfehlen, die `CachePercentDirty` CloudWatch Metrik zu verwenden, um die Menge der auf den lokalen Gateway-Cache-Festplatten gespeicherten Daten zu überwachen, die noch nicht auf Amazon S3 hochgeladen wurden, und Kontakt aufzunehmen, Support um festzustellen, ob eine Erhöhung der Anzahl der Upload-Thread-Pools den Durchsatz für Ihr S3 File Gateway verbessern könnte. Weitere Informationen finden Sie unter Grundlegendes zu Gateway-Metriken.

> **Note**
>
> Diese Einstellung verbraucht zusätzliche Gateway-CPU-Ressourcen. Wir empfehlen, die CPU-Auslastung des Gateways zu überwachen und die zugewiesenen CPU-Ressourcen bei Bedarf zu erhöhen.

Erhöhen Sie die SMB-Timeout-Einstellungen

Wenn S3 File Gateway große Dateien auf eine SMB-Dateifreigabe kopiert, kann es nach einem längeren Zeitraum zu einem Timeout bei der SMB-Clientverbindung kommen.

Wir empfehlen, die Einstellung für das SMB-Sitzungs-Timeout für Ihre SMB-Clients auf 20 Minuten oder mehr zu verlängern, abhängig von der Größe der Dateien und der Schreibgeschwindigkeit Ihres Gateways. Die Standardeinstellung ist 300 Sekunden oder 5 Minuten. Weitere Informationen finden Sie unter Ihr Gateway-Backup-Job schlägt fehl oder es treten Fehler beim Schreiben auf Ihr Gateway auf.

Aktivieren Sie das opportunistische Sperren für kompatible Anwendungen

Opportunistisches Sperren oder „Oplocks“ ist standardmäßig für jedes neue S3 File Gateway aktiviert. Wenn Oplocks mit kompatiblen Anwendungen verwendet werden, fasst der Client mehrere kleinere Operationen zu größeren zusammen, was für den Client, das Gateway und das Netzwerk effizienter ist. Wir empfehlen, die opportunistische Sperre aktiviert zu lassen, wenn Sie Anwendungen verwenden, die clientseitiges lokales Caching nutzen, wie Microsoft Office, Adobe Suite und viele andere, da dies die Leistung erheblich verbessern kann.

Wenn Sie das opportunistische Sperren deaktivieren, öffnen Anwendungen, die Oplocks unterstützen, große Dateien (50 MB oder größer) in der Regel viel langsamer. Diese Verzögerung tritt auf, weil das Gateway Daten in Teilen von 4 KB sendet, was zu einem hohen I/O und niedrigen Durchsatz führt.

Passen Sie die Gateway-Kapazität an die Größe des Arbeitsdateisatzes an

Der Gateway-Kapazitätsparameter gibt die maximale Anzahl von Dateien an, für die Ihr Gateway Metadaten in seinem lokalen Cache speichert. Standardmäßig ist die Gateway-Kapazität auf Klein eingestellt, was bedeutet, dass das Gateway Metadaten für bis zu 5 Millionen Dateien speichert. Die Standardeinstellung funktioniert für die meisten Workloads gut, auch wenn es Hunderte von Millionen oder sogar Milliarden von Objekten in Amazon S3 gibt, da in einer typischen Bereitstellung nur auf eine kleine Teilmenge von Dateien zu einem bestimmten Zeitpunkt aktiv zugegriffen wird. Diese Gruppe von Dateien wird als „Working Set“ bezeichnet.

Wenn Ihr Workload regelmäßig auf eine Gruppe von Dateien mit mehr als 5 Millionen zugreift, muss Ihr Gateway häufig Cache-Räumungen durchführen. Dabei handelt es sich um kleine I/O-Operationen, die im RAM gespeichert und auf der Root-Festplatte dauerhaft gespeichert werden. Dies kann sich negativ auf die Gateway-Leistung auswirken, da das Gateway neue Daten von Amazon S3 abruft.

Sie können die `IndexEvictions` Metrik überwachen, um die Anzahl der Dateien zu ermitteln, deren Metadaten aus dem Cache entfernt wurden, um Platz für neue Einträge zu schaffen. Weitere Informationen finden Sie unter Grundlegendes zu Gateway-Metriken.

Wir empfehlen, die `UpdateGatewayInformation` API-Aktion zu verwenden, um die Gateway-Kapazität so zu erhöhen, dass sie der Anzahl der Dateien in Ihrem typischen Arbeitssatz entspricht. Weitere Informationen finden Sie unter UpdateGatewayInformation.

> **Note**
>
> Die Erhöhung der Gateway-Kapazität erfordert zusätzliche RAM- und Root-Festplattenkapazität.
>
> - Für kleine Dateien (5 Millionen Dateien) sind mindestens 16 GB RAM und 80 GB Root-Festplatte erforderlich.
> - Medium (10 Millionen Dateien) erfordert mindestens 32 GB RAM und 160 GB Root-Festplatte.

- Groß (20 Millionen Dateien) erfordert 64 GB RAM und 240 GB Root-Festplatte.

Important

Die Gateway-Kapazität kann nicht verringert werden.

Stellen Sie mehrere Gateways für größere Workloads bereit

Wir empfehlen, Ihre Arbeitslast nach Möglichkeit auf mehrere Gateways aufzuteilen, anstatt viele Dateifreigaben auf einem einzigen großen Gateway zu konsolidieren. Sie könnten beispielsweise eine häufig genutzte Dateifreigabe auf einem Gateway isolieren und die weniger häufig verwendeten Dateifreigaben auf einem anderen Gateway gruppieren.

Wenn Sie eine Bereitstellung mit mehreren Gateways und Dateifreigaben planen, sollten Sie Folgendes berücksichtigen:

- Die maximale Anzahl von Dateifreigaben auf einem einzelnen Gateway beträgt 50, aber die Anzahl der von einem Gateway verwalteten Dateifreigaben kann sich auf die Leistung des Gateways auswirken. Weitere Informationen finden Sie unter Leistungsanleitung für Gateways mit mehreren Dateifreigaben.
- Die Ressourcen auf jedem S3 File Gateway werden ohne Partitionierung von allen Dateifreigaben gemeinsam genutzt.
- Eine einzelne Dateifreigabe mit hoher Auslastung kann sich auf die Leistung anderer Dateifreigaben auf dem Gateway auswirken.

Note

Es wird nicht empfohlen, mehrere Dateifreigaben, die demselben Amazon S3 S3-Standort zugeordnet sind, von mehreren Gateways aus zu erstellen, es sei denn, mindestens eines davon ist schreibgeschützt.
Gleichzeitige Schreibvorgänge von mehreren Gateways in dieselbe Datei gelten als Szenario mit mehreren Schreibern, was zu Problemen mit der Datenintegrität führen kann.

Optimierung von S3 File Gateway für SQL Server-Datenbanksicherungen

Datenbank-Backups sind ein gängiger und empfohlener Anwendungsfall für S3 File Gateway, das eine kostengünstige kurz- und langfristige Aufbewahrung ermöglicht, indem Datenbank-Backups in Amazon S3 gespeichert werden, wobei der Lebenszyklus bei Bedarf auf kostengünstigere Speicherebenen umgestellt werden kann. Mit dieser Lösung können Sie mithilfe integrierter Tools wie SQL Server Management Studio und Oracle RMAN den Bedarf an Backup-Anwendungen für Unternehmen reduzieren.

In den folgenden Abschnitten werden bewährte Methoden zur Optimierung Ihrer S3 File Gateway-Bereitstellung für optimierte Leistung und kostengünstigen Support für Hunderte von Terabyte an SQL-Datenbank-Backups beschrieben. Die in den einzelnen Abschnitten enthaltenen Anleitungen tragen schrittweise zur Verbesserung des Gesamtdurchsatzes bei. Obwohl keine dieser Empfehlungen erforderlich ist und sie nicht voneinander abhängig sind, wurden sie auf logische Weise ausgewählt und angeordnet, sodass sie zum Testen und Optimieren von S3 File Gateway-Implementierungen Support verwendet werden. Denken Sie beim Implementieren und Testen dieser Vorschläge daran, dass jede S3 File Gateway-Bereitstellung einzigartig ist, sodass Ihre Ergebnisse variieren können.

S3 File Gateway bietet eine Dateischnittstelle zum Speichern und Abrufen von Amazon S3 S3-Objekten mithilfe der branchenüblichen NFS- oder SMB-Dateiprotokolle mit einer systemeigenen 1:1 -Zuordnung zwischen Datei und Objekt. Sie stellen S3 File Gateway als virtuelle Maschine entweder lokal in Ihrer VMware Microsoft Hyper-V- oder Linux-KVM-Umgebung oder in der AWS Cloud als Amazon EC2 EC2-Instanz bereit. S3 File Gateway ist nicht als vollständiger NAS-Ersatz für Unternehmen konzipiert. S3 File Gateway emuliert ein Dateisystem, aber es ist kein Dateisystem. Die Verwendung von Amazon S3 als dauerhaftem Back-End-Speicher erzeugt zusätzlichen Overhead bei jedem I/O Vorgang, sodass die Bewertung der Leistung von S3 File Gateway mit einem vorhandenen NAS oder Dateiserver kein gleichwertiger Vergleich ist.

Stellen Sie Ihr Gateway am selben Standort wie Ihre SQL-Server bereit

Wir empfehlen, Ihre virtuelle S3 File Gateway-Appliance an einem physischen Standort mit möglichst geringer Netzwerklatenz zwischen ihr und Ihren SQL-Servern bereitzustellen. Beachten Sie bei der Auswahl eines Standorts für Ihr Gateway Folgendes:

- Eine geringere Netzwerklatenz bis zum Gateway kann dazu beitragen, die Leistung von SMB-Clients wie SQL-Servern zu verbessern.

- S3 File Gateway ist so konzipiert, dass es eine höhere Netzwerklatenz zwischen dem Gateway und Amazon S3 toleriert als zwischen dem Gateway und den Clients.
- Für S3 File Gateway-Instances, die in Amazon EC2 bereitgestellt werden, empfehlen wir, das Gateway und die SQL-Server in derselben Platzierungsgruppe zu belassen. Weitere Informationen finden Sie unter Platzierungsgruppen für Ihre Amazon EC2 EC2-Instances im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Reduzieren Sie Engpässe, die durch langsame Festplatten verursacht werden

Wir empfehlen, die `IoWaitPercent` CloudWatch Metrik zu überwachen, um Leistungsengpässe zu identifizieren, die auf langsame Speicherfestplatten auf Ihrem S3 File Gateway zurückzuführen sein können. Wenn Sie versuchen, festplattenbedingte Leistungsprobleme zu optimieren, sollten Sie Folgendes berücksichtigen:

- `IoWaitPercent`gibt an, wie lange die CPU in Prozent auf eine Antwort von den Root- oder Cache-Festplatten wartet.
- Wenn der Wert höher als 5-10% `IoWaitPercent` ist, deutet dies in der Regel auf einen Gateway-Leistungsengpass hin, der durch Festplatten mit schlechter Leistung verursacht wird. Diese Metrik sollte so nahe wie möglich bei 0% liegen — was bedeutet, dass das Gateway nie auf die Festplatte wartet —, was zur Optimierung der CPU-Ressourcen beiträgt.
- Sie können dies `IoWaitPercent` auf der Registerkarte Überwachung der Storage Gateway Gateway-Konsole überprüfen oder empfohlene CloudWatch Alarme so konfigurieren, dass Sie automatisch benachrichtigt werden, wenn die Metrik einen bestimmten Schwellenwert überschreitet. Weitere Informationen finden Sie unter Empfohlene CloudWatch Alarme für Ihr Gateway erstellen.
- Zur Minimierung empfehlen wir, für die Root- und Cache-Festplatten Ihres Gateways entweder eine SSD NVMe oder eine SSD zu verwenden`IoWaitPercent`.

Passen Sie die Ressourcenzuweisung für virtuelle Maschinen mit S3 File Gateway für CPU-, RAM- und Cache-Festplatten an

Wenn Sie versuchen, den Durchsatz für Ihr S3 File Gateway zu optimieren, ist es wichtig, der Gateway-VM ausreichend Ressourcen zuzuweisen, einschließlich CPU-, RAM- und Cache-Festplatten. Die Mindestanforderungen an virtuelle Ressourcen von 4 CPUs, 16 GB RAM und 150

GB Cache-Speicher sind in der Regel nur für kleinere Workloads geeignet. Bei der Zuweisung virtueller Ressourcen für größere Workloads empfehlen wir Folgendes:

- Erhöhen Sie die zugewiesene Anzahl auf 16 CPUs bis 48, abhängig von der typischen CPU-Auslastung, die von Ihrem S3 File Gateway generiert wird. Sie können die CPU-Auslastung mithilfe der `UserCpuPercent` Metrik überwachen. Weitere Informationen finden Sie unter Grundlegendes zu Gateway-Metriken.
- Erhöhen Sie den zugewiesenen Arbeitsspeicher auf 32 bis 64 GB.

> **Note**
>
> S3 File Gateway kann nicht mehr als 64 GB RAM verwenden.

- Verwenden Sie NVMe oder SSD für Root-Festplatten und Cache-Festplatten, und passen Sie die Größe Ihrer Cache-Festplatten so an, dass sie dem Datenbestand entsprechen, den Sie in das Gateway schreiben möchten. Weitere Informationen finden Sie unter Best Practices zur Cache-Dimensionierung von S3 File Gateway auf dem offiziellen Amazon Web Services YouTube Services-Kanal.
- Fügen Sie dem Gateway mindestens 4 virtuelle Cache-Festplatten hinzu, anstatt eine einzige große Festplatte zu verwenden. Mehrere virtuelle Laufwerke können die Leistung verbessern, selbst wenn sie dieselbe zugrunde liegende physische Festplatte verwenden. Die Verbesserungen sind jedoch in der Regel größer, wenn sich die virtuellen Laufwerke auf verschiedenen zugrunde liegenden physischen Festplatten befinden.

  Wenn Sie beispielsweise 12 TB Cache bereitstellen möchten, können Sie eine der folgenden Konfigurationen verwenden:

  - 4 x 3 TB Cache-Festplatten
  - 8 x 1,5 TB Cache-Festplatten
  - 12 x 1-TB-Cache-Festplatten

  Zusätzlich zur Leistung ermöglicht dies im Laufe der Zeit eine effizientere Verwaltung der virtuellen Maschine. Wenn sich Ihre Arbeitslast ändert, können Sie die Anzahl der Cache-Festplatten und Ihre gesamte Cachekapazität schrittweise erhöhen und gleichzeitig die ursprüngliche Größe jedes einzelnen virtuellen Laufwerks beibehalten, um die Gateway-Integrität zu wahren.

  Weitere Informationen finden Sie unter Festlegung der Größe des lokalen Festplattenspeichers.

Beachten Sie bei der Bereitstellung von S3 File Gateway als Amazon EC2 EC2-Instance Folgendes:

- Der von Ihnen gewählte Instance-Typ kann sich erheblich auf die Gateway-Leistung auswirken. Amazon EC2 bietet umfassende Flexibilität bei der Anpassung der Ressourcenzuweisung für Ihre S3 File Gateway-Instance.
- Die empfohlenen Amazon EC2 EC2-Instance-Typen für S3 File Gateway finden Sie unter Anforderungen für Amazon EC2 EC2-Instance-Typen.
- Sie können den Amazon EC2 EC2-Instance-Typ ändern, der ein aktives S3 File Gateway hostet. Auf diese Weise können Sie die Amazon EC2 EC2-Hardwaregenerierung und die Ressourcenzuweisung einfach anpassen, um ein ideales price-to-performance Verhältnis zu finden. Gehen Sie in der Amazon EC2 EC2-Konsole wie folgt vor, um den Instance-Typ zu ändern:

  1. Stoppen Sie die Amazon EC2 EC2-Instance.
  2. Ändern Sie den Amazon EC2 EC2-Instance-Typ.
  3. Schalten Sie die Amazon EC2 EC2-Instance ein.

  > **Note**
  >
  > Durch das Stoppen einer Instance, die ein S3 File Gateway hostet, wird der Dateifreigabezugriff vorübergehend unterbrochen. Stellen Sie sicher, dass Sie bei Bedarf ein Wartungsfenster einplanen.

- Das price-to-performance Verhältnis einer Amazon EC2 EC2-Instance bezieht sich darauf, wie viel Rechenleistung Sie für den Preis erhalten, den Sie zahlen. In der Regel bieten Amazon EC2 EC2-Instances der neueren Generation das beste price-to-performance Verhältnis mit neuerer Hardware und verbesserter Leistung zu relativ geringeren Kosten im Vergleich zu älteren Generationen. Faktoren wie Instance-Typ, Region und Nutzungsmuster wirken sich auf dieses Verhältnis aus. Daher ist es wichtig, die richtige Instance für Ihren spezifischen Workload auszuwählen, um die Kosteneffizienz zu optimieren.

Verbessern Sie den Durchsatz von SMB-Clients, indem Sie die Sicherheitsstufe Ihres S3 File Gateways anpassen

Das SMBv3 Protokoll ermöglicht sowohl SMB-Signaturen als auch SMB-Verschlüsselung, was einige Kompromisse in Bezug auf Leistung und Sicherheit mit sich bringt. Um den Durchsatz zu optimieren, können Sie die SMB-Sicherheitsstufe Ihres Gateways anpassen, um festzulegen, welche dieser

Sicherheitsfunktionen für Client-Verbindungen durchgesetzt werden. Weitere Informationen finden Sie unter Einstellen einer Sicherheitsstufe für Ihr Gateway.

Beachten Sie bei der Anpassung der SMB-Sicherheitsstufe Folgendes:

- Die Standardsicherheitsstufe für S3 File Gateway ist Enforce encryption. Diese Einstellung erzwingt sowohl die Verschlüsselung als auch die Signierung für SMB-Clientverbindungen zu Gateway-Dateifreigaben, was bedeutet, dass der gesamte Datenverkehr vom Client zum Gateway verschlüsselt wird. Diese Einstellung wirkt sich nicht auf den Datenverkehr vom Gateway zum aus AWS, der immer verschlüsselt ist.

  Das Gateway begrenzt jede verschlüsselte Client-Verbindung auf eine einzelne vCPU. Wenn Sie beispielsweise nur einen verschlüsselten Client haben, ist dieser Client auf nur 1 vCPU beschränkt, auch wenn dem Gateway 4 oder mehr v zugewiesen CPUs sind. Aus diesem Grund liegt der Durchsatz für verschlüsselte Verbindungen von einem einzelnen Client zum S3 File Gateway in der Regel zwischen 40 und 60 MB/s.
- Wenn Ihre Sicherheitsanforderungen eine entspanntere Haltung zulassen, können Sie die Sicherheitsstufe auf „Vom Kunden ausgehandelt“ ändern. Dadurch wird die SMB-Verschlüsselung deaktiviert und nur die SMB-Signatur erzwungen. Mit dieser Einstellung können Client-Verbindungen zum Gateway mehrere V verwendenCPUs, was in der Regel zu einer erhöhten Durchsatzleistung führt.

> **Note**
>
> Nachdem Sie die SMB-Sicherheitsstufe für Ihr S3 File Gateway geändert haben, müssen Sie warten, bis sich der Dateifreigabestatus in der Storage Gateway Gateway-Konsole von Aktuell auf Verfügbar ändert, und dann Ihre SMB-Clients trennen und erneut verbinden, damit die neue Einstellung wirksam wird.

Verbessern Sie den SMB-Client-Durchsatz, indem Sie SQL-Backups in mehrere Dateien aufteilen

- Es ist schwierig, die maximale Durchsatzleistung mit einem S3 File Gateway zu erreichen, bei dem jeweils nur ein SQL-Server eine Datei schreibt, da sequentielles Schreiben von einem einzelnen SQL-Server aus ein Single-Thread-Vorgang ist. Stattdessen empfehlen wir, mehrere Threads von jedem SQL-Server zu verwenden, um mehrere Dateien parallel zu schreiben, und mehrere

SQL-Server gleichzeitig für Ihr S3 File Gateway zu verwenden, um den Gateway-Durchsatz zu maximieren. Bei SQL-Backups ermöglicht das Aufteilen von Backups in mehrere Dateien, dass jede Datei einen separaten Thread verwendet, der mehrere Dateien gleichzeitig auf die S3 File Gateway-Dateifreigabe schreibt. Je mehr Threads Sie haben, desto mehr Durchsatz können Sie bis zu den Grenzen des Gateways erreichen.

- SQL Server unterstützt das gleichzeitige Schreiben in mehrere Dateien während eines einzelnen Sicherungsvorgangs. Sie können beispielsweise mehrere Dateiziele mithilfe von T-SQL-Befehlen oder SQL Server Management Studio (SSMS) angeben. Jede Datei verwendet einen separaten Thread, um Daten vom SQL-Server an die Gateway-Dateifreigabe zu senden. Dieser Ansatz ermöglicht einen besseren I/O Durchsatz, wodurch die Geschwindigkeit und Effizienz von Backups erheblich verbessert werden können.

Beachten Sie bei der Konfiguration Ihrer SQL Server-Backups Folgendes:

- Durch die Aufteilung von Backups in mehrere Dateien können SQL Server-Administratoren die Sicherungszeiten optimieren und große Datenbanksicherungen effektiver verwalten.
- Die Anzahl der verwendeten Dateien hängt von der Speicherkonfiguration und den Leistungsanforderungen des Servers ab. Für große Datenbanken empfehlen wir, Backups in mehrere kleinere Dateien zwischen jeweils 10 GB und 20 GB aufzuteilen.
- Es gibt keine strikte Beschränkung für die Anzahl der Dateien, in die SQL Server während einer Sicherung schreiben kann, aber praktische Überlegungen wie Speicherarchitektur und Netzwerkbandbreite sollten bei dieser Auswahl als Richtschnur dienen.

Weitere Informationen finden Sie unter:

- Sie können SQL Server 43-67% schneller sichern, indem Sie in mehrere Dateien schreiben
- Speichern Sie Ihre SQL Server-Backups mit File Gateway ganz einfach in Amazon S3

Vermeiden Sie Fehler beim Kopieren großer Dateien, indem Sie die SMB-Timeout-Einstellungen erhöhen

Wenn S3 File Gateway große SQL-Backupdateien auf eine SMB-Dateifreigabe kopiert, kann es nach einem längeren Zeitraum zu einem Timeout bei der SMB-Clientverbindung kommen. Wir empfehlen, die Einstellung für das SMB-Sitzungstimeout für Ihre SQL Server-SMB-Clients auf 20 Minuten oder mehr zu verlängern, abhängig von der Größe der Dateien und der Schreibgeschwindigkeit Ihres

Gateways. Die Standardeinstellung ist 300 Sekunden oder 5 Minuten. Weitere Informationen finden Sie unter Ihr Gateway-Backup-Job schlägt fehl oder es treten Fehler beim Schreiben auf Ihr Gateway auf.

Erhöhen Sie die Anzahl der Amazon S3 S3-Uploader-Threads

Standardmäßig öffnet S3 File Gateway 8 Threads für den Amazon S3 S3-Datenupload, was ausreichend Upload-Kapazität für die meisten typischen Bereitstellungen bietet. Es ist jedoch möglich, dass ein Gateway Daten von SQL-Servern mit einer höheren Geschwindigkeit empfängt, als es mit der Standardkapazität von 8 Threads auf Amazon S3 hochladen kann, was dazu führen kann, dass der lokale Cache sein Speicherlimit erreicht.

Unter bestimmten Umständen Support kann die Anzahl der Amazon S3 S3-Upload-Thread-Pools für Ihr Gateway von 8 auf 40 erhöht werden, sodass mehr Daten parallel hochgeladen werden können. Abhängig von der Bandbreite und anderen Faktoren, die für Ihre Bereitstellung spezifisch sind, kann dies die Upload-Leistung erheblich steigern und dazu beitragen, den zur Unterstützung Ihrer Arbeitslast benötigten Cache-Speicher zu reduzieren.

Wir empfehlen, die `CachePercentDirty` CloudWatch Metrik zu verwenden, um die Menge der auf den lokalen Gateway-Cache-Festplatten gespeicherten Daten zu überwachen, die noch nicht auf Amazon S3 hochgeladen wurden, und Kontakt aufzunehmen, Support um festzustellen, ob eine Erhöhung der Anzahl der Upload-Thread-Pools den Durchsatz für Ihr S3 File Gateway verbessern könnte. Weitere Informationen finden Sie unter Grundlegendes zu Gateway-Metriken.

> **Note**
>
> Diese Einstellung verbraucht zusätzliche Gateway-CPU-Ressourcen. Wir empfehlen, die CPU-Auslastung des Gateways zu überwachen und die zugewiesenen CPU-Ressourcen bei Bedarf zu erhöhen.

Schalten Sie die automatische Cache-Aktualisierung aus

Die automatische Cache-Aktualisierungsfunktion ermöglicht es Ihrem S3 File Gateway, seine Metadaten automatisch zu aktualisieren. Dies kann dazu beitragen, alle Änderungen zu erfassen, die Benutzer oder Anwendungen an Ihrem Dateisatz vornehmen, indem sie direkt in den Amazon S3 S3-Bucket schreiben und nicht über das Gateway. Weitere Informationen finden Sie unter Aktualisieren des Amazon S3 S3-Bucket-Objekt-Caches.

Um den Gateway-Durchsatz zu optimieren, empfehlen wir, diese Funktion in Bereitstellungen zu deaktivieren, in denen alle Lese- und Schreibvorgänge in den Amazon S3 S3-Bucket über Ihr S3 File Gateway ausgeführt werden.

Beachten Sie bei der Konfiguration der automatischen Cache-Aktualisierung Folgendes:

- Wenn Sie die automatische Cache-Aktualisierung verwenden müssen, weil Benutzer oder Anwendungen in Ihrer Bereitstellung gelegentlich direkt in Amazon S3 schreiben, empfehlen wir, das längstmögliche Zeitintervall zwischen den Aktualisierungen zu konfigurieren, das für Ihre Geschäftsanforderungen immer noch praktikabel ist. Ein längeres Cache-Aktualisierungsintervall trägt dazu bei, die Anzahl der Metadatenoperationen zu reduzieren, die das Gateway beim Durchsuchen von Verzeichnissen oder beim Ändern von Dateien ausführen muss.

  Beispiel: Stellen Sie die automatische Cache-Aktualisierung auf 24 Stunden statt auf 5 Minuten ein, wenn dies für Ihre Arbeitslast tolerierbar ist.
- Das Mindestzeitintervall beträgt 5 Minuten. Das maximale Intervall beträgt 30 Tage.
- Wenn Sie sich dafür entscheiden, ein sehr kurzes Cache-Aktualisierungsintervall festzulegen, empfehlen wir, das Durchsuchen von Verzeichnissen auf Ihren SQL-Servern zu testen. Die Zeit, die zum Aktualisieren des Gateway-Cache benötigt wird, kann je nach Anzahl der Dateien und Unterverzeichnisse in Ihrem Amazon S3-Bucket erheblich länger dauern.

Stellen Sie mehrere Gateways bereit, um die Arbeitslast zu unterstützen

Storage Gateway kann SQL-Backups für große Umgebungen mit Hunderten von SQL-Datenbanken, mehreren SQL-Servern und Hunderten von Terabyte an Backup-Daten unterstützen, indem die Arbeitslast auf mehrere Gateways aufgeteilt wird.

Beachten Sie bei der Planung einer Bereitstellung mit mehreren Gateways und SQL-Servern Folgendes:

- Ein einzelnes Gateway kann bei ausreichender Hardwareressourcen und Bandbreite in der Regel bis zu 20 TB pro Tag hochladen. Sie können dieses Limit auf bis zu 40 TB pro Tag erhöhen, indem Sie die Anzahl der Amazon S3 S3-Uploader-Threads erhöhen.
- Wir empfehlen, einen proof-of-concept Test durchzuführen, um die Leistung zu messen und alle Variablen in Ihrer Bereitstellung zu berücksichtigen. Nachdem Sie den Spitzendurchsatz Ihres SQL-Backup-Workloads ermittelt haben, können Sie die Anzahl der Gateways Ihren Anforderungen entsprechend skalieren.

- Wir empfehlen, Ihre Lösung mit Blick auf das Wachstum zu entwickeln, da die Anzahl der Datenbanken und die Größe der Datenbanken im Laufe der Zeit zunehmen können. Um die steigende Arbeitslast weiterhin zu skalieren und zu unterstützen, können Sie bei Bedarf zusätzliche Gateways bereitstellen.

Zusätzliche Ressourcen für Datenbank-Backup-Workloads

- Speichern Sie SQL Server-Backups in Amazon S3 mit AWS Storage Gateway
- Speichern Sie Ihre SQL Server-Backups mit File Gateway ganz einfach in Amazon S3
- Wird AWS Storage Gateway zum Speichern von Oracle-Datenbank-Backups in Amazon S3 verwendet
- Oracle-Datenbanken in großem Umfang auf Amazon S3 sichern
- Integrieren Sie eine SAP ASE-Datenbank in Amazon S3 mithilfe von AWS Storage Gateway
- Wie One AWS Hero AWS Storage Gateway für In-Cloud-Backups verwendet
- Bewährte Methoden zur Skalierung des S3-File Gateway-Caches

Sicherheit beiAWSStorage Gateway

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWSbietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-partyPrüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AWS Storage Gateway gelten, finden Sie unter AWSServices in Scope by Compliance Program AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. 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 lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Storage Gateway Gateway-Ressourcen zu überwachen und zu sichern.

Datenschutz inAWSStorage Gateway

Das AWS Modell der gilt für den Datenschutz in AWS Storage Gateway. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufenAWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM)

einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit einAWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrailBenutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen StandardsicherheitskontrollenAWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, 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 anderen Geräten arbeiten und die Konsole, die API oder AWS SDKs AWS-Services verwenden. AWS CLI Alle Daten, die Sie in Tags oder Freitextfelder 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, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung mitAWS KMS

Storage Gateway verwendet SSL/TLS (Secure Socket Layers/Transport Layer Security), um Daten zu verschlüsseln, die zwischen Ihrer Gateway-Appliance und dem AWS Speicher übertragen werden. Standardmäßig verwendet Storage Gateway S3-Managed Amazon-Verschlüsselungsschlüssel (SSE-S3), um alle in Amazon S3 gespeicherten Daten serverseitig zu verschlüsseln. Sie haben die Möglichkeit, die Storage Gateway Gateway-API zu verwenden, um Ihr Gateway so zu konfigurieren, dass in der Cloud gespeicherte Daten mithilfe einer serverseitigen Verschlüsselung mit AWS Key Management Service (SSE-KMS) -Schlüsseln verschlüsselt werden.

Verschlüsseln einer Dateifreigabe

Sie können die Dateifreigaben auf Ihrem S3 File Gateway so konfigurieren, dass gespeicherte Objekte mit AWS KMS verwalteten Schlüsseln verschlüsselt werden, indem Sie oder verwenden. SSE-KMS DSSE-KMS Informationen zu unterstützten Verschlüsselungsmethoden für Dateifreigaben finden Sie unter Verschlüsseln von Objekten, die von File Gateway in Amazon S3 gespeichert wurden.

Beachten Sie bei der Verwendung AWS KMS zur Verschlüsselung Ihrer Daten Folgendes:

- Ihre Daten werden im Ruhezustand in der Cloud verschlüsselt. Das heißt, die Daten werden in Amazon S3 Amazon verschlüsselt.
- IAM-Benutzer müssen über die erforderlichen Berechtigungen verfügen, um die AWS KMS API-Operationen aufrufen zu können. Weitere Informationen finden Sie unter Verwenden von IAM-Richtlinien mit AWS KMS im Entwicklerhandbuch zu AWS Key Management Service.

> **Important**
>
> Wenn Sie einen AWS KMS Schlüssel für die serverseitige Verschlüsselung verwenden, müssen Sie einen symmetrischen Schlüssel wählen. Storage Gateway unterstützt keine asymmetrischen Schlüssel. Weitere Informationen finden Sie unter Using Symmetric and Asymmetric Keys (Verwenden von symmetrischen und asymmetrischen Schlüsseln) im AWS Key Management Service-Benutzerhandbuch.

Weitere Informationen zu finden Sie AWS KMS unter Was ist? AWS Key Management Service

Identitäts- und Zugriffsmanagement fürAWSStorage Gateway

AWS Identity and Access Management(IAM) hilft einem AdministratorAWS-Service, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um SGW-Ressourcen zu verwendenAWS. IAM ist ein ProgrammAWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe

- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- WieAWSStorage Gateway arbeitet mit IAM
- Identity-based politische Beispiele fürAWSStorage Gateway
- FehlerbehebungAWSIdentität und Zugriff auf Storage Gateway
- Verwenden Sie Tags, um den Zugriff auf Ihr Gateway und Ihre Ressourcen zu kontrollieren
- Verwendung von Windows-ACLs zur Beschränkung des SMB-Dateifreigabezugriffs

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe FehlerbehebungAWSIdentität und Zugriff auf Storage Gateway).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe WieAWSStorage Gateway arbeitet mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based politische Beispiele fürAWSStorage Gateway).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung.

AWSBietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-KontoRoot-Benutzer

Wenn Sie einen erstellenAWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWSbewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien.

In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWSunterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

WieAWSStorage Gateway arbeitet mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf AWS SGW verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen mit SGW verwendet werden können. AWS

IAM-Funktionen, die Sie mit verwenden könnenAWSStorage Gateway

IAM-Feature	AWSSGW-Unterstützung
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-linked Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS SGW und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWSIAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Identity-based Richtlinien fürAWSSGW

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Identity-based Richtlinienbeispiele fürAWSSGW

Beispiele für identitätsbasierte Richtlinien von AWS SGW finden Sie unter. Identity-based politische Beispiele fürAWSStorage Gateway

Resource-based Richtlinien innerhalbAWSSGW

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen fürAWSSGW

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS SGW-Aktionen finden Sie unter Von AWS Storage Gateway definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in AWS SGW verwenden vor der Aktion das folgende Präfix:

```
sgw
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

Beispiele für identitätsbasierte AWS SGW-Richtlinien finden Sie unter. Identity-based politische Beispiele fürAWSStorage Gateway

Politische Ressourcen fürAWSSGW

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS SGW-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Storage Gateway definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Storage Gateway definierte Aktionen.

Beispiele für identitätsbasierte AWS SGW-Richtlinien finden Sie unter. Identity-based politische Beispiele fürAWSStorage Gateway

Bedingungsschlüssel für Richtlinien fürAWSSGW

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS SGW-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Storage Gateway in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Storage Gateway definierte Aktionen.

Beispiele für identitätsbasierte AWS SGW-Richtlinien finden Sie unter. Identity-based politische Beispiele fürAWSStorage Gateway

ACLs inAWSSGW

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mitAWSSGW

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Attribute-based Access Control (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-

Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mitAWSSGW

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWSempfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Zugriffssitzungen weiterleiten fürAWSSGW

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Principals, der einen aufruftAWS-Service, in Kombination mit der Anfrage, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen fürAWSSGW

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern

und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS SGW-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AWS SGW Sie dazu anleitet.

Service-linked Rollen fürAWSSGW

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Dienst, der einen `Yes` in der Service-linked Rollenspalte enthält. Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Identity-based politische Beispiele fürAWSStorage Gateway

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS SGW-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS SGW definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Storage Gateway in der Service Authorization Reference.

Themen

- Best Practices für Richtlinien

- Verwendung der AWSSGW-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand AWS SGW-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWSverwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werdenAWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als

100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordertAWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwendung der AWSSGW-Konsole

Um auf die AWS Storage Gateway Gateway-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS SGW-Ressourcen in Ihrem AWS-Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS SGW-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS SGW `ConsoleAccess` - oder `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API oder. AWS CLI AWS

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

FehlerbehebungAWSIdentität und Zugriff auf Storage Gateway

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS SGW und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen inAWSSGW
- Ich bin nicht berechtigt, iam durchzuführen: PassRole

- Ich möchte Personen außerhalb meiner Umgebung zulassenAWS-Kontoum auf meine zuzugreifenAWSSGW-Ressourcen

Ich bin nicht berechtigt, eine Aktion durchzuführen inAWSSGW

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `sgw:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `sgw:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AWS SGW übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS SGW auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

> **Important**
>
> Storage Gateway kann bestehende Servicerollen übernehmen, die mithilfe der `iam:PassRole` Richtlinienaktion übergeben werden, unterstützt jedoch keine IAM-Richtlinien, die den `iam:PassedToService` Kontextschlüssel verwenden, um die Aktion auf bestimmte Dienste zu beschränken.
> Weitere Informationen finden Sie in folgenden Themen im AWS Identity and Access Management-Benutzerhandbuch:
>
> - IAM: Übergibt eine IAM-Rolle an einen bestimmten Dienst AWS
> - Erteilen Sie einem Benutzer die Erlaubnis, eine Rolle an einen Dienst zu übergeben AWS
> - Verfügbare Schlüssel für IAM

Ich möchte Personen außerhalb meiner Umgebung zulassenAWS-Kontoum auf meine zuzugreifenAWSSGW-Ressourcen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS SGW diese Funktionen unterstützt, finden Sie unterWieAWSStorage Gateway arbeitet mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderenAWS-Konto, den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren könnenAWS-Konten, finden Sie AWS-Kontenim IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.

- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwenden Sie Tags, um den Zugriff auf Ihr Gateway und Ihre Ressourcen zu kontrollieren

Um den Zugriff auf Gateway-Ressourcen und -Aktionen zu kontrollieren, können Sie AWS Identity and Access Management (IAM-) Richtlinien verwenden, die auf Tags basieren. 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.

Bestimmung des Zugriffs auf Ressourcen basierend auf Tags

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.

JSON

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
}
```

Bestimmung des Zugriffs basierend auf Tags in einer IAM-Anforderung

Um zu steuern, was ein Benutzer mit einer Gateway-Ressource tun kann, können Sie Bedingungen in einer IAM-Richtlinie verwenden, die auf Tags basiert. Sie können beispielsweise eine Richtlinie schreiben, die es einem Benutzer erlaubt oder verweigert, bestimmte API-Operationen auf der Grundlage des Tags auszuführen, das er bei der Erstellung der Ressource angegeben hat.

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 ermöglicht 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 **`Department`** und **`Finance`** übereinstimmt. 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.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/Department":"Finance",
               "aws:RequestTag/Department":"Finance"
            }
         }
      }
   ]
}
```

Verwendung von Windows-ACLs zur Beschränkung des SMB-Dateifreigabezugriffs

Amazon S3 File Gateway unterstützt zwei verschiedene Methoden zur Steuerung des Zugriffs auf Dateien und Verzeichnisse, die über eine SMB-Dateifreigabe gespeichert sind: POSIX-Berechtigungen oder Windows-ACLs.

In diesem Abschnitt wird beschrieben, wie Microsoft Windows Access Control Lists (ACLs) auf SMB-Dateifreigaben verwendet werden, die Microsoft Active Directory (AD) zur Authentifizierung verwenden. 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 werden standardmäßig für SMB-Dateifreigaben ausgewählt, wenn Ihr File-Gateway mit einer Active Directory-Domäne verbunden ist.
- Wenn ACLs aktiviert sind, werden die ACL-Informationen in den Amazon S3 S3-Objektmetadaten gespeichert.
- Die Gateway bewahrt bis zu 10 ACLs pro Datei oder Ordner auf.
- Wenn Sie eine SMB-Dateifreigabe mit aktivierten ACLs für den Zugriff auf S3-Objekte verwenden, die außerhalb Ihres Gateways erstellt wurden, erben die Objekte die ACL-Informationen aus dem übergeordneten Ordner.

> **Note**
>
> 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 aktivieren, wenn Sie mithilfe der API-Operation eine neue SMB-Dateifreigabe erstellen. CreateSMBFileShare Oder Sie können Windows-ACLs für eine bestehende SMB-Dateifreigabe mithilfe des API-Vorgangs aktivieren. UpdateSMBFileShare

Windows-ACLs auf einer neuen SMB-Dateifreigabe aktivieren

Gehen Sie wie folgt vor, 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 Erstellen Sie Ihr Gateway.
2. Wenn das Gateway keiner Domäne beigetreten ist, fügen Sie es einer Domäne hinzu. Weitere Informationen finden Sie unter Verwenden von Active Directory zur Benutzerauthentifizierung.
3. Erstellen Sie eine SMB-Dateifreigabe Die Ausgabe des obigen Befehls sieht in etwa folgendermaßen aus (JSON format).
4. Aktivieren Sie Windows-ACLs auf der Dateifreigabe von der Storage Gateway Gateway-Konsole aus.

   Gehen Sie wie folgt vor, um die Storage Gateway Console 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 Zugriff gesteuert durch die Option Windows Access Control List aus.
5. (Optional) Fügen Sie einen Admin-Benutzer hinzu AdminUsersList, wenn Sie möchten, dass der Admin-Benutzer berechtigt ist, ACLs für alle Dateien und Ordner in der Dateifreigabe zu aktualisieren.

> **Note**
>
> Wenn Sie die Listen Zulässige und Abgelehnte Benutzer und Gruppen in den Einstellungen der SMB-Dateifreigabe konfiguriert haben, gewähren ACLs keinen Zugriff, der diese Listen außer Kraft setzt.
> Die Listen „Zulässige“ und „Abgelehnte Benutzer“ und „Gruppen“ werden vor den ACLs ausgewertet und legen fest, welche Benutzer die Dateifreigabe bereitstellen oder darauf zugreifen können. Wenn Benutzer oder Gruppen in die Liste der zugelassenen Benutzer oder Gruppen aufgenommen werden, gilt die Liste als aktiv, und nur diese Benutzer können die Dateifreigabe bereitstellen.

Nachdem ein Benutzer eine Dateifreigabe bereitgestellt hat, bieten ACLs einen detaillierteren Schutz, der steuert, auf welche spezifischen Dateien oder Ordner der Benutzer zugreifen kann.

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 im Stammverzeichnis statt im übergeordneten Ordner unter Root konfigurieren, werden die ACL-Berechtigungen in Amazon S3 nicht dauerhaft gespeichert.

   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 werden die Informationen als Objektmetadaten in Amazon S3 beibehalten.

7. Aktivieren Sie gegebenenfalls die Vererbung.

   > **Note**
   >
   > Sie können die Vererbung für Dateifreigaben aktivieren, 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.

Aktivierung von Windows-ACLs auf einer vorhandenen SMB-Dateifreigabe

Gehen Sie wie folgt vor, um Windows-ACLs auf einer vorhandenen SMB-Dateifreigabe mit POSIX-Berechtigungen zu aktivieren.

So aktivieren Sie Windows-ACLs auf einer vorhandenen SMB-Dateifreigabe mithilfe der Storage Gateway Console

1. Wählen Sie die Dateifreigabe aus und klicken Sie auf Edit file share (Dateifreigabe bearbeiten).
2. Wählen Sie für die Option File/directory Zugriff gesteuert durch die Option Windows Access Control List aus.
3. Aktivieren Sie gegebenenfalls die Vererbung.

> **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 für Dateifreigaben unterstützt, die Active Directory für die Authentifizierung verwenden, wenn Sie Windows SMB-Clients für den Zugriff auf die Dateifreigaben verwenden.
- File Gateways unterstützt maximal 10 ACL-Einträge für die einzelnen Dateien und Ordner.
- File-Gateways unterstützen `Audit` keine `Alarm` AD-Einträge, bei denen es sich um SACL-Einträge (System Access Control List) handelt. Datei-Gateways unterstützen AD-Einträge, bei denen es sich um `Deny` DACL-Einträge (`Allow`Discretionary Access Control List) handelt.
- File-Gateways unterstützen keine ACE-Berechtigungen (Advanced Access Control Entry).
- 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 im Stammverzeichnis statt im übergeordneten Ordner unter dem Stammverzeichnis konfigurieren, werden die ACL-Berechtigungen in Amazon S3 nicht dauerhaft gespeichert.

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 Root-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 dieselben Root-ACLs verwenden.

Konformitätsüberprüfung fürAWSStorage Gateway

Third-party Prüfer bewerten die Sicherheit und Konformität von AWS Storage Gateway im Rahmen mehrerer AWS Compliance-Programme. Dazu gehören SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, ENS High, OSPAR und K-ISMS HITRUST CSF.

Allgemeine Informationen finden Sie unter AWSCompliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladenAWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Compliance-Verantwortung bei der Verwendung von Storage Gateway wird durch die Sensibilität Ihrer Daten, die Compliance-Ziele Ihres Unternehmens und die geltenden Gesetze und Vorschriften bestimmt. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Schnellstartanleitungen zu Sicherheit und Compliance Schnellstartanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Implementierung von sicherheits- und Compliance-orientierten Basisumgebungen beschrieben. AWS
- Whitepaper „Architecting for HIPAA Security and Compliance“ — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen entwickeln können. AWS HIPAA-compliant

- AWSCompliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS ConfigEntwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub CSPM— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen könnenAWS, ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Resilienz inAWSStorage Gateway

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones.

An AWS-Region ist ein physischer Standort auf der ganzen Welt, an dem Rechenzentren gebündelt sind. Jede Gruppe logischer Rechenzentren wird als Availability Zone (AZ) bezeichnet. Jedes AWS-Region besteht aus mindestens drei isolierten und physisch getrennten AZs innerhalb eines geografischen Gebiets. Im Gegensatz zu anderen Cloud-Anbietern, die eine Region häufig als ein einzelnes Rechenzentrum definieren, AWS-Region bietet das Design mit mehreren AZs deutliche Vorteile. Jede AZ verfügt über unabhängige Stromversorgung, Kühlung und physische Sicherheit und ist über redundante Netzwerke mit extrem niedriger Latenz verbunden. Wenn Ihre Bereitstellung einen Schwerpunkt auf Hochverfügbarkeit erfordert, können Sie Dienste und Ressourcen in mehreren AZs konfigurieren, um eine höhere Fehlertoleranz zu erreichen.

AWS-Regionenerfüllen die höchsten Standards in Bezug auf Infrastruktursicherheit, Compliance und Datenschutz. Der gesamte Datenverkehr zwischen AZs ist verschlüsselt. Die Netzwerkleistung reicht aus, um eine synchrone Replikation zwischen AZs zu erreichen. AZs erleichtern die Partitionierung von Diensten und Ressourcen für hohe Verfügbarkeit. Wenn Ihre Bereitstellung auf mehrere AZs aufgeteilt ist, sind Ihre Ressourcen besser isoliert und vor Problemen wie Stromausfällen, Blitzeinschlägen, Tornados, Erdbeben und mehr geschützt. AZs sind physisch durch eine nennenswerte Entfernung von allen anderen AZ getrennt, obwohl sich alle innerhalb von 100 km (60 Meilen) voneinander befinden.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWSGlobale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur unterstützt Storage Gateway VMware vSphere High Availability (VMware HA), um Storage-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen

zu schützen. Weitere Informationen finden Sie unter Verwenden von VMware vSphere High Availability mit Storage Gateway.

Sicherheit der Infrastruktur inAWSStorage Gateway

Als verwalteter Service ist AWS Storage Gateway durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die in Security Pillar — AWS Well-Architected Framework beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Storage Gateway zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.2 unterstützen. Clients müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie Ephemeral (DHE) oder Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) unterstützen. Diffie-Hellman 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.

> **Note**
>
> Sie sollten die AWS Storage Gateway Gateway-Appliance wie eine verwaltete virtuelle Maschine behandeln und nicht versuchen, auf ihre Installation zuzugreifen oder sie in irgendeiner Weise zu ändern. Der Versuch, Scansoftware zu installieren oder Softwarepakete mit anderen Methoden als dem normalen Gateway-Aktualisierungsmechanismus zu aktualisieren, kann zu Fehlfunktionen des Gateways führen und unsere Fähigkeit, das Gateway zu unterstützen oder zu reparieren, beeinträchtigen.
> AWSüberprüft, analysiert und behebt CVEs regelmäßig. Im Rahmen unseres normalen Softwareveröffentlichungszyklus integrieren wir Korrekturen für diese Probleme in Storage Gateway. Diese Fixes werden in der Regel als Teil des normalen Gateway-Aktualisierungsprozesses während planmäßiger Wartungsfenster angewendet. Weitere Informationen zu Gateway-Updates finden Sie unter Gateway-Updates mit der AWS Storage Gateway Konsole verwalten.

AWSBewährte Methoden für die Sicherheit

AWSbietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Diese bewährten Methoden stellen allgemeine Leitlinien dar und bilden keine vollständige Sicherheitslösung. Da diese 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 unter Bewährte Methoden für die AWS-Sicherheit.

Anmeldung und ÜberwachungAWS Storage Gateway

Storage Gateway ist in einen Dienst integriertAWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Storage Gateway ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Storage Gateway als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Storage-Gateway-Konsole und Code-Aufrufe der Storage-Gateway-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung 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 trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Storage Gateway gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrailBenutzerhandbuch.

Storage Gateway Gateway-Informationen in CloudTrail

CloudTrail ist auf Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität in Storage Gateway auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Dienstereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Ereignissen für Storage Gateway, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übertragung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen

in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Storage-Gateway-Aktionen werden protokolliert und im Thema Aktionen dokumentiert. Beispielsweise generieren Aufrufe der `ShutdownGateway` Aktionen `ActivateGatewayListGateways`, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Grundlegendes zu Storage Gateway Gateway-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

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 ListGateways 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 - 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"
              }]
}
```

Behebung von Problemen mit Ihrer Storage Gateway Gateway-Bereitstellung

Im Folgenden finden Sie Informationen zu bewährten Methoden und zur Behebung von Problemen im Zusammenhang mit Gateways, Hostplattformen, Dateifreigaben, Hochverfügbarkeit, Datenwiederherstellung und Sicherheit. Die Informationen zur Fehlerbehebung bei lokalen Gateways beziehen sich auf Gateways, die auf unterstützten Virtualisierungsplattformen bereitgestellt werden. Die Informationen zur Fehlerbehebung bei Hochverfügbarkeitsproblemen beziehen sich auf Gateways, die auf der VMware vSphere High Availability (HA) -Plattform ausgeführt werden.

Topics

- Fehlerbehebung: Gateway-Offline-Probleme- Erfahren Sie, wie Sie Probleme diagnostizieren, die dazu führen können, dass Ihr Gateway in der Storage Gateway Gateway-Konsole als offline angezeigt wird.
- Fehlerbehebung: Active Directory-Probleme- Erfahren Sie, was zu tun ist, wenn Sie Fehlermeldungen wie`NETWORK_ERROR`, oder erhalten`TIMEOUT`, `ACCESS_DENIED` wenn Sie versuchen, Ihr File Gateway mit einer Microsoft Active Directory-Domäne zu verbinden.
- Fehlerbehebung: Probleme mit der Gateway-Aktivierung- Erfahren Sie, wie Sie vorgehen, wenn Sie beim Versuch, Ihr Storage Gateway zu aktivieren, eine interne Fehlermeldung erhalten.
- Fehlerbehebung: Probleme mit dem lokalen Gateway- Erfahren Sie mehr über typische Probleme, die bei der Arbeit mit Ihren lokalen Gateways auftreten können, und darüber, wie Sie eine Verbindung zu Ihrem Gateway herstellen können Support , um Sie bei der Fehlerbehebung zu unterstützen.
- Fehlerbehebung: Probleme mit der Installation von Microsoft Hyper-V- Erfahren Sie mehr über typische Probleme, die bei der Bereitstellung von Storage Gateway auf der Microsoft Hyper-V-Plattform auftreten können.
- Fehlerbehebung: Probleme mit dem Amazon EC2 EC2-Gateway- Hier finden Sie Informationen zu typischen Problemen, die bei der Arbeit mit Gateways auftreten können, die auf Amazon EC2 bereitgestellt werden.
- Fehlerbehebung: Probleme mit der Hardware-Appliance- Erfahren Sie, wie Sie Probleme lösen können, die möglicherweise mit der AWS Storage Gateway Gateway-Hardware-Appliance auftreten.

- Fehlerbehebung: Probleme mit File Gateway- Hier finden Sie Informationen, die Ihnen helfen können, die Ursache von Fehlern und Integritätsmeldungen zu verstehen, die in den CloudWatch Protokollen Ihres File Gateways erscheinen.
- Fehlerbehebung: Probleme mit der Dateifreigabe- Erfahren Sie mehr über Maßnahmen, die Sie ergreifen können, wenn Sie unerwartete Probleme mit Ihrer Dateifreigabe haben.
- Fehlerbehebung: Probleme mit der Hochverfügbarkeit- Erfahren Sie, wie Sie vorgehen können, wenn Probleme mit Gateways auftreten, die in einer VMware HA-Umgebung bereitgestellt werden.

Fehlerbehebung: Gateway ist in der Storage Gateway Gateway-Konsole offline

Ermitteln Sie anhand der folgenden Informationen zur Fehlerbehebung, was zu tun ist, wenn die AWS Storage Gateway Konsole anzeigt, dass Ihr Gateway offline ist.

Ihr Gateway wird möglicherweise aus einem oder mehreren der folgenden Gründe als offline angezeigt:

- Das Gateway kann die Storage Gateway-Dienstendpunkte nicht erreichen.
- Das Gateway wurde unerwartet heruntergefahren.
- Eine dem Gateway zugeordnete Cache-Festplatte wurde getrennt oder geändert oder ist ausgefallen.

Um Ihr Gateway wieder online zu schalten, identifizieren und beheben Sie das Problem, das dazu geführt hat, dass Ihr Gateway offline gegangen ist.

Überprüfen Sie die zugehörige Firewall oder den zugehörigen Proxy

Wenn Sie Ihr Gateway für die Verwendung eines Proxys konfiguriert haben oder Ihr Gateway hinter einer Firewall platziert haben, überprüfen Sie die Zugriffsregeln des Proxys oder der Firewall. Der Proxy oder die Firewall muss den Datenverkehr zu und von den Netzwerkports und Dienstendpunkten zulassen, die von Storage Gateway benötigt werden. Weitere Informationen finden Sie unter Netzwerk- und Firewallanforderungen .

Suchen Sie nach einer laufenden SSL- oder Deep-Packet-Inspektion des Datenverkehrs Ihres Gateways

Wenn derzeit eine SSL- oder Deep-Packet-Inspection für den Netzwerkverkehr zwischen Ihrem Gateway und durchgeführt wird AWS, kann Ihr Gateway möglicherweise nicht mit den erforderlichen Service-Endpunkten kommunizieren. Um Ihr Gateway wieder online zu schalten, müssen Sie die Inspektion deaktivieren.

Überprüfen Sie die Metrik IOWait Prozent nach einem Neustart oder Softwareupdate

Prüfen Sie nach einem Neustart oder Softwareupdate, ob die `IOWaitPercent` Metrik für Ihr File Gateway 10 oder höher ist. Dies kann dazu führen, dass Ihr Gateway langsam reagiert, während es den Index-Cache im RAM neu aufbaut. Weitere Informationen finden Sie unter Problembehandlung: Verwenden von CloudWatch Metriken .

Suchen Sie nach einem Strom- oder Hardwarefehler auf dem Hypervisor-Host

Ein Strom- oder Hardwarefehler auf dem Hypervisor-Host Ihres Gateways kann dazu führen, dass Ihr Gateway unerwartet heruntergefahren wird und nicht mehr erreichbar ist. Nachdem Sie die Stromversorgung und die Netzwerkkonnektivität wiederhergestellt haben, ist Ihr Gateway wieder erreichbar.

Nachdem Ihr Gateway wieder online ist, sollten Sie unbedingt Maßnahmen ergreifen, um Ihre Daten wiederherzustellen. Weitere Informationen finden Sie unter Bewährte Methoden: Wiederherstellen Ihrer Daten .

Suchen Sie nach Problemen mit einer zugehörigen Cache-Festplatte

Ihr Gateway kann offline gehen, wenn mindestens eine der mit Ihrem Gateway verbundenen Cache-Festplatten entfernt, geändert oder in der Größe geändert wurde oder wenn sie beschädigt ist.

Wenn eine funktionierende Cache-Festplatte vom Hypervisor-Host entfernt wurde:

1. Fahren Sie das Gateway herunter.
2. Fügen Sie die Festplatte erneut hinzu.

> **Note**
>
> Stellen Sie sicher, dass Sie die Festplatte demselben Festplattenknoten hinzufügen.

3. Starten Sie Ihr Gateway neu.

Wenn ein Cache-Laufwerk beschädigt ist, ersetzt wurde oder dessen Größe geändert wurde:

- Folgen Sie dem Verfahren nach Methode 2, das unter Ersetzen Ihres vorhandenen S3 File Gateways durch eine neue Instanz beschrieben ist, um ein neues Gateway einzurichten und Cache-Festplatteninformationen erneut aus der AWS Cloud herunterzuladen.

Fehlerbehebung: Probleme beim Verbinden des Gateways mit Active Directory

Verwenden Sie die folgenden Informationen zur Problembehandlung, um zu ermitteln, was zu tun ist, wenn Sie Fehlermeldungen wie`NETWORK_ERROR`,`TIMEOUT`, oder erhalten, `ACCESS_DENIED` wenn Sie versuchen, Ihr File Gateway mit einer Microsoft Active Directory-Domäne zu verbinden.

Führen Sie die folgenden Prüfungen und Konfigurationen durch, um diese Fehler zu beheben.

Stellen Sie sicher, dass das Gateway den Domänencontroller erreichen kann, indem Sie einen NPING-Test ausführen

So führen Sie einen NPING-Test durch:

1. Stellen Sie mit Ihrer Hypervisor-Verwaltungssoftware (VMware, Hyper-V oder KVM) für lokale Gateways oder mit SSH für Amazon EC2 EC2-Gateways eine Connect zur lokalen Gateway-Konsole her.
2. Geben Sie die entsprechende Zahl ein, um die Gateway-Konsole auszuwählen, und geben Sie dann die Eingabetaste ein, um alle verfügbaren Befehle aufzulisten. h Führen Sie den folgenden Befehl aus, um die Konnektivität zwischen der virtuellen Storage Gateway Gateway-Maschine und der Domäne zu testen:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp
```

> **Note**
>
> `corp.domain.com`Ersetzen Sie es durch den DNS-Namen Ihrer Active Directory-Domäne und 389 ersetzen Sie es durch den LDAP-Port für Ihre Umgebung.
> Stellen Sie sicher, dass Sie die erforderlichen Ports innerhalb Ihrer Firewall geöffnet haben.

Im Folgenden finden Sie ein Beispiel für einen erfolgreichen NPING-Test, bei dem das Gateway den Domänencontroller erreichen konnte:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>

Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

Im Folgenden finden Sie ein Beispiel für einen NPING-Test, bei dem keine Konnektivität zum Ziel besteht oder keine Antwort vom `corp.domain.com` Ziel erfolgt:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Überprüfen Sie die für die VPC Ihrer Amazon EC2 EC2-Gateway-Instance festgelegten DHCP-Optionen.

Wenn das File Gateway auf einer Amazon EC2 EC2-Instance läuft, müssen Sie sicherstellen, dass ein DHCP-Optionssatz ordnungsgemäß konfiguriert und an die Amazon Virtual Private Cloud (VPC) angehängt ist, die die Gateway-Instance enthält. Weitere Informationen finden Sie unter DHCP-Optionssätze in Amazon VPC.

Vergewissern Sie sich, dass das Gateway die Domain auflösen kann, indem Sie eine Dig-Abfrage ausführen

Wenn die Domäne vom Gateway nicht aufgelöst werden kann, kann das Gateway der Domäne nicht beitreten.

Um eine Dig-Abfrage auszuführen:

1. Stellen Sie mit Ihrer Hypervisor-Verwaltungssoftware (VMware, Hyper-V oder KVM) für lokale Gateways oder mit SSH für Amazon EC2 EC2-Gateways eine Connect zur lokalen Gateway-Konsole her.
2. Geben Sie die entsprechende Zahl ein, um die Gateway-Konsole auszuwählen, und geben Sie dann die Eingabetaste ein, um alle verfügbaren Befehle aufzulisten. h Führen Sie den folgenden Befehl aus, um zu testen, ob das Gateway die Domäne auflösen kann:

   ```
   dig -d corp.domain.com
   ```

   > **Note**
   >
   > `corp.domain.com`Ersetzen Sie es durch den DNS-Namen Ihrer Active Directory-Domäne.

Im Folgenden finden Sie ein Beispiel für eine erfolgreiche Antwort:

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

Überprüfen Sie die Einstellungen und Rollen des Domänencontrollers

Vergewissern Sie sich, dass der Domänencontroller nicht schreibgeschützt ist und dass der Domänencontroller über genügend Rollen verfügt, sodass Computer diesem beitreten können. Um dies zu testen, versuchen Sie, andere Server aus demselben VPC-Subnetz wie die Gateway-VM mit der Domäne zu verbinden.

Stellen Sie sicher, dass das Gateway mit dem nächstgelegenen Domänencontroller verbunden ist

Als bewährte Methode empfehlen wir, Ihr Gateway mit einem Domänencontroller zu verbinden, der sich geografisch in der Nähe des Gatewaygeräts befindet. Wenn das Gatewaygerät aufgrund der Netzwerklatenz nicht innerhalb von 20 Sekunden mit dem Domänencontroller kommunizieren kann, kann es beim Domänenbeitritt zu einem Timeout kommen. Beispielsweise kann es bei dem Vorgang zu einem Timeout kommen, wenn sich die Gateway-Appliance im Osten der USA (Nord-Virginia) AWS-Region und der Domänencontroller im asiatisch-pazifischen Raum (Singapur) befindet AWS-Region.

> **Note**
>
> Um den standardmäßigen Timeoutwert von 20 Sekunden zu erhöhen, können Sie den Befehl join-domain in AWS Command Line Interface (AWS CLI) ausführen und die `--timeout-in-seconds` Option zur Verlängerung der Zeit hinzufügen. Sie können auch den JoinDomain API-Aufruf verwenden und den `TimeoutInSeconds` Parameter hinzufügen, um die Zeit zu verlängern. Der maximale Timeout-Wert beträgt 3.600 Sekunden.

Wenn Sie beim Ausführen von AWS CLI Befehlen Fehler erhalten, stellen Sie sicher, dass Sie die neueste AWS CLI Version verwenden.

Vergewissern Sie sich, dass Active Directory neue Computerobjekte in der Standard-Organisationseinheit (OU) erstellt

Stellen Sie sicher, dass Microsoft Active Directory über keine Gruppenrichtlinienobjekte verfügt, die neue Computerobjekte an einem anderen Ort als der Standardorganisationseinheit erstellen. Bevor Sie Ihr Gateway der Active Directory-Domäne hinzufügen können, muss in der Standard-OU ein neues Computerobjekt vorhanden sein. Einige Active Directory-Umgebungen sind so angepasst, dass sie OUs für neu erstellte Objekte unterschiedlich sind. Um sicherzustellen, dass ein neues Computerobjekt für die Gateway-VM in der Standard-OU vorhanden ist, versuchen Sie, das Computerobjekt manuell auf Ihrem Domänencontroller zu erstellen, bevor Sie das Gateway der Domäne hinzufügen. Sie können den Befehl join-domain auch mit dem ausführen. AWS CLI Geben Sie dann die Option für an. `--organizational-unit`

> **Note**
>
> Der Prozess der Erstellung des Computerobjekts wird als Pre-Staging bezeichnet.

Überprüfen Sie die Ereignisprotokolle Ihres Domänencontrollers

Wenn Sie das Gateway nicht mit der Domäne verbinden können, nachdem Sie alle anderen in den vorherigen Abschnitten beschriebenen Prüfungen und Konfigurationen ausprobiert haben, empfehlen wir, Ihre Domänencontroller-Ereignisprotokolle zu überprüfen. Suchen Sie in der Ereignisanzeige des Domänencontrollers nach Fehlern. Stellen Sie sicher, dass die Gatewayabfragen den Domänencontroller erreicht haben.

Fehlerbehebung: interner Fehler bei der Gateway-Aktivierung

Storage Gateway Gateway-Aktivierungsanforderungen durchlaufen zwei Netzwerkpfade. Eingehende Aktivierungsanfragen, die von einem Client gesendet werden, stellen über Port 80 eine Verbindung zur virtuellen Maschine (VM) oder Amazon Elastic Compute Cloud (Amazon EC2) -Instance des Gateways her. Wenn das Gateway die Aktivierungsanfrage erfolgreich empfängt, kommuniziert

das Gateway mit den Storage Gateway Gateway-Endpunkten, um einen Aktivierungsschlüssel zu erhalten. Wenn das Gateway die Storage Gateway Gateway-Endpunkte nicht erreichen kann, antwortet das Gateway dem Client mit einer internen Fehlermeldung.

Verwenden Sie die folgenden Informationen zur Fehlerbehebung, um zu ermitteln, was zu tun ist, wenn Sie beim Versuch, Ihren AWS Storage Gateway zu aktivieren, eine interne Fehlermeldung erhalten.

> **Note**
>
> - Stellen Sie sicher, dass Sie neue Gateways mit der neuesten Image-Datei für virtuelle Maschinen oder der neuesten Version von Amazon Machine Image (AMI) bereitstellen. Sie erhalten einen internen Fehler, wenn Sie versuchen, ein Gateway zu aktivieren, das ein veraltetes AMI verwendet.
> - Stellen Sie sicher, dass Sie den richtigen Gateway-Typ auswählen, den Sie bereitstellen möchten, bevor Sie das AMI herunterladen. Die OVA-Dateien AMIs für jeden Gateway-Typ sind unterschiedlich und nicht austauschbar.

Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt

Um Aktivierungsfehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt zu beheben, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Überprüfen Sie die erforderlichen Ports

Vergewissern Sie sich bei Gateways, die vor Ort bereitgestellt werden, dass die Ports auf Ihrer lokalen Firewall geöffnet sind. Überprüfen Sie bei Gateways, die auf einer Amazon EC2 EC2-Instance bereitgestellt werden, ob die Ports in der Sicherheitsgruppe der Instance geöffnet sind. Um zu überprüfen, ob die Ports geöffnet sind, führen Sie auf dem öffentlichen Endpunkt von einem Server aus einen Telnet-Befehl aus. Dieser Server muss sich im selben Subnetz wie das Gateway befinden. Mit den folgenden Telnet-Befehlen wird beispielsweise die Verbindung zu Port 443 getestet:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
```

```
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Um zu überprüfen, ob das Gateway selbst den Endpunkt erreichen kann, greifen Sie auf die lokale VM-Konsole des Gateways zu (für lokal bereitgestellte Gateways). Oder Sie können eine SSH-Verbindung zur Gateway-Instance herstellen (für Gateways, die auf Amazon EC2 bereitgestellt werden). Führen Sie dann einen Netzwerkverbindungstest durch. Vergewissern Sie sich, dass der Test zurückkehrt`[PASSED]`. Weitere Informationen finden Sie unter Testen der Netzwerkkonnektivität Ihres Gateways .

> **Note**
>
> Der Standard-Anmeldename für die Gateway-Konsole lautet`admin`, und das Standardkennwort ist`password`.

Stellen Sie sicher, dass die Firewall-Sicherheit keine Pakete verändert, die vom Gateway an die öffentlichen Endpunkte gesendet werden

SSL-Inspektionen, Deep Packet Inspections oder andere Formen der Firewall-Sicherheit können die vom Gateway gesendeten Pakete beeinträchtigen. Der SSL-Handshake schlägt fehl, wenn das SSL-Zertifikat so geändert wird, wie es der Aktivierungsendpunkt erwartet. Um sicherzustellen, dass keine SSL-Inspektion im Gange ist, führen Sie einen OpenSSL-Befehl auf dem Hauptaktivierungsendpunkt (`anon-cp.storagegateway.region.amazonaws.com`) an Port 443 aus. Sie müssen diesen Befehl von einem Computer aus ausführen, der sich im selben Subnetz wie das Gateway befindet:

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Ersetze es *`region`* durch dein AWS-Region.

Wenn keine SSL-Überprüfung im Gange ist, gibt der Befehl eine Antwort zurück, die der folgenden ähnelt:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Wenn eine laufende SSL-Inspektion stattfindet, zeigt die Antwort eine veränderte Zertifikatskette, die der folgenden ähnelt:

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

Der Aktivierungsendpunkt akzeptiert SSL-Handshakes nur, wenn er das SSL-Zertifikat erkennt. Das bedeutet, dass der ausgehende Datenverkehr des Gateways zu den Endpunkten von Inspektionen ausgenommen werden muss, die von Firewalls in Ihrem Netzwerk durchgeführt werden. Bei diesen Inspektionen kann es sich um eine SSL-Inspektion oder eine Deep Packet Inspection handeln.

Überprüfen Sie die Gateway-Zeitsynchronisierung

Übermäßige Zeitverschiebungen können zu SSL-Handshake-Fehlern führen. Bei lokalen Gateways können Sie die lokale VM-Konsole des Gateways verwenden, um die Zeitsynchronisierung Ihres Gateways zu überprüfen. Der Zeitversatz sollte nicht größer als 60 Sekunden sein.

Die Option System Time Management ist auf Gateways, die auf Amazon EC2 EC2-Instances gehostet werden, nicht verfügbar. Um sicherzustellen, dass Amazon EC2 EC2-Gateways die Zeit ordnungsgemäß synchronisieren können, stellen Sie sicher, dass die Amazon EC2 EC2-Instance über die Ports UDP und TCP 123 eine Verbindung zur folgenden NTP-Serverpool-Liste herstellen kann:

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

Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen Amazon VPC-Endpunkt

Um Aktivierungsfehler bei der Aktivierung Ihres Gateways über einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt zu beheben, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Überprüfen Sie die erforderlichen Ports

Stellen Sie sicher, dass die erforderlichen Ports innerhalb Ihrer lokalen Firewall (für lokal bereitgestellte Gateways) oder Sicherheitsgruppe (für in Amazon EC2 bereitgestellte Gateways) geöffnet sind. Die Ports, die für die Verbindung eines Gateways mit einem Storage Gateway Gateway-VPC-Endpunkt erforderlich sind, unterscheiden sich von denen, die für die Verbindung

eines Gateways mit öffentlichen Endpunkten erforderlich sind. Die folgenden Ports sind für die Verbindung mit einem Storage Gateway Gateway-VPC-Endpunkt erforderlich:

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

Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts für Storage Gateway für Storage Gateway.

Überprüfen Sie außerdem die Sicherheitsgruppe, die an Ihren Storage Gateway Gateway-VPC-Endpunkt angehängt ist. Die dem Endpunkt zugeordnete Standardsicherheitsgruppe lässt möglicherweise nicht die erforderlichen Ports zu. Erstellen Sie eine neue Sicherheitsgruppe, die Datenverkehr aus dem IP-Adressbereich Ihres Gateways über die erforderlichen Ports zulässt. Fügen Sie dann diese Sicherheitsgruppe dem VPC-Endpunkt hinzu.

> **Note**
>
> Verwenden Sie die Amazon VPC-Konsole, um die Sicherheitsgruppe zu überprüfen, die mit dem VPC-Endpunkt verbunden ist. Sehen Sie sich Ihren Storage Gateway Gateway-VPC-Endpunkt von der Konsole aus an und wählen Sie dann die Registerkarte Sicherheitsgruppen aus.

Um zu überprüfen, ob die erforderlichen Ports geöffnet sind, können Sie Telnet-Befehle auf dem Storage Gateway Gateway-VPC-Endpunkt ausführen. Sie müssen diese Befehle von einem Server aus ausführen, der sich im selben Subnetz wie das Gateway befindet. Sie können die Tests für den ersten DNS-Namen ausführen, der keine Availability Zone angibt. Mit den folgenden Telnet-Befehlen werden beispielsweise die erforderlichen Portverbindungen mithilfe des DNS-Namens vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com getestet:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
```

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Stellen Sie sicher, dass die Firewall-Sicherheit keine Pakete verändert, die vom Gateway an Ihren Storage Gateway Amazon VPC-Endpunkt gesendet werden.

SSL-Inspektionen, Deep Packet Inspections oder andere Formen der Firewall-Sicherheit können die vom Gateway gesendeten Pakete beeinträchtigen. Der SSL-Handshake schlägt fehl, wenn das SSL-Zertifikat so geändert wird, wie es der Aktivierungsendpunkt erwartet. Um sicherzustellen, dass keine SSL-Inspektion im Gange ist, führen Sie einen OpenSSL-Befehl auf Ihrem Storage Gateway Gateway-VPC-Endpunkt aus. Sie müssen diesen Befehl von einem Computer aus ausführen, der sich im selben Subnetz wie das Gateway befindet. Führen Sie den Befehl für jeden erforderlichen Port aus:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Wenn keine SSL-Überprüfung durchgeführt wird, gibt der Befehl eine Antwort zurück, die der folgenden ähnelt:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Wenn eine laufende SSL-Inspektion stattfindet, zeigt die Antwort eine veränderte Zertifikatskette, die der folgenden ähnelt:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
```

```
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

Der Aktivierungsendpunkt akzeptiert SSL-Handshakes nur, wenn er das SSL-Zertifikat erkennt. Das bedeutet, dass der ausgehende Datenverkehr des Gateways zu Ihrem VPC-Endpunkt über die erforderlichen Ports von den Inspektionen Ihrer Netzwerk-Firewalls ausgenommen ist. Bei diesen Inspektionen kann es sich um SSL-Inspektionen oder Deep-Packet-Inspektionen handeln.

Überprüfen Sie die Gateway-Zeitsynchronisierung

Übermäßige Zeitverschiebungen können zu SSL-Handshake-Fehlern führen. Bei lokalen Gateways können Sie die lokale VM-Konsole des Gateways verwenden, um die Zeitsynchronisierung Ihres Gateways zu überprüfen. Der Zeitversatz sollte nicht größer als 60 Sekunden sein.

Die Option System Time Management ist auf Gateways, die auf Amazon EC2 EC2-Instances gehostet werden, nicht verfügbar. Um sicherzustellen, dass Amazon EC2 EC2-Gateways die Zeit ordnungsgemäß synchronisieren können, stellen Sie sicher, dass die Amazon EC2 EC2-Instance über die Ports UDP und TCP 123 eine Verbindung zur folgenden NTP-Serverpool-Liste herstellen kann:

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

Suchen Sie nach einem HTTP-Proxy und bestätigen Sie die zugehörigen Sicherheitsgruppeneinstellungen

Prüfen Sie vor der Aktivierung, ob Sie einen HTTP-Proxy auf Amazon EC2 auf der lokalen Gateway-VM als Squid-Proxy auf Port 3128 konfiguriert haben. Bestätigen Sie in diesem Fall Folgendes:

- Die Sicherheitsgruppe, die an den HTTP-Proxy auf Amazon EC2 angehängt ist, muss über eine Regel für eingehenden Datenverkehr verfügen. Diese Regel für eingehenden Datenverkehr muss Squid-Proxyverkehr auf Port 3128 von der IP-Adresse der Gateway-VM aus zulassen.
- Die Sicherheitsgruppe, die dem Amazon EC2 VPC-Endpunkt zugeordnet ist, muss Regeln für eingehenden Datenverkehr haben. Diese Regeln für eingehenden Datenverkehr müssen den Verkehr auf den Ports 1026-1028, 1031, 2222 und 443 von der IP-Adresse des HTTP-Proxys auf Amazon EC2 zulassen.

Beheben Sie Fehler, wenn Sie Ihr Gateway über einen öffentlichen Endpunkt aktivieren und es in derselben VPC einen Storage Gateway Gateway-VPC-Endpunkt gibt

Um Fehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt zu beheben, wenn sich in derselben VPC ein Amazon Virtual Private Cloud (Amazon VPC) -Endpoint befindet, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Vergewissern Sie sich, dass die Einstellung Privaten DNS-Namen aktivieren auf Ihrem Storage Gateway Gateway-VPC-Endpunkt nicht aktiviert ist

Wenn Enable Private DNS Name aktiviert ist, können Sie keine Gateways von dieser VPC zum öffentlichen Endpunkt aktivieren.

Gehen Sie wie folgt vor, um die Option für private DNS-Namen zu deaktivieren:

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Ihren Storage Gateway VPC-Endpunkt.
4. Wählen Sie Aktionen.
5. Wählen Sie Private DNS-Namen verwalten aus.
6. Deaktivieren Sie für „Privaten DNS-Namen aktivieren“ die Option „Für diesen Endpunkt aktivieren“.
7. Wählen Sie Private DNS-Namen ändern, um die Einstellung zu speichern.

Fehlerbehebung: Probleme mit dem lokalen Gateway

Im Folgenden finden Sie Informationen zu typischen Problemen, die bei der Arbeit mit Ihren lokalen Gateways auftreten können, und darüber, wie Sie eine Verbindung zu Ihrem Gateway herstellen können Support , um Sie bei der Fehlerbehebung zu unterstützen.

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. • Denn VMware ESXi die IP-Adresse der VM finden Sie im vSphere-Client auf der Registerkarte Zusammenfassung. • 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. • Falls Sie den Netzwerkdatenverkehr mithilfe einer Firewall oder eines Routers filtern oder einschränken, müssen Sie die Firewall und den Router so konfigurieren, dass diese Service-Endpunkte für die ausgehende Kommunikation mit AWS verwendet werden dürfen. Weitere Informationen zum Netzwerk und Firewall-Anforderungen finden Sie unter Netzwerk- und Firewall-Anforderu ngen.
Die Aktivierung des Gateways schlägt fehl, wenn Sie in der Storage-Gateway-Managementk onsole auf die Schaltflä che Weiter zur Aktivierung klicken.	• 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 synchronisiert und dass die Gateway-VM auf die richtige Uhrzeit eingestellt ist. Informationen zum Synchronisieren der Uhrzeit von Hypervisor-Hosts und VMs finden Sie unter. Konfiguration eines NTP-Serve rs (Network Time Protocol) für Ihr Gateway • Nachdem Sie diese Schritte befolgt haben, können Sie die Bereitstellung des Gateways wiederholen, indem sie die Storage-Gateway-Konsole und den Assistenten zum Einrichten und Aktivieren des Gateways verwenden. • Stellen Sie sicher, dass Ihre VM über mindestens 16 GB RAM verfügt. Die Gateway-Zuweisung schlägt fehl, wenn weniger als 16 GB RAM vorhanden sind. Weitere Informationen finden Sie unter Setup-Anforderungen für File Gateway.
Sie müssen die Bandbreit e zwischen Ihrem Gateway und AWS verbessern.	Sie können die Bandbreite zwischen Ihrem Gateway und verbesser n, AWS indem Sie Ihre Internetverbindung AWS auf einem Netzwerkadapter (NIC) einrichten, der von dem Netzwerkadapter (NIC) getrennt ist, der Ihre Anwendungen und die Gateway-VM verbindet. Dieser Ansatz ist nützlich, wenn Sie eine Verbindung mit hoher Bandbreite haben AWS und Bandbreitenkonflikte vermeiden möchten, insbesondere bei einer Snapshot-Wiederherstellung. Für Workloads mit hohem Durchsatz können Sie Direct Connect verwenden, um eine dedizierte Netzwerkverbindung zwischen dem lokalen Gateway und AWS herzustellen. Verwenden Sie die `CloudBytesUploaded` Metriken `CloudBytesDownloaded` und des Gateways AWS, um die Bandbreite der Verbindung von Ihrem Gateway zu zu messen. Weitere Informationen zu diesem Thema finden Sie unter Leistung und Optimierung. 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.	• Stellen Sie auf der Registerkarte Gateway der Storage Gateway Gateway-Konsole sicher, dass die IP-Adressen für Ihre Gateway-VM denen entsprechen, die Sie mit Ihrer Hypervisor-Client-Software (d. h. dem VMware vSphere-Client oder Microsoft Hyper-V Manager) sehen. Wenn Sie eine Nichtübereinstimmung finden, starten Sie das Gateway über die Storage-Gateway-Konsole neu, wie unter Ihre Gateway-VM wird heruntergefahren gezeigt. Nach dem Neustart sollten die Adressen in der Liste IP-Adressen in der Storage-Gateway-Konsole auf der Registerkarte Gateway mit den IP-Adressen Ihres Gateways übereinstimmen, die Sie über den Hypervisor-Client bestimmen.
	  • Denn VMware ESXi die IP-Adresse der VM finden Sie im vSphere-Client auf der Registerkarte Zusammenfassung.
	  • Für Microsoft Hyper-V, kann die IP-Adresse der VM's gefunden werden, indem man sich auf der lokalen Konsole anmeldet.
	• Überprüfen Sie die Konnektivität Ihres Gateways AWS wie unter beschriebenTesten der Netzwerkkonnektivität Ihres Gateways.
	• Überprüfen Sie die Netzwerkadapterkonfiguration Ihres Gateways in Ihrem Hypervisor-Management-Client und stellen Sie sicher, dass alle Schnittstellen, die Sie für das Gateway verwenden möchten, aktiviert sind.
	• Überprüfen Sie die Netzwerkadapterkonfiguration Ihres Gateways in der lokalen Gateway-Konsole. Detaillierte Anweisungen finden Sie unter Konfiguration Ihrer Gateway-Netzwerkeinstellungen.
	
	Sie können den Durchsatz zu und von Ihrem Gateway von der CloudWatch Amazon-Konsole aus anzeigen. Weitere Informationen zur Messung des Durchsatzes zu und von Ihrem Gateway zu AWS finden Sie unterLeistung und Optimierung.

Problem	Maßnahme
Sie haben Schwierig keiten mit dem Importieren (Bereitstellen) von Storage Gateway auf Microsoft Hyper-V.	Weitere Informationen finden Sie unter Problembehandlung: Microsoft Hyper-V-Setup, in dem einige der gängigen Themen der Bereitstellung einer Gateway auf Microsoft Hyper-V diskutiert werden.
Sie erhalten die Fehlermel dung: „Die Daten, die in das Volume in Ihrem Gateway geschrieben wurden, sind nicht sicher bei AWS gespeichert.“	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 an den Support.

Fehlerbehebung: Sicherheitsscans zeigen offene NFS-Ports

Bestimmte NFS-Ports sind standardmäßig aktiviert, auch auf Gateways, die Sie nur mit SMB-Dateifreigaben verwenden. Wenn Sie Sicherheitssoftware von Drittanbietern wie Qualys verwenden, um das Netzwerk zu scannen, in dem Ihr File Gateway installiert ist, könnten die Scanergebnisse diese offenen NFS-Ports als potenzielle Sicherheitslücke melden. Wenn Sie Ihr Gateway nur mit SMB-Dateifreigaben verwenden und die ungenutzten NFS-Ports aus Sicherheitsgründen deaktivieren möchten, gehen Sie wie folgt vor:

So deaktivieren Sie NFS-Ports auf einem File Gateway:

1. Greifen Sie mit dem unter beschriebenen Verfahren auf die Eingabeaufforderung der lokalen Gateway-Konsole zuAusführen von Storage Gateway-Befehlen auf der lokalen Konsole.
2. Geben Sie die folgenden Befehle ein, um den NFS-Verkehr zu deaktivieren:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

IPv6

```
ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die blockierten NFS-Ports in den IP-Tabellen angezeigt werden:

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

Aktivieren Sie den Support Zugriff, um die Fehlerbehebung für Ihr lokal gehostetes Gateway zu erleichtern

Storage Gateway bietet eine lokale Konsole, mit der Sie verschiedene Wartungsaufgaben ausführen können, einschließlich des Zugriffs auf Ihr Gateway, Support um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Standardmäßig ist der Support Zugriff auf Ihr Gateway deaktiviert. Sie aktivieren diesen Zugriff über die lokale Konsole des Hosts. Um Support Zugriff auf Ihr Gateway zu gewähren, melden Sie sich zunächst bei der lokalen Konsole für den Host an, navigieren zur Konsole des Storage Gateways und stellen dann eine Verbindung zum Support-Server her.

Um den Support Zugriff auf Ihr Gateway zu aktivieren

1. Melden Sie sich bei der lokalen Konsole Ihres Hosts an.

   - VMware ESXi — Weitere Informationen finden Sie unterZugreifen auf die lokale Konsole mit VMware ESXi.

- Microsoft Hyper-V: Weitere Informationen finden Sie unter Greifen Sie mit Microsoft auf die lokale Gateway-Konsole zu Hyper-V.

2. Geben Sie bei der Eingabeaufforderung die entsprechende Zahl ein, um Gateway-Konsole auszuwählen.
3. Geben Sie **h** ein, um die Liste der verfügbaren Befehle zu öffnen.
4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, geben Sie im Fenster VERFÜGBARE BEFEHLE **`open-support-channel`** ein, um eine Verbindung zum Storage-Gateway-Kundensupport herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. 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, für die eine Verbindung mit dem Storage-Gateway-Kundensupport hergestellt werden soll. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. 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 Portnummer (Transmission ControlProtocol/User Datagram Protocol (TCP/UDP). Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP 22)-Verbindung zu den Storage-Gateway-Servern her und stellt den Support-Kanal für die Verbindung bereit.

5. Nachdem der Support-Kanal eingerichtet wurde, geben Sie Ihre Support-Servicenummer an, Support damit wir Ihnen bei der Fehlerbehebung weiterhelfen Support können.
6. Wenn die Supportsitzung beendet ist, geben Sie **`q`** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn Sie vom Amazon Web Services Support darüber informiert werden, dass die Support-Sitzung abgeschlossen ist.
7. Geben Sie **`exit`** ein, um sich von der Storage-Gateway-Konsole abzumelden.
8. Folgen Sie den Eingabeaufforderungen, um die lokale Konsole zu beenden.

Problembehandlung: Microsoft Hyper-V-Setup

In der folgenden Tabelle sind typische Probleme aufgeführt, die beim Bereitstellen von Storage Gateway auf der Microsoft Hyper-V-Plattform auftreten können.

Problem	Maßnahme
Sie versuchen, ein Gateway zu importieren und erhalten die folgende Fehlermeldung: „Beim Versuch, die virtuelle Maschine zu importier en, ist ein Serverfehler aufgetreten. Der Import ist fehlgeschlagen. Die Importdateien der virtuelle n Maschine konnten unter dem Speicherort [...] nicht gefunden werden. Sie können eine virtuelle Maschine nur importieren, wenn Sie sie mit Hyper-V erstellt und exportiert haben.“	Dieser Fehler kann aus folgenden Gründen auftreten: • Wenn Sie nicht auf das Stammverzeichnis der entpackten Gateway-Quell-Dateien zeigen. Der letzte Teil des Speicherorts, den Sie im Dialogfeld Virtuelle Maschine importieren angeben, sollte. `AWS-Storage-Gateway` Beispiel: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • 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 Importque lle. Wenn Sie mehrere Gateways von einem Speicherort für entpackte Quelldateien aus erstellen möchten, müssen Sie die Option Virtuelle Maschine kopieren auswählen und im Dialogfeld Virtuelle Maschine importieren das Kontrollkästchen Alle Dateien duplizieren aktivieren.
Sie versuchen, ein Gateway zu importieren, und erhalten die folgende Fehlermeldung:	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. Um dieses

Problem	Maßnahme
„Beim Versuch, die virtuelle Maschine zu importier en, ist ein Serverfehler aufgetreten. Der Import ist fehlgeschlagen. Die Importaufgabe konnte die Datei nicht von [...] kopieren: Die Datei existiert . (0x80070050)“	Problem zu beheben, geben Sie im Bereich auf der linken Seite des Dialogfelds Hyper-V-Einstellungen unter Server neue Speicherorte an.
Sie versuchen, ein Gateway zu importieren, und erhalten die folgende Fehlermeldung: „Beim Versuch, die virtuelle Maschine zu importier en, ist ein Serverfehler aufgetreten. Der Import ist 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.“	Stellen Sie beim Import des Gateways sicher, dass Sie die Option Virtuelle Maschine kopieren auswählen und im Dialogfeld Virtuelle Maschine importieren das Kontrollkästchen Alle Dateien duplizieren aktivieren, um eine neue eindeutige ID für die VM zu erstellen.

Problem	Maßnahme
Sie versuchen, eine Gateway-VM zu starten und erhalten die folgende Fehlermeldung: „Beim Versuch, die ausgewählten virtuelle n Maschinen zu starten, ist ein Fehler aufgetret en. Die Prozessor-Einstell ung für die untergeordnete Partition ist nicht mit der übergeordneten Partition kompatibel. 'AWS-Stor age-Gateway' konnte nicht initialisiert werden. (ID der virtuellen Maschine [...])“	Dieser Fehler wird wahrscheinlich durch eine CPU-Diskrepanz zwischen den CPUs für das Gateway erforderlichen und den CPUs auf dem Host verfügbaren Werten verursacht. Stellen Sie sicher, dass die VM-CPU-Inventur von der zugrunde liegenden Hypervisor unterstützt wird. Weitere Informationen zu den Anforderungen für Storage Gateway finden Sie unter Setup-Anforderungen für File Gateway.

Problem	Maßnahme
Sie versuchen, eine Gateway-VM zu starten und erhalten die folgende Fehlermeldung: „Beim Versuch, die ausgewählten virtuellen Maschinen zu starten, ist ein Fehler aufgetreten. 'AWS-Storage-Gateway' konnte nicht initialisiert werden. (ID der virtuelle n Maschine [...]) Partition konnte nicht erstellt werden: Es sind nicht genügend Systemres sourcen vorhanden, um den angeforderten Dienst abzuschließen. (0x800705 AA)“	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 für Storage Gateway finden Sie unter Setup-Anforderungen für File Gateway.
Ihre Snapshots und Gateway-Software-A ktualisierungen treten zu geringfügig anderen Zeiten als erwartet auf.	Die Uhr der Gateway-VM, weicht möglicherweise von der tatsächli chen 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 Konfiguration eines NTP-Servers (Network Time Protocol) für Ihr Gateway.
Sie müssen die entzippten Microsoft Hyper-V-Dateien für Storage Gateway im Host-Dateisystem ablegen.	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 Hyperviso r herstellen.	Fügen Sie Ihre Benutzer-Anmeldeinformationen als lokaler Administrator für den Hypervisor-Host mithilfe des Sconfig.cmd Tool hinzu.
Möglicherweise stellen Sie eine schlechte Netzwerkl eistung fest, wenn Sie die Virtual Machine Queue (VMQ) für einen Hyper-V-Host aktivieren, der einen Broadcom-Netzwerka dapter verwendet.	Informationen zu einer Problemumgehung finden Sie in der Microsoft-Dokumentation unter Schlechte Netzwerkleistung auf virtuellen Maschinen auf einem Windows Server 2012 Hyper-V-H ost, wenn VMQ eingeschaltet ist.

Fehlerbehebung: Probleme mit dem Amazon EC2 EC2-Gateway

In den folgenden Abschnitten werden typische Probleme beschrieben, die bei der Arbeit mit dem auf Amazon EC2 bereitgestellten Gateway auftreten können. Weitere Informationen über den Unterschied zwischen einem On-Premises-Gateway und einem Gateway, das auf Amazon EC2 bereitgestellt ist, finden Sie unter Stellen Sie einen Amazon EC2 EC2-Standardhost für S3 File Gateway bereit.

Weitere Informationen zur Verwendung des flüchtigen Speichers finden Sie unter Verwendung von kurzlebigem Speicher mit EC2-Gateways.

Themen

- Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.
- EC2-Gateway-Instance in der Instance-Liste nicht gefunden
- Sie möchten sich mit Ihrer Gateway-Instance über die serielle Amazon-EC2-Konsole verbinden
- Sie Support möchten bei der Fehlerbehebung für Ihr Amazon EC2 EC2-Gateway helfen

Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.

Prüfen Sie in der Amazon-EC2-Konsole Folgendes:

- Port 80 ist in der Sicherheitsgruppe geöffnet, die Sie der Instance zugeordnet haben. Weitere Informationen zum Hinzufügen einer Sicherheitsgruppenregel finden Sie unter Hinzufügen einer Sicherheitsgruppenregel im Amazon EC2 EC2-Benutzerhandbuch.
- Die Gateway-Instance ist als laufend markiert. In der Amazon-EC2-Konsole für die Instance sollte der State-Wert der Instance RUNNING lauten.
- Stellen Sie sicher, dass der Typ der Amazon-EC2-Instance die unter Speicheranforderungen beschriebenen Mindestanforderungen erfüllt.

Versuchen Sie erneut, das Gateway zu aktivieren, nachdem Sie das Problem behoben haben. Öffnen Sie dazu die Storage-Gateway-Konsole, wählen Sie Neues Gateway auf Amazon EC2 bereitstellen aus und geben Sie die IP-Adresse der Instance erneut ein.

EC2-Gateway-Instance in der Instance-Liste nicht gefunden

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 auf der Grundlage der Storage Gateway AMI muss mit dem Text **`aws-storage-gateway-ami`** beginnen.
- Wenn Sie über mehrere Instances verfügen, die auf der Storage Gateway AMI basieren, prüfen Sie die Startzeit der Instance, um die richtige Instance zu finden.

Sie möchten sich mit Ihrer Gateway-Instance über die serielle Amazon-EC2-Konsole verbinden

Sie können die serielle Amazon-EC2-Konsole zur Fehlerbehebung beim Booten, bei der Netzwerkkonfiguration und anderen Problemen verwenden. Anweisungen und Tipps zur Fehlerbehebung finden Sie unter Serielle Amazon-EC2-Konsole im Benutzerhandbuch zu Amazon Elastic Compute Cloud.

Sie Support möchten bei der Fehlerbehebung für Ihr Amazon EC2 EC2-Gateway helfen

Storage Gateway bietet eine lokale Konsole, mit der Sie verschiedene Wartungsaufgaben ausführen können, einschließlich des Zugriffs auf Ihr Gateway, Support um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Standardmäßig ist der Support Zugriff auf Ihr Gateway deaktiviert. Sie aktivieren diesen Zugriff über die lokale Amazon EC2 EC2-Konsole. Sie melden sich über Secure Shell (SSH) bei der lokalen Amazon-EC2-Konsole 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 unter Amazon-EC2-Sicherheitsgruppen im Amazon-EC2-Benutzerhandbuch.

Um eine Support Verbindung zu Ihrem Gateway herzustellen, melden Sie sich zunächst bei der lokalen Konsole für die Amazon EC2 EC2-Instance an, navigieren zur Storage Gateway-Konsole und gewähren dann den Zugriff.

So aktivieren Sie den Support Zugriff für ein Gateway, das auf einer Amazon EC2 EC2-Instance bereitgestellt ist

1. Melden Sie sich bei der lokalen Konsole für Ihre Amazon-EC2-Instance an. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Instance im Amazon-EC2-Benutzerhandbuch.

   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**
   >
   > Das *PRIVATE-KEY* ist die `.pem` Datei, die das private Zertifikat des EC2-Schlüsselpaars enthält, das Sie zum Starten der Amazon EC2 EC2-Instance verwendet haben. Weitere

Informationen finden Sie unter Abrufen des öffentlichen Schlüssels für Ihr Schlüsselpaar im Amazon-EC2-Benutzerhandbuch.
Das *INSTANCE-PUBLIC-DNS-NAME* ist der öffentliche DNS-Name (Domain Name System) Ihrer Amazon EC2 EC2-Instance, auf der Ihr Gateway läuft. Sie erhalten diesen öffentlichen DNS-Namen, indem Sie die Amazon-EC2-Instance in der EC2-Konsole auswählen und auf die Registerkarte Beschreibung klicken.

2. Geben Sie an der Eingabeaufforderung **`6 - Command Prompt`** ein, um die Channel-Konsole für Support zu öffnen.
3. Geben Sie **h** ein, um das Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) zu öffnen.
4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, geben Sie im Fenster VERFÜGBARE BEFEHLE **`open-support-channel`** ein, um eine Verbindung zum Storage-Gateway-Kundensupport herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. 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, für die eine Verbindung mit dem Storage-Gateway-Kundensupport hergestellt werden soll. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. 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 Portnummer (Transmission ControlProtocol/User Datagram Protocol (TCP/UDP). Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP 22)-Verbindung zu den Storage-Gateway-Servern her und stellt den Support-Kanal für die Verbindung bereit.

5. Nachdem der Support-Kanal eingerichtet wurde, geben Sie Ihre Support-Servicenummer an, Support damit wir Ihnen bei der Fehlerbehebung weiterhelfen Support können.

6. Wenn die Supportsitzung beendet ist, geben Sie **q** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn Sie vom Amazon Web Services Support darüber informiert werden, dass die Support-Sitzung abgeschlossen ist.
7. Geben Sie **`exit`** ein, um die Storage-Gateway-Konsole zu verlassen.
8. Verwenden Sie die Konsolenmenüs, um sich von der Storage-Gateway-Instance abzumelden.

Fehlerbehebung: Probleme mit der Hardware-Appliance

> **Note**
>
> Hinweis zum Ende der Verfügbarkeit: Ab dem 12. Mai 2025 wird die AWS Storage Gateway Hardware-Appliance nicht mehr angeboten. Bestandskunden mit der AWS Storage Gateway Hardware-Appliance können die Hardware-Appliance bis Mai 2028 weiter nutzen und Support erhalten. Alternativ können Sie den AWS Storage Gateway Service nutzen, um Ihren Anwendungen vor Ort und in der Cloud Zugriff auf praktisch unbegrenzten Cloud-Speicher zu gewähren.

In den folgenden Themen werden Probleme behandelt, die bei der AWS Storage Gateway Hardware-Appliance auftreten können, sowie Vorschläge zu deren Behebung.

Themen

Festlegen der Service-IP-Adresse nicht möglich

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 lässt sich eine Zurücksetzung auf die Werkseinstellungen durchführen?

Wenn Sie Ihre Appliance auf die Werkseinstellungen zurücksetzen müssen, wenden Sie sich an das AWS Storage Gateway Hardware Appliance-Team, um Unterstützung zu erhalten, wie im Abschnitt Support weiter unten beschrieben.

Wie erfolgt der Remote-Neustart?

Wenn Sie einen Remote-Neustart Ihrer Appliance durchführen müssen, können Sie dazu die Dell iDRAC-Verwaltungsschnittstelle verwenden. Weitere Informationen finden Sie unter i DRAC9 Virtueller Energiezyklus: Dell EMC PowerEdge Server aus der Ferne ein- und ausschalten auf der InfoHub Website von Dell Technologies.

Wo erhalten Sie Dell iDRAC-Support?

Der Dell PowerEdge Server ist mit der Dell iDRAC-Verwaltungsschnittstelle ausgestattet. Wir empfehlen Folgendes:

- Wenn Sie die iDRAC-Verwaltungsschnittstelle verwenden, sollten Sie das Standardkennwort ändern. Weitere Informationen zu den iDRAC-Anmeldeinformationen finden Sie unter Dell PowerEdge — Was sind die Standardanmeldedaten für iDRAC? .
- Stellen Sie sicher, dass die Firmware Sicherheitslücken verhindern up-to-date soll.
- Wenn die iDRAC-Netzwerkschnittstelle an einen normalen Port (`em`) verschoben wird, kann dies zu Leistungsproblemen führen oder die normale Funktionsweise der Appliance beeinträchtigen.

Die Seriennummer der Hardware-Appliance lässt sich nicht finden

Sie können die Seriennummer für Ihre AWS Storage Gateway Hardware-Appliance in der Storage Gateway Gateway-Konsole finden.

So finden Sie die Seriennummer der Hardware-Appliance:

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.

2. Wählen Sie im Navigationsmenü auf der linken Seite Hardware aus.
3. Wählen Sie Ihre Hardware-Appliance aus der Liste aus.
4. Suchen Sie das Feld Seriennummer auf der Registerkarte Details für Ihre Appliance.

Wo Sie Hardware-Appliance-Support erhalten?

AWS Informationen zum technischen Support für Ihre Hardware-Appliance finden Sie unter Support.

Das Support Team bittet Sie möglicherweise, den Support-Kanal zu aktivieren, um Ihre Gateway-Probleme aus der Ferne 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.

Um einen Support-Kanal zu öffnen für AWS

1. Öffnen Sie die Hardwarekonsole.
2. Wählen Sie unten auf der Hauptseite der Hardwarekonsole die Option Open Support Channel aus, und drücken Sie dann`Enter`.

   Die zugewiesene Portnummer sollte innerhalb von 30 Sekunden angezeigt werden, sofern keine Probleme mit der Netzwerkkonnektivität oder der Firewall vorliegen. Beispiel:

   Status: Auf Port 19599 geöffnet
3. Notieren Sie sich die Portnummer und geben Sie sie an Support.

Fehlerbehebung: Probleme mit File Gateway

Sie können Ihr File Gateway so konfigurieren, dass Protokolleinträge in eine CloudWatch Amazon-Protokollgruppe geschrieben werden. Wenn Sie dies tun, erhalten Sie Benachrichtigungen über den Status des Gateways und über alle Fehler, auf die das Gateway stößt. Informationen zu diesen Fehler- und Integritätsbenachrichtigungen finden Sie in den CloudWatch Protokollen.

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: 1344 (0x00000540)

Fehler: 1344 (0x00000540)

Bei der Migration von Dateien zu Amazon S3 kann es vorkommen, dass `ERROR 1344 (0x00000540)` Sie versuchen, Dateien mit mehr als 10 Zugriffskontrolleinträgen (ACEs) nach Amazon S3 zu kopieren. Zugriffskontrolleinträge sind in der Access Control List (ACL) aufgeführt.

Das Amazon S3 File Gateway kann nur 10 ACE-Einträge pro Datei oder Ordner speichern.

So beheben Sie den Fehler 1344: NTFS-Sicherheit in das Zielverzeichnis kopieren.

Reduzieren Sie die Anzahl der Einträge in den Windows-Berechtigungen für Dateien oder Ordner, die mehr als 10 Einträge enthalten. Ein gängiger Ansatz besteht darin, eine Gruppe zu erstellen, die die vollständige Liste der Einträge enthält, und dann die Liste der Einträge durch diese einzelne Gruppe zu ersetzen. Sobald die Anzahl der Einträge unter 10 liegt, können Sie erneut versuchen, die Dateien oder Ordner auf das Gateway zu kopieren.

Fehler: GatewayClockOutOfSync

Sie können eine `GatewayClockOutOfSync` Fehlermeldung erhalten, wenn das Gateway eine Differenz von 5 Minuten oder mehr zwischen der lokalen Systemzeit und der von den AWS Storage Gateway Gateway-Servern gemeldeten Zeit feststellt. Probleme mit der Uhrsynchronisierung können sich negativ auf die Konnektivität zwischen dem Gateway und auswirken AWS. Wenn die Gateway-

Uhr nicht synchron ist, können I/O-Fehler bei NFS- und SMB-Verbindungen auftreten, und bei SMB-Benutzern können Authentifizierungsfehler auftreten.

Um einen Fehler zu beheben GatewayClockOutOfSync

- Überprüfen Sie die Netzwerkkonfiguration zwischen dem Gateway und dem NTP-Server. Weitere Informationen zum Synchronisieren der Gateway-VM-Zeit und zum Aktualisieren der NTP-Serverkonfiguration finden Sie unter Konfiguration eines Network Time Protocol (NTP) -Servers für Ihr Gateway -Servers für Ihr Gateway.

Fehler: InaccessibleStorageClass

Sie können eine `InaccessibleStorageClass` Fehlermeldung erhalten, wenn ein Objekt die Amazon S3 S3-Standard-Speicherklasse verlassen hat.

Ihr File Gateway stößt normalerweise auf diesen Fehler, wenn es versucht, ein Objekt entweder in den Amazon S3-Bucket hochzuladen oder ein Objekt aus dem Amazon S3 S3-Bucket zu lesen. Im Allgemeinen bedeutet dieser Fehler, dass das Objekt zu Amazon Glacier verschoben wurde und sich entweder in der Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive befindet.

Ihr S3 File Gateway kann einen Cache-Bericht generieren, der alle Dateien im Gateway-Cache auflistet, die aufgrund dieses Fehlers derzeit nicht auf Amazon S3 hochgeladen werden können. Die Informationen in diesem Bericht können Ihnen bei der Lösung von Problemen mit Support Ihrer Gateway-, Amazon S3- oder IAM-Konfiguration helfen. Weitere Informationen finden Sie unter Cache-Bericht erstellen.

Um einen InaccessibleStorageClass Fehler zu beheben

- Stellen Sie das Objekt aus der Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive wieder auf die ursprüngliche Speicherklasse in S3 zurück.

  Wenn Sie das Objekt im S3-Bucket wiederherstellen, um einen Upload-Fehler zu beheben, wird die Datei schließlich hochgeladen. Wenn Sie das Objekt wiederherstellen, um einen Lesefehler zu beheben, kann der SMB- oder NFS-Client des File Gateways die Datei dann lesen.

Fehler: InvalidObjectState

Sie können eine `InvalidObjectState` Fehlermeldung erhalten, wenn ein anderer Writer als das angegebene File Gateway die angegebene Datei im angegebenen Amazon S3 S3-Bucket ändert.

Daher entspricht der Status der Datei für das File Gateway nicht dem Status in Amazon S3. Alle nachfolgenden Uploads der Datei auf Amazon S3 oder Abrufe der Datei von Amazon S3 schlagen fehl.

Ihr S3 File Gateway kann einen Cache-Bericht generieren, der alle Dateien im Gateway-Cache auflistet, die aufgrund dieses Fehlers derzeit nicht auf Amazon S3 hochgeladen werden können. Die Informationen in diesem Bericht können Ihnen bei der Lösung von Problemen mit Support Ihrer Gateway-, Amazon S3- oder IAM-Konfiguration helfen. Weitere Informationen finden Sie unter Cache-Bericht erstellen.

Um einen InvalidObjectState Fehler zu beheben

Wenn der Vorgang, der die Datei ändert`S3GetObject`, `S3Upload` oder ist, gehen Sie wie folgt vor:

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 ist, laden Sie diese Version herunter. Sie können dies mit dem AWS-Managementkonsole oder tun AWS CLI.
2. Löschen Sie die Datei in Amazon S3 mit dem AWS-Managementkonsole oder AWS CLI.
3. Löschen Sie die Datei mit Ihrem SMB- oder NFS-Client vom File Gateway.
4. Kopieren Sie die neueste Version der Datei, die Sie in Schritt 1 gespeichert haben, mit Ihrem SMB- oder NFS-Client nach Amazon S3. Tun Sie dies über Ihr File Gateway.

Fehler: ObjectMissing

Sie können eine `ObjectMissing` Fehlermeldung erhalten, wenn ein anderer Writer als das angegebene File Gateway die angegebene Datei aus dem S3-Bucket löscht. Alle nachfolgenden Uploads zu Amazon S3 oder Abrufe von Amazon S3 für das Objekt schlagen fehl.

Ihr S3 File Gateway kann einen Cache-Bericht generieren, der alle Dateien im Gateway-Cache auflistet, die aufgrund dieses Fehlers derzeit nicht auf Amazon S3 hochgeladen werden können. Die Informationen in diesem Bericht können Ihnen bei der Lösung von Problemen mit Support Ihrer Gateway-, Amazon S3- oder IAM-Konfiguration helfen. Weitere Informationen finden Sie unter Cache-Bericht erstellen.

Um einen ObjectMissing Fehler zu beheben

Wenn der Vorgang, der die Datei ändert`S3GetObject`, `S3Upload` oder ist, gehen Sie wie folgt vor:

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 vom File Gateway.
3. Kopieren Sie die neueste Version der Datei, die Sie in Schritt 1 gespeichert haben, mit Ihrem SMB- oder NFS-Client. Tun Sie dies über Ihr File Gateway.

Fehler: RoleTrustRelationshipInvalid

Dieser Fehler wird angezeigt, wenn die IAM-Rolle für eine Dateifreigabe eine falsch konfigurierte IAM-Vertrauensstellung hat (d. h., die IAM-Rolle vertraut dem genannten Storage Gateway Gateway-Prinzipal nicht). `storagegateway.amazonaws.com` Infolgedessen wäre das File Gateway nicht in der Lage, die Anmeldeinformationen für die Ausführung von Vorgängen auf dem S3-Bucket abzurufen, der die Dateifreigabe unterstützt.

Um einen RoleTrustRelationshipInvalid Fehler zu beheben

- Verwenden Sie die IAM-Konsole oder die IAM-API, um das Objekt `storagegateway.amazonaws.com` als Principal einzubinden, das von Ihren Dateifreigaben als vertrauenswürdig eingestuft wird. IAMrole Informationen zur IAM-Rolle finden Sie unter Tutorial: AWS Kontoübergreifendes Delegieren des Zugriffs mithilfe von IAM-Rollen.

Fehler: S3 AccessDenied

Sie können eine `S3AccessDenied` Fehlermeldung für die Amazon S3 S3-Bucket Access-Rolle AWS Identity and Access Management (IAM) einer Dateifreigabe erhalten. In diesem Fall lässt die im Fehler angegebene IAM-Rolle für den S3-Bucket-Zugriff den betreffenden Vorgang nicht zu. `roleArn` Der Vorgang ist aufgrund der Berechtigungen für die Objekte in dem durch das Amazon S3 S3-Präfix angegebenen Verzeichnis nicht zulässig.

Ihr S3 File Gateway kann einen Cache-Bericht generieren, der alle Dateien im Gateway-Cache auflistet, die aufgrund dieses Fehlers derzeit nicht auf Amazon S3 hochgeladen werden können. Die Informationen in diesem Bericht können Ihnen bei der Lösung von Problemen mit Support Ihrer Gateway-, Amazon S3- oder IAM-Konfiguration helfen. Weitere Informationen finden Sie unter Cache-Bericht erstellen.

Um einen AccessDenied S3-Fehler zu beheben

- Ändern Sie die Amazon S3 S3-Zugriffsrichtlinie, die `roleArn` im File Gateway-Zustandsprotokoll angehängt ist, um Berechtigungen für den Amazon S3 S3-Vorgang zuzulassen. 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. Informationen zu Amazon S3 S3-Berechtigungen finden Sie unter Spezifizieren von Berechtigungen in einer Richtlinie im Amazon Simple Storage Service-Benutzerhandbuch.

  Die folgenden Operationen können zum Auftreten des Fehlers `S3AccessDenied` führen.

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

Fehler: DroppedNotifications

Möglicherweise wird anstelle anderer erwarteter Typen von CloudWatch Protokolleinträgen ein `DroppedNotifications` Fehler angezeigt, wenn der freie Speicherplatz auf der Root-Festplatte Ihres Gateways weniger als 1 GB beträgt oder wenn innerhalb eines Intervalls von 1 Minute mehr als 100 Integritätsbenachrichtigungen generiert werden. Unter diesen Umständen generiert das Gateway vorsichtshalber CloudWatch keine detaillierten Protokollbenachrichtigungen mehr.

Um einen Fehler zu beheben DroppedNotifications

1. Überprüfen Sie anhand der `Root Disk Usage` Metrik auf der Registerkarte Überwachung für Ihr Gateway in der Storage Gateway Gateway-Konsole, ob der verfügbare Root-Festplattenspeicher knapp wird.
2. Erhöhen Sie die Größe der Root-Speicherfestplatte des Gateways, wenn der verfügbare Speicherplatz weniger als 1 GB beträgt. Anweisungen finden Sie in der Dokumentation Ihres Hypervisors für virtuelle Maschinen.

   Informationen zur Erhöhung der Root-Festplattengröße für Amazon EC2 EC2-Gateways finden Sie unter Änderungen an Ihren EBS-Volumes beantragen im Amazon Elastic Compute Cloud-Benutzerhandbuch.

> **Note**
>
> Es ist nicht möglich, die Root-Festplattengröße für die AWS Storage Gateway Hardware Appliance zu erhöhen.

3. Starten Sie Ihr Gateway neu.

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 Reset durch vSphere High Availability Application Monitoring dieses Ereignis auslösen.

Wenn Ihr Gateway in einer solchen Umgebung ausgeführt wird, überprüfen Sie, ob die `HealthCheckFailure` Benachrichtigung vorhanden ist, und lesen Sie im VMware Ereignisprotokoll für die VM nach.

Benachrichtigung: Reboot

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-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.

Fehlerbehebung: Sicherheitsscans zeigen offene NFS-Ports

Bestimmte NFS-Ports sind standardmäßig aktiviert, auch auf Gateways, die Sie nur mit SMB-Dateifreigaben verwenden. Wenn Sie Sicherheitssoftware von Drittanbietern wie Qualys verwenden, um das Netzwerk zu scannen, in dem Ihr File Gateway installiert ist, könnten die Scanergebnisse diese offenen NFS-Ports als potenzielle Sicherheitslücke melden. Wenn Sie Ihr Gateway nur mit SMB-Dateifreigaben verwenden und die ungenutzten NFS-Ports aus Sicherheitsgründen deaktivieren möchten, gehen Sie wie folgt vor:

So deaktivieren Sie NFS-Ports auf einem File Gateway:

1. Greifen Sie mit dem unter beschriebenen Verfahren auf die Eingabeaufforderung der lokalen Gateway-Konsole zuAusführen von Storage Gateway-Befehlen auf der lokalen Konsole.
2. Geben Sie die folgenden Befehle ein, um den NFS-Verkehr zu deaktivieren:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

3. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die blockierten NFS-Ports in den IP-Tabellen angezeigt werden:

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

Problembehandlung: Verwendung von CloudWatch Metriken

Im Folgenden finden Sie Informationen zu Maßnahmen zur Behebung von Problemen mithilfe von CloudWatch Amazon-Metriken mit Storage Gateway.

Themen

Ihr Gateway reagiert langsam beim Durchsuchen von Verzeichnissen

Wenn Ihr File Gateway langsam reagiert, wenn Sie den ls Befehl ausführen oder Verzeichnisse durchsuchen, überprüfen Sie die `IndexEviction` CloudWatch Messwerte `IndexFetch` und:

- Wenn die `IndexFetch` Metrik größer als 0 ist, wenn Sie einen `ls` Befehl ausführen oder Verzeichnisse durchsuchen, wurde Ihr File Gateway ohne Informationen über den Inhalt des betroffenen Verzeichnisses gestartet und musste auf Amazon S3 FSx zugreifen. Nachfolgende Versuche, den Inhalt dieses Verzeichnisses aufzulisten, sollten schneller ausgeführt werden.
- Wenn die `IndexEviction` Metrik größer als 0 ist, bedeutet dies, dass Ihr File Gateway die Grenze dessen erreicht hat, was es zu diesem Zeitpunkt in seinem Cache verwalten kann. In diesem Fall muss Ihr File Gateway Speicherplatz aus dem Verzeichnis freigeben, auf das zuletzt zugegriffen wurde, um ein neues Verzeichnis aufzulisten. Wenn dies häufig vorkommt und die Leistung beeinträchtigt wird, wenden Sie sich an Support.

  Besprechen Sie mit Support dem Inhalt des entsprechenden S3-Buckets und den Empfehlungen zur Leistungssteigerung auf der Grundlage Ihres Anwendungsfalls.

Ihr Gateway reagiert nicht

Wenn Ihr File Gateway nicht reagiert, gehen Sie wie folgt vor:

- Wenn kürzlich ein Neustart oder ein Softwareupdate vorgenommen wurde, überprüfen Sie die Metrik `IOWaitPercent`. Diese Metrik zeigt den Prozentsatz der Zeit, in der sich die CPU im Leerlauf befindet, wenn eine I/O Festplattenanforderung aussteht. In einigen Fällen ist dieser Prozentsatz möglicherweise hoch (10 oder höher) und angestiegen, nachdem der Server neu gestartet oder aktualisiert wurde. In diesen Fällen kann es sein, dass Ihr File Gateway bei der Neuerstellung des Index-Caches in RAM durch eine langsame Root-Festplatte einen Engpass

bekommt. Sie können dieses Problem beheben, indem Sie einen schnelleren physischen Datenträger für den Stamm-Datenträger verwenden.

- Wenn die `MemUsedBytes` Metrik der Metrik entspricht oder fast der `MemTotalBytes` Metrik entspricht, geht Ihrem File Gateway der verfügbare Arbeitsspeicher aus. Stellen Sie sicher, dass Ihr File Gateway mindestens über den erforderlichen Arbeitsspeicher verfügt. Falls dies bereits der Fall ist, sollten Sie erwägen, Ihrem File Gateway je nach Arbeitslast und Anwendungsfall mehr RAM hinzuzufügen.

  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 angeschlossen sind, müssen Sie Ihrem File Gateway möglicherweise mehr RAM hinzufügen.

Ihr Gateway überträgt langsam Daten an Amazon S3

Wenn Ihr File Gateway Daten langsam an Amazon S3 überträgt, gehen Sie wie folgt vor:

- Wenn die `CachePercentDirty` Metrik 80 oder höher ist, schreibt Ihr File Gateway Daten schneller auf die Festplatte, als es die Daten auf Amazon S3 hochladen kann. Erwägen Sie, die Bandbreite für den Upload von Ihrem File Gateway zu erhöhen, eine oder mehrere Cache-Festplatten hinzuzufügen oder Client-Schreibvorgänge zu verlangsamen.
- Wenn die `CachePercentDirty` Metrik niedrig ist, überprüfen Sie die `IoWaitPercent` Metrik. Wenn der `IoWaitPercent` Wert größer als 10 ist, hat Ihr File Gateway möglicherweise einen Engpass aufgrund der Geschwindigkeit des lokalen Cache-Laufwerks. Wir empfehlen lokale Solid-State-Drive-Festplatten (SSD) für Ihren 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 `S3PutObjectRequestTimeS3UploadPartRequestTime`, oder hoch `S3GetObjectRequestTime` sind, liegt möglicherweise ein Netzwerkengpass vor. Versuchen Sie, Ihr Netzwerk zu analysieren, um sicherzustellen, dass das Gateway über die erwartete Bandbreite verfügt.

Ihr Gateway führt mehr Amazon S3 S3-Operationen als erwartet aus

Wenn Ihr File Gateway mehr Amazon S3 S3-Operationen als erwartet ausführt, überprüfen Sie die `FilesRenamed` Metrik. Die Ausführung von Umbenennungsvorgängen in Amazon S3 ist teuer. Optimieren Sie Ihren Arbeitsablauf, 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 wiedergegeben werden, überprüfen Sie die `FilesFailingUpload` Metrik. Wenn die Metrik meldet, dass einige Dateien nicht hochgeladen werden können, überprüfen Sie Ihre Statusmeldungen. Wenn Dateien nicht hochgeladen werden können, generiert das Gateway eine Statusmeldung mit weiteren Informationen zu dem Problem.

Ihr Gateway-Backup-Job schlägt fehl oder es treten Fehler beim Schreiben auf Ihr Gateway auf

Wenn Ihr File Gateway-Backup-Job fehlschlägt oder Fehler beim Schreiben auf Ihr File Gateway auftreten, gehen Sie wie folgt vor:

- Wenn die `CachePercentDirty` Metrik 90 Prozent oder mehr beträgt, kann Ihr File Gateway keine neuen Schreibvorgänge auf die Festplatte akzeptieren, da auf der Cache-Festplatte nicht genügend Speicherplatz verfügbar ist. Um zu sehen, wie schnell Ihr File Gateway auf Amazon S3 FSx hochlädt, sehen Sie sich die `CloudBytesUploaded` Metrik an. Vergleichen Sie diese Metrik mit der `WriteBytes` Metrik, die zeigt, wie schnell der Client Dateien auf Ihr File Gateway schreibt. Wenn der SMB-Client schneller auf Ihr File Gateway schreibt, als er auf Amazon S3 FSx hochladen kann, fügen Sie mehr Cache-Festplatten hinzu, um die Größe des Backup-Jobs mindestens abzudecken. Oder erhöhen Sie die Upload-Bandbreite.
- Wenn eine große Dateikopie, z. B. ein Backup-Job, fehlschlägt, die `CachePercentDirty` Metrik jedoch unter 80 Prozent liegt, hat Ihr File Gateway möglicherweise ein clientseitiges Sitzungs-Timeout erreicht. Für SMB können Sie dieses Timeout mit dem Befehl erhöhen. PowerShell `Set-SmbClientConfiguration -SessionTimeout 300` 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: Probleme mit der Dateifreigabe

Informationen über die Aktionen finden Sie nachfolgend, Aktionen die Sie vornehmen können, wenn Sie unerwartete Probleme mit Ihrer Datenfreigabe haben.

Themen

Die Dateifreigabe blieb im Status ERSTELLEN, AKTUALISIEREN oder LÖSCHEN hängen

Der Dateifreigabestatus fasst den Zustand Ihrer Dateifreigabe zusammen. Wenn Ihre S3 File Gateway-Dateifreigabe im `DELETING` Status`CREATING`, oder feststeckt`UPDATING`, gehen Sie wie folgt vor, um das Problem zu identifizieren und zu beheben.

Bestätigen Sie die IAM-Rollenberechtigungen und die Vertrauensbeziehung

Die mit Ihrer Dateifreigabe verknüpfte AWS Identity and Access Management (IAM-) Rolle muss über ausreichende Berechtigungen für den Zugriff auf den Amazon S3 S3-Bucket verfügen.

Darüber hinaus muss die Vertrauensrichtlinie der Rolle dem Storage Gateway Gateway-Dienst Berechtigungen zur Übernahme der Rolle gewähren.

So überprüfen Sie die IAM-Rollenberechtigungen:

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen.
3. Wählen Sie die IAM-Rolle aus, die Ihrer Dateifreigabe zugeordnet ist.
4. Wählen Sie die Registerkarte Trust relationships (Vertrauensstellungen).
5. Vergewissern Sie sich, dass Storage Gateway als vertrauenswürdige Entität aufgeführt ist. Wenn Storage Gateway keine vertrauenswürdige Entität ist, wählen Sie Vertrauensstellung bearbeiten aus und fügen Sie dann die folgende Richtlinie hinzu:

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

6. Stellen Sie sicher, dass die IAM-Rolle über die richtigen Berechtigungen verfügt und dass der Amazon S3 S3-Bucket in der IAM-Richtlinie als Ressource aufgeführt ist. Weitere Informationen finden Sie unter Zugriff auf einen Amazon S3 S3-Bucket gewähren.

> **Note**
>
> Verwenden Sie eine Vertrauensbeziehungsrichtlinie, die Schlüssel zum Bedingungskontext enthält, um Probleme mit dienstübergreifendem Zugriff auf Stellvertreter zu vermeiden. Weitere Informationen finden Sie unter the section called “Serviceübergreifende Confused-Deputy-Prävention”.

Stellen Sie sicher AWS , dass STS in Ihrer Region aktiviert ist

Fileshares können in dem `UPDATING` Bundesstaat `CREATING` oder hängen bleiben, wenn AWS -Security-Token-Service (AWS STS) in Ihrer AWS Region deaktiviert ist.

Um den AWS STS-Status zu überprüfen:

1. Öffnen Sie die AWS Identity and Access Management Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
3. Vergewissern Sie sich im Abschnitt Security Token Service (STS), dass der Status für die AWS Region, in der Sie die Dateifreigabe erstellen möchten, Aktiv lautet.
4. Wenn der Status Inaktiv ist, wählen Sie Aktivieren aus, um die Aktivierung AWS STS in dieser Region durchzuführen.

Stellen Sie sicher, dass der S3-Bucket existiert und die Benennungsregeln

Für Ihre Dateifreigabe ist ein gültiger Amazon S3 S3-Bucket erforderlich, der den Amazon S3 S3-Benennungskonventionen entspricht.

So verifizieren Sie Ihren S3-Bucket:

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Vergewissern Sie sich, dass der Amazon S3 S3-Bucket, der Ihrer Dateifreigabe zugeordnet ist, existiert. Wenn der Bucket nicht existiert, erstellen Sie ihn. Nachdem Sie den Bucket erstellt haben, sollte sich der Status der Dateifreigabe auf ändern`AVAILABLE`. Weitere Informationen finden Sie unter Erstellen eines Buckets im Benutzerhandbuch zu Amazon Simple Storage Service.
3. Stellen Sie sicher, dass Ihr Bucket-Name den Regeln für die Bucket-Benennung im Amazon Simple Storage Service-Benutzerhandbuch entspricht.

> **Note**
>
> S3 File Gateway unterstützt keine Amazon S3 S3-Buckets mit Punkten (`.`) im Bucket-Namen.

Erzwingt das Löschen einer Dateifreigabe, die im Status DELETING feststeckt

Wenn Sie eine Dateifreigabe löschen, entfernt das Gateway die Freigabe aus dem zugehörigen Amazon S3 S3-Bucket. Daten, die gerade hochgeladen werden, werden jedoch weiterhin hochgeladen, bevor der Löschvorgang abgeschlossen ist. Während dieses Vorgangs zeigt die Dateifreigabe einen `DELETING` Status an.

> **Important**
>
> Prüfen Sie anhand der CloudWatch Amazon-Metrik `CachePercentDirty` für Ihr Gateway, wie viele Daten noch hochgeladen werden müssen. Weitere Informationen zu Storage Gateway Gateway-Metriken finden Sie unterthe section called “Überwachung Ihres S3 File Gateway FSx ”.

Wenn Sie nicht warten möchten, bis alle laufenden Uploads abgeschlossen sind, können Sie das Löschen der Dateifreigabe erzwingen.

So erzwingen Sie das Löschen einer Dateifreigabe:

1. Öffnen Sie die Storage Gateway Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/.
2. Wählen Sie im Navigationsbereich die Option Dateifreigaben aus.
3. Wählen Sie die Dateifreigabe aus, die Sie löschen möchten.
4. Wählen Sie die Registerkarte Details und überprüfen Sie die Meldung Diese Dateifreigabe wird gelöscht.
5. Überprüfen Sie die ID der Dateifreigabe in der Nachricht und wählen Sie dann das Bestätigungsfeld aus.

   > **Note**
   >
   > Sie können den erzwungenen Löschvorgang nicht rückgängig machen.

6. Wählen Sie „Jetzt löschen erzwingen“.

Alternativ können Sie den AWS CLI delete-file-shareBefehl verwenden, wobei der `--force-delete` Parameter auf gesetzt ist`true`.

> **Important**
>
> Bevor Sie das Löschen einer Dateifreigabe erzwingen, vergewissern Sie sich, dass sich Ihr Gateway nicht in einem bestimmten `OFFLINE` Zustand befindet. Wenn das Gateway offline ist, lösen Sie zunächst das Offline-Problem. Weitere Informationen finden Sie unter the section called “Fehlerbehebung: Gateway-Offline-Probleme”.

Wenn die virtuelle Gateway-Maschine (VM) bereits gelöscht wurde, müssen Sie das Gateway aus der Storage Gateway Gateway-Konsole löschen, um alle zugehörigen Dateifreigaben zu entfernen, einschließlich der Dateifreigaben, die im `DELETING` Status hängen geblieben sind. Weitere Informationen finden Sie unter the section called “Ihr Gateway löschen und Ressourcen entfernen”.

Fehlerbehebung bei Netzwerk-Verbindungsproblemen

Netzwerkprobleme können verhindern, dass Ihre Dateifreigabe den `DELETING` Status `CREATINGUPDATING`, oder verlässt. Zu den häufigsten Netzwerkproblemen gehören:

- Ihr Gateway ist offline oder die Gateway-VM wurde gelöscht.
- Der Netzwerkzugriff zwischen Storage Gateway und dem Amazon S3 S3-Serviceendpunkt ist blockiert.
- Der Amazon S3-Amazon-VPC-Endpunkt, den das Gateway für die Kommunikation mit Amazon S3 verwendet, wurde gelöscht.
- Die erforderlichen Netzwerkports sind nicht geöffnet oder das Netzwerk-Routing ist falsch konfiguriert.

Testen Sie die S3-Konnektivität von der lokalen Gateway-Konsole aus

So testen Sie die S3-Konnektivität:

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Weitere Informationen finden Sie unter the section called “Melden Sie sich bei der lokalen File Gateway-Konsole an”.
2. Geben Sie im Hauptmenü Storage Gateway — Konfiguration die Nummer ein, die Test S3 Connectivity entspricht.
3. Wählen Sie den Amazon S3 S3-Endpunkttyp:

- Wählen Sie für Amazon S3-Verkehr, der über einen Internet Gateway-, NAT Gateway-, Transit Gateway- oder Amazon S3 Gateway Amazon VPC-Endpunkt fließt, die Option Öffentlich.
- Wählen Sie für Amazon S3 S3-Verkehr, der über einen Amazon VPC-Endpunkt mit Amazon S3-Schnittstelle fließt, VPC () PrivateLink.
- Wählen Sie für einen FIPS-Endpunkt die FIPS-Option.

4. Geben Sie die Amazon S3 S3-Bucket-Region ein.
5. Wenn Sie einen Amazon VPC-Endpunkt verwenden, geben Sie den DNS-Namen Amazon S3 S3-Amazon-VPC-Endpunkts ein (z. B.`vpce-0329c2790456f2d01-0at85l34`).

Das Gateway führt automatisch einen Konnektivitätstest durch, der sowohl die Netzwerkverbindung als auch die SSL-Verbindung validiert. Wenn der Test fehlschlägt:

- Netzwerktestfehler — Wird normalerweise durch Firewallregeln, Sicherheitsgruppenkonfigurationen oder falsches Netzwerk-Routing verursacht. Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind und das Netzwerk-Routing korrekt konfiguriert ist.
- SSL-Testfehler — Zeigt an, dass zwischen Ihrer Gateway-VM und den Amazon S3 S3-Service-Endpunkten eine SSL- oder Deep Packet Inspection stattfindet. Deaktivieren Sie SSL und Deep Packet Inspection für Storage Gateway Gateway-Verkehr.

Überprüfen Sie die Proxykonfiguration

Wenn Ihr Gateway einen Proxyserver verwendet, stellen Sie sicher, dass der Proxy die Netzwerkkommunikation nicht blockiert.

Um die Proxykonfiguration zu überprüfen:

1. Geben Sie im Hauptmenü Storage Gateway — Konfiguration die Nummer ein, die der HTTP/SOCKS-Proxykonfiguration entspricht.
2. Wählen Sie die Option, um die aktuelle Netzwerk-Proxykonfiguration anzuzeigen.
3. Wenn ein Proxy konfiguriert ist, stellen Sie sicher, dass Amazon S3 S3-Verkehr vom Storage Gateway über Port 3128 (oder Ihren konfigurierten Listener-Port) zum Proxy-Server und dann über Port 443 zum Amazon S3 S3-Endpunkt fließen kann.
4. Vergewissern Sie sich, dass der Proxy oder die Firewall den Datenverkehr zu und von den Netzwerkports und Dienstendpunkten zulässt, die von Storage Gateway benötigt werden. Weitere Informationen finden Sie unter den erforderlichen Netzwerkports.

Wenn die Probleme weiterhin bestehen, können Sie die Proxykonfiguration vorübergehend entfernen, um festzustellen, ob der Proxy das Problem verursacht.

Überprüfen Sie die Sicherheitsgruppen und das Netzwerk-Routing

- Für Gateways auf Amazon EC2 — Vergewissern Sie sich, dass für die Sicherheitsgruppe Port 443 für Amazon S3 S3-Endpunkte geöffnet ist. Stellen Sie sicher, dass die Routing-Tabelle des Amazon EC2-Subnetzes Amazon S3 S3-Verkehr ordnungsgemäß an Amazon S3 S3-Endpunkte weiterleitet. Weitere Informationen finden Sie unter den erforderlichen Netzwerkports.
- Für lokale Gateways — Vergewissern Sie sich, dass die Firewall-Regeln die erforderlichen Ports zulassen und dass lokale Routing-Tabellen den Amazon S3 S3-Verkehr ordnungsgemäß an Amazon S3 S3-Endpunkte weiterleiten. Weitere Informationen finden Sie unter Erforderliche Netzwerkports.
- VPC-Endpunkte — Stellen Sie sicher, dass der Amazon S3 Amazon VPC-Endpunkt, der vom Gateway verwendet wird, nicht gelöscht wurde. Wenn der Amazon VPC-Endpunkt gelöscht wird und das Gateway keine öffentliche IP-Adresse hat, kann das Gateway nicht mit Amazon S3 kommunizieren.

Sie können keine Dateifreigabe erstellen

1. Wenn Sie keine Dateifreigabe erstellen können, weil Ihre Dateifreigabe im Status CREATING feststeckt, überprüfen Sie, ob der S3-Bucket, dem Sie Ihre Dateifreigabe zugeordnet haben, existiert. Weitere Informationen über wie dies getan wird finden Sie unter Die Dateifreigabe blieb im Status ERSTELLEN, AKTUALISIEREN oder LÖSCHEN hängen, oben.
2. Wenn der S3-Bucket existiert, vergewissern Sie AWS -Security-Token-Service sich, dass er in der Region aktiviert ist, in der Sie die Dateifreigabe erstellen. Wenn ein Sicherheitstoken nicht aktiv ist, sollten Sie es aktivieren. Informationen zur Aktivierung eines Tokens mithilfe von AWS -Security-Token-Service finden Sie unter Aktivieren und Deaktivieren von AWS STS in einer AWS Region im IAM-Benutzerhandbuch.

SMB-Dateifreigaben ermöglichen nicht mehrere unterschiedliche 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 zugewiesenen S3-Bucket schreiben

Wir empfehlen nicht, Ihren S3-Bucket so zu konfigurieren, dass mehrere Dateifreigaben in einen S3-Bucket schreiben können. 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 File Gateway.

Benachrichtigung für gelöschte Protokollgruppen bei Verwendung von Audit-Logs

Wenn die Protokollgruppe nicht existiert, kann der Benutzer auf den Link zur Protokollgruppe unter der Nachricht klicken, um entweder eine neue Protokollgruppe zu erstellen oder eine bestehende Protokollgruppe als Ziel für Audit-Logs zu verwenden

Sie können keine Dateien in Ihren S3-Bucket hochladen

Wenn Sie keine Dateien in Ihren S3-Bucket hochladen können, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie dem Amazon S3 File Gateway den erforderlichen Zugriff gewährt haben, um Dateien in Ihren S3-Bucket hochzuladen. Weitere Informationen finden Sie unter Zugriff auf einen Amazon S3 S3-Bucket gewähren.
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 File Gateway.

3. Wenn Ihr File Gateway SSE-KMS oder DSSE-KMS für die Verschlüsselung verwendet, stellen Sie sicher, dass die der Dateifreigabe zugeordnete IAM-Rolle die Berechtigungen kms:Encrypt, kms:Decrypt, kms: *, kms: und kms: umfasst. ReEncrypt GenerateDataKey DescribeKey Weitere Informationen finden Sie unter Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für Storage Gateway.

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 (serverseitige Verschlüsselung mit AWS KMS—verwalteten Schlüsseln) zum Standard für Ihren S3-Bucket machen, werden Objekte, die ein Amazon S3 File Gateway im Bucket speichert, nicht mit SSE-KMS verschlüsselt. Standardmäßig verwendet ein S3 File Gateway 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 so zu ändern, dass 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. Dieses Update gilt für Objekte, die nach dem Update in den S3-Buckets gespeichert wurden. Weitere Informationen finden Sie unter Datenverschlüsselung mitAWS KMS.

Änderungen, die direkt in einem S3-Bucket mit aktivierter Objektversionierung vorgenommen wurden, können sich darauf auswirken, was Sie in Ihrer Dateifreigabe sehen

Wenn in Ihren S3-Bucket Objekte von einem anderen Client geschrieben wurden, ist Ihre Ansicht des S3-Buckets möglicherweise up-to-date nicht auf die Versionierung von S3-Bucket-Objekten zurückzuführen. 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 erhält

einen separaten ID-Wert, z. B. `file1.jpg`: `ID="xxx"` und `file1.jpg`: `ID="yyy"`. Die Anzahl der Objekte mit identischem Namen und ihre Lebensdauer werden durch die Lebenszyklusrichtlinien von Amazon S3 gesteuert. Weitere Informationen zu diesen Amazon S3-Konzepten finden Sie unter Using Versioning and Object Lifecycle Management im Amazon S3 Developer Guide.

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.

In Ihrem S3 File Gateway sind die angezeigten Dateien die neuesten Versionen von Objekten in einem S3-Bucket zum Zeitpunkt des Abrufs des Objekts oder der Aktualisierung des Caches. S3 File Gateways ignorieren alle älteren Versionen oder Objekte, die zum Löschen 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 eines benannten Objekts mit Ihren Änderungen, und diese Version wird zur neuesten Version.

Ihr S3 File Gateway liest weiterhin aus der früheren Version, und Aktualisierungen, die Sie vornehmen, basieren auf der früheren Version, falls dem S3-Bucket außerhalb Ihrer Anwendung eine neue Version hinzugefügt wird. Um die neueste Version eines Objekts zu lesen, verwenden Sie die RefreshCacheAPI-Aktion oder aktualisieren Sie es von der Konsole aus, wie unter beschriebenAktualisieren des Amazon S3 S3-Bucket-Objekt-Caches.

> **Important**
>
> Es wird nicht empfohlen, Objekte oder Dateien von außerhalb der Dateifreigabe in Ihren S3 File Gateway S3-Bucket zu schreiben.

Beim Schreiben in einen S3-Bucket mit aktivierter Versionierung erstellt das Amazon S3 File Gateway möglicherweise mehrere Versionen von Amazon S3 S3-Objekten

Wenn die Objektversionierung aktiviert ist, können bei jeder Aktualisierung einer Datei von Ihrem NFS- oder SMB-Client mehrere Versionen eines Objekts in Amazon S3 erstellt werden. Im Folgenden finden Sie 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 auf das S3 File Gateway geschrieben wird, lädt das S3 File Gateway die Daten der Datei auf Amazon S3 hoch, gefolgt von ihren Metadaten (Besitzverhältnisse, Zeitstempel usw.). Durch das Hochladen der Dateidaten wird ein Amazon S3 S3-Objekt erstellt, und beim Hochladen der Metadaten für die Datei werden die Metadaten für das Amazon S3 S3-Objekt aktualisiert. Durch diesen Vorgang wird eine weitere Version des Objekts erstellt, 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 auf das File Gateway fertig ist. Einige Gründe hierfür sind die Freigabe von Cache-Speicherplatz oder eine hohe Schreibgeschwindigkeit 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 existieren, 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 von Same-Region-Replication (SRR) oder Cross-Region-Replication (CRR) zwischen S3-Buckets erhöht den Speicherverbrauch. Weitere Informationen zur Replikation finden Sie unter Replikation.

> **Important**
>
> Konfigurieren Sie die Replikation zwischen S3-Buckets erst, wenn Sie wissen, wie viel Speicherplatz verwendet wird, wenn die Objektversionierung aktiviert ist.

Die Verwendung von versionierten S3-Buckets kann den Speicherplatz in Amazon S3 erheblich erhöhen, da bei jeder Änderung an einer Datei eine neue Version des S3-Objekts erstellt wird. Standardmäßig speichert Amazon S3 weiterhin all diese Versionen, es sei denn, Sie erstellen ausdrücklich eine Richtlinie, um dieses Verhalten außer Kraft zu setzen und die Anzahl der gespeicherten Versionen zu begrenzen. Wenn Sie bei aktivierter Objektversionierung eine ungewöhnlich hohe Speichernutzung feststellen, überprüfen Sie, ob Ihre Speicherrichtlinien entsprechend festgelegt sind. 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 die Objektversionierung aktiviert haben, kann Ihr S3-Bucket nicht wieder in einen Zustand ohne Versionierung zurückversetzt 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 nicht in Storage Gateway widergespiegelt

Storage Gateway aktualisiert den Dateifreigabe-Cache automatisch, wenn Sie Dateien mithilfe der Dateifreigabe lokal 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 einen `RefreshCache` Vorgang ausführen, um die Änderungen auf der Dateifreigabe zu sehen. Wenn Sie mehr als eine Dateifreigabe haben, müssen Sie den `RefreshCache` Vorgang für jede Dateifreigabe ausführen.

Sie können den Cache mit der Storage Gateway Gateway-Konsole und dem AWS Command Line Interface (AWS CLI) aktualisieren:

- Informationen zum Aktualisieren des Caches mithilfe der Storage Gateway Gateway-Konsole finden Sie unter Objekte in Ihrem Amazon S3 S3-Bucket aktualisieren.
- Um den Cache zu aktualisieren, verwenden Sie AWS 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. Führen Sie den `refresh-cache` Befehl mit Ihrem ARN als Wert aus für`--file-share-arn`:

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

Informationen zur Automatisierung des `RefreshCache` Vorgangs finden Sie unter 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.

Die Leistung Ihres Gateways ist gesunken, nachdem Sie einen rekursiven Vorgang ausgeführt haben

In einigen Fällen können Sie einen rekursiven Vorgang ausführen, z. B. ein Verzeichnis umbenennen oder die Vererbung für eine ACL aktivieren, und diesen Vorgang in der Baumstruktur erzwingen. In diesem Fall wendet Ihr S3 File Gateway den Vorgang rekursiv auf alle Objekte in der Dateifreigabe an.

Nehmen wir beispielsweise an, Sie wenden die Vererbung auf vorhandene Objekte in einem S3-Bucket an. Ihr S3 File Gateway wendet die 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 Statusmeldungen. Weitere Informationen zu Zustandsbenachrichtigungen finden Sie unter Fehlerbehebung: Probleme mit der Hochverfügbarkeit.

Fehlerbehebung: Probleme mit der Hochverfügbarkeit

Im Folgenden finden Sie Informationen zu Aktionen, die Sie ausführen müssen, wenn Probleme im Zusammenhang mit der Verfügbarkeit auftreten.

Themen

- Zustandsbenachrichtigungen

- Kennzahlen

Zustandsbenachrichtigungen

Wenn Sie Ihr Gateway auf VMware vSphere HA ausführen, senden alle Gateways die folgenden Integritätsbenachrichtigungen an Ihre konfigurierte CloudWatch Amazon-Protokollgruppe. Diese Benachrichtigungen werden in einem Protokollstream mit dem Namen `AvailabilityMonitor` erfasst.

Themen

- Benachrichtigung: Reboot
- Benachrichtigung: HardReboot
- Benachrichtigung: HealthCheckFailure
- Benachrichtigung: AvailabilityMonitorTest

Benachrichtigung: Reboot

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-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 Reset durch vSphere High Availability Application Monitoring dieses Ereignis auslösen.

Maßnahme

Wenn Ihr Gateway in einer solchen Umgebung ausgeführt wird, überprüfen Sie, ob die `HealthCheckFailure` Benachrichtigung vorhanden ist, und lesen Sie im VMware Ereignisprotokoll für die VM nach.

Benachrichtigung: HealthCheckFailure

Für ein Gateway auf VMware vSphere HA können Sie eine `HealthCheckFailure` Benachrichtigung erhalten, wenn eine Integritätsprüfung fehlschlägt und ein VM-Neustart 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 Support Sie sich an.

Benachrichtigung: AvailabilityMonitorTest

Für ein Gateway auf VMware vSphere HA können Sie eine `AvailabilityMonitorTest` Benachrichtigung erhalten, wenn Sie einen Test des Verfügbarkeits- und Anwendungsüberwachungssystems in VMware ausführen.

Kennzahlen

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. Einzelheiten zu den Ereignissen erhalten Sie von Ihrer konfigurierten CloudWatch Protokollgruppe.

Bewährte Methoden für File Gateway

Dieser Abschnitt enthält die folgenden Themen, die Informationen zu den bewährten Methoden für die Arbeit mit Gateways, Dateifreigaben, Buckets und Daten enthalten. Wir empfehlen Ihnen, sich mit den Informationen in diesem Abschnitt vertraut zu machen und zu versuchen, diese Richtlinien zu befolgen, um Probleme mit Ihrem zu vermeiden. AWS Storage Gateway Weitere Hinweise zur Diagnose und Lösung häufiger Probleme, die bei Ihrer Bereitstellung auftreten können, finden Sie unterBehebung von Problemen mit Ihrer Storage Gateway Gateway-Bereitstellung.

Themen

Bewährte Methoden: 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**
>
> Das Wiederherstellen einer Gateway-VM von einem Snapshot, der von Ihrem Hypervisor oder aus Ihrem Amazon-EC2-Computerabbild (AMI) erstellt wurde, wird von Storage Gateway nicht unterstützt. Wenn Ihre Gateway VM, ein neues Gateway aktiviert und Ihre Daten auf diesem Gateway wiederhergestellt werden, dann folgen Sie folgenden Anweisungen.

Wiederherstellung nach dem unerwarteten Herunterfahren einer 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.

Wiederherstellen Ihrer Daten von einem fehlerhaften Cache-Datenträger

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.

Wiederherstellen Ihrer Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann

Wenn aus irgendeinem Grund nicht auf Ihr Gateway oder Rechenzentrum zugegriffen werden kann, können Sie Ihre Daten in einem anderen Gateway in einem anderen Rechenzentrum oder in einem Gateway, das auf einer Amazon-EC2-Instance gehostet ist, wiederherstellen. Wenn Sie keinen Zugriff auf ein anderes Rechenzentrum haben, empfehlen wir, das Gateway auf einer Amazon-EC2-Instance anzulegen. Die weiteren Schritte sind abhängig vom Gateway-Typ, von dem aus Sie die Daten wiederherstellen.

Um Daten von einem File Gateway in einem Rechenzentrum wiederherzustellen, auf das nicht zugegriffen werden kann

Für File Gateway ordnen Sie dem Amazon S3 S3-Bucket FSx zu, das die Daten enthält, die Sie wiederherstellen möchten.

1. Erstellen und aktivieren Sie ein neues File Gateway auf einem Amazon EC2 EC2-Host. Weitere Informationen finden Sie unter Stellen Sie einen Amazon EC2 EC2-Standardhost für S3 File Gateway bereit.
2. Erstellen Sie ein neues auf dem von Ihnen erstellten EC2-Gateway. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe .
3. Stellen Sie Ihr auf Ihrem Client bereit und ordnen Sie es dem S3-Bucket FSx zu, der die Daten enthält, die Sie wiederherstellen möchten. Weitere Informationen finden Sie unter Bereitstellen und Verwenden Ihrer Dateifreigabe Bereitstellen .

Bewährte Methoden: Verwaltung mehrteiliger Uploads

Bei der Übertragung großer Dateien nutzt S3 File Gateway die mehrteilige Upload-Funktion von Amazon S3, um die Dateien in kleinere Teile aufzuteilen und sie zur Steigerung der Effizienz parallel zu übertragen. Weitere Informationen zum mehrteiligen Upload finden Sie unter Hochladen und Kopieren von Objekten mithilfe des mehrteiligen Uploads im Amazon Simple Storage Service-Benutzerhandbuch.

Wenn ein mehrteiliger Upload aus irgendeinem Grund nicht erfolgreich abgeschlossen werden kann, stoppt das Gateway in der Regel die Übertragung, löscht alle teilweise übertragenen Teile der Datei aus Amazon S3 und versucht erneut, die Übertragung durchzuführen. In seltenen Fällen, z. B. wenn Hardware- oder Netzwerkfehler verhindern, dass das Gateway nach einem erfolglosen mehrteiligen Upload bereinigt, verbleiben Teile der teilweise übertragenen Datei möglicherweise auf Amazon S3, wo Speichergebühren anfallen können.

Als bewährte Methode zur Minimierung der Amazon S3 S3-Speicherkosten aufgrund unvollständiger mehrteiliger Uploads empfehlen wir die Konfiguration einer Amazon S3 S3-Bucket-Lebenszyklusregel, die die `AbortIncompleteMultipartUpload` API-Aktion verwendet, um erfolglose Übertragungen automatisch zu stoppen und zugehörige Dateibestandteile nach einer bestimmten Anzahl von Tagen zu löschen. Anweisungen finden Sie unter Konfiguration einer Bucket-Lebenszykluskonfiguration zum Löschen unvollständiger mehrteiliger Uploads im Amazon Simple Storage Service-Benutzerhandbuch.

Bewährte Methoden: Entpacken Sie komprimierte Dateien lokal, bevor Sie sie auf ein Gateway kopieren

Wenn Sie versuchen, ein komprimiertes Archiv mit Tausenden von Dateien zu entpacken, während es auf Ihrem Gateway gespeichert ist, kann es zu erheblichen Leistungsverzögerungen kommen. Das Entpacken eines Archivs, das eine große Anzahl von Dateien auf einer beliebigen Netzwerkdateifreigabe enthält, ist naturgemäß mit einem hohen Volumen an input/output Vorgängen, Manipulation des Metadaten-Caches, Netzwerkaufwand und Latenz verbunden. Darüber hinaus kann Storage Gateway nicht feststellen, wann jede Datei aus dem Archiv mit dem Entpacken fertig ist, und kann mit dem Hochladen von Dateien beginnen, bevor der Vorgang abgeschlossen ist, was die Leistung weiter beeinträchtigt. Diese Probleme verschärfen sich, wenn die Dateien im Archiv zahlreich, aber klein sind.

Als bewährte Methode empfehlen wir, komprimierte Archive zuerst von Ihrem Gateway auf Ihren lokalen Computer zu übertragen, bevor Sie sie entpacken. Anschließend können Sie bei Bedarf ein Tool wie Robocopy oder rsync verwenden, um die entpackten Dateien zurück zum Gateway zu übertragen.

Behalten Sie beim Kopieren von Daten von Windows Server die Dateiattribute bei

Es ist möglich, Dateien mit dem `copy` Basisbefehl unter Microsoft Windows auf Ihr File Gateway zu kopieren, aber dieser Befehl kopiert standardmäßig nur die Dateidaten, wobei bestimmte Dateiattribute wie Sicherheitsbeschreibungen weggelassen werden. Wenn die Dateien ohne die entsprechenden Sicherheitseinschränkungen und DACL-Informationen (Discretionary Access Control List) auf das Gateway kopiert werden, ist es möglich, dass unbefugte Benutzer auf sie zugreifen können.

Als bewährte Methode zur Beibehaltung aller Dateiattribute und Sicherheitsinformationen beim Kopieren von Dateien auf Ihr Gateway auf Microsoft Windows Server empfehlen wir die Verwendung der `xcopy` Befehle `robocopy` oder bzw. mit den `/o` Flags `/copy:DS` oder. Weitere Informationen finden Sie unter robocopy und xcopy in der Microsoft Windows Server-Befehlsreferenzdokumentation.

Bewährte Methoden: Richtige Dimensionierung von Cache-Festplatten

Um eine optimale Leistung zu erzielen, muss die Gesamtgröße des Festplatten-Caches groß genug sein, um die Größe Ihres aktiven Arbeitssatzes abzudecken. Bei leseintensiven und gemischten read/write Arbeitslasten wird dadurch sichergestellt, dass Sie bei Lesevorgängen einen hohen Prozentsatz an Cache-Treffern erzielen können, was wünschenswert ist. Sie können dies über die `CacheHitPercent` Metrik für Ihr S3 File Gateway überwachen.

Bei schreibintensiven Workloads (z. B. für Backup und Archivierung) puffert das S3 File Gateway eingehende Schreibvorgänge im Festplatten-Cache, bevor diese Daten asynchron nach Amazon S3 kopiert werden. Sie sollten sicherstellen, dass Sie über ausreichend Cachekapazität verfügen, um geschriebene Daten zu puffern. Die `CachePercentDirty` Metrik gibt Aufschluss über den Prozentsatz des Festplatten-Caches, der noch nicht dauerhaft gespeichert wurde. AWS

Niedrige Werte von `CachePercentDirty` sind wünschenswert. Werte, die durchweg nahe 100% liegen, deuten darauf hin, dass das S3 File Gateway nicht in der Lage ist, mit der Rate des eingehenden Schreibverkehrs Schritt zu halten. Sie können dies vermeiden, indem Sie entweder die bereitgestellte Festplatten-Cache-Kapazität erhöhen oder die dedizierte Netzwerkbandbreite erhöhen, die vom S3 File Gateway zu Amazon S3 verfügbar ist, oder beides.

Weitere Informationen zur Cache-Festplattengröße finden Sie auf dem offiziellen Amazon Web YouTube Services-Kanal unter Bewährte Methoden zur Cache-Dimensionierung von Amazon S3 File Gateway.

Arbeiten mit mehreren Dateifreigaben und Amazon S3 S3-Buckets

Wenn Sie einen einzelnen Amazon S3 S3-Bucket so konfigurieren, dass mehrere Gateways oder Dateifreigaben in ihn schreiben können, können die Ergebnisse unvorhersehbar sein. Sie können Ihre Buckets auf eine von zwei Arten konfigurieren, um unvorhersehbare Ergebnisse zu vermeiden. Wählen Sie aus den folgenden Optionen die Konfigurationsmethode aus, die am besten zu Ihrem Anwendungsfall passt:

- Konfigurieren Sie Ihre S3-Buckets so, dass nur eine Dateifreigabe in jeden Bucket schreiben kann. Verwenden Sie eine andere Dateifreigabe, um in jeden Bucket zu schreiben.

  Erstellen Sie dazu eine S3-Bucket-Richtlinie, die alle Rollen verweigert, mit Ausnahme der Rolle, die für eine bestimmte Dateifreigabe verwendet wird, um Objekte im Bucket zu platzieren oder

zu löschen. Fügen Sie jedem Bucket eine ähnliche Richtlinie hinzu und geben Sie eine andere Dateifreigabe an, um in jeden Bucket zu schreiben.

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

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

- Wenn Sie möchten, dass mehrere Dateifreigaben in denselben Amazon S3 S3-Bucket schreiben, müssen Sie verhindern, dass die Dateifreigaben versuchen, gleichzeitig in dieselben Objekte zu schreiben.

  Konfigurieren Sie dazu für jede Dateifreigabe ein separates, eindeutiges Objektpräfix. Das bedeutet, dass jede Dateifreigabe nur in Objekte mit dem entsprechenden Präfix schreibt und nicht in Objekte, die den anderen Dateifreigaben in Ihrer Bereitstellung zugeordnet sind. Sie konfigurieren das Objektpräfix im Feld S3-Präfixname, wenn Sie eine neue Dateifreigabe erstellen.

Bereinigen Sie unnötige Ressourcen

Als bewährte Methode empfehlen wir, die Storage Gateway Gateway-Ressourcen zu bereinigen, um unerwartete oder unnötige Kosten zu vermeiden. Wenn Sie beispielsweise ein Gateway zu Demonstrations- oder Testzwecken erstellt haben, sollten Sie erwägen, es und seine virtuelle Appliance aus Ihrer Bereitstellung zu löschen. Gehen Sie wie folgt vor, um Ressourcen zu bereinigen.

So bereinigen Sie nicht benötigte Ressourcen

1. Wenn Sie ein Gateway nicht mehr weiter verwenden möchten, löschen Sie es. Weitere Informationen finden Sie unter Löschen Sie Ihr Gateway und entfernen Sie die zugehörigen Ressourcen.
2. Löschen Sie die Storage-Gateway-VM von Ihrem On-Premises-Host. Wenn Sie Ihr Gateway auf einer Amazon EC2-Instance erstellt haben, beenden Sie die Instance.

Zusätzliche Storage Gateway Gateway-Ressourcen

Dieser Abschnitt enthält die folgenden Themen, die zusätzliche Informationen und Ressourcen zur Einrichtung und Verwendung enthalten AWS Storage Gateway:

Topics

- Host-Setup- Erfahren Sie, wie Sie einen VM-Host für Ihr Gateway bereitstellen und konfigurieren.
- Verwenden von Storage Gateway mit VMware HA- Erfahren Sie, wie Sie Storage Gateway für die Verwendung mit den Hochverfügbarkeitsfunktionen von VMware vSphere einrichten.
- Den Aktivierungsschlüssel erhalten- Erfahren Sie, wo Sie den Aktivierungsschlüssel finden, den Sie bei der Bereitstellung eines neuen Gateways angeben müssen.
- Unterstützung von Dateiattributen- Erfahren Sie, wie Ihr Gateway mit DOS- und Windows-Dateiattributen umgeht.
- Verwenden Direct Connect- Erfahren Sie, wie Sie eine dedizierte Netzwerkverbindung zwischen Ihrem lokalen Gateway und der AWS Cloud herstellen.
- Active Directory-Berechtigungen- Erfahren Sie, über welche Berechtigungen Ihr Dienstkonto verfügen muss, um Ihr Gateway mit Ihrer Active Directory-Domäne verbinden zu können.
- Abrufen der IP-Adresse für Ihr Gatewaygerät- Erfahren Sie, wo Sie die Host-IP-Adresse des Gateways für die virtuelle Maschine finden, die Sie bei der Bereitstellung eines neuen Gateways angeben müssen.
- Ressourcen und Ressourcen verstehen IDs- Erfahren Sie, wie die Ressourcen und Unterressourcen AWS identifiziert werden, die von Storage Gateway erstellt wurden.
- Markieren von Ressourcen- Erfahren Sie, wie Sie mithilfe von Metadaten-Tags Ihre Ressourcen kategorisieren und einfacher verwalten können.
- Open-Source-Komponenten- Erfahren Sie mehr über die Tools und Lizenzen von Drittanbietern, die zur Bereitstellung der Storage Gateway Gateway-Funktionalität verwendet werden.
- Kontingente- Erfahren Sie mehr über Beschränkungen und Kontingente für File Gateway, einschließlich Mindest- und Höchstbeschränkungen für Dateifreigaben und lokale Cache-Festplatten.
- Verwendung von Speicherklassen- Erfahren Sie mehr über die Amazon S3 S3-Speicherklassen, die File Gateway unterstützt, und was Sie bei der Auswahl einer Speicherklasse beachten sollten.

- Verwendung von Kubernetes-CSI-Treibern- Erfahren Sie, wie Sie Container Storage Interface (CSI) -Treiber installieren und konfigurieren, damit Kubernetes-Instances File Gateway als Speicher verwenden können.
- Terraform-Modul- Erfahren Sie, wie Sie mit Terraform File Gateway als virtuelle Maschine bereitstellen.

Bereitstellung und Konfiguration des Gateway-VM-Hosts

Die folgenden Themen enthalten Informationen zur Einrichtung der Hostplattform für virtuelle Maschinen für Ihr Gateway.

Themen

Stellen Sie einen Amazon EC2 EC2-Standardhost für S3 File Gateway bereit

In diesem Thema werden die Schritte zur Bereitstellung eines Amazon-EC2-Hosts unter Verwendung der Standardspezifikationen aufgeführt.

Sie können ein Amazon S3 File Gateway Amazon FSx File Gateway Elastic Compute Cloud (Amazon EC2) -Instance bereitstellen und aktivieren. Das AWS Storage Gateway Amazon Machine Image (AMI) ist als Community-AMI verfügbar.

> **Note**
>
> AMIs Die Storage Gateway Gateway-Community wird veröffentlicht und vollständig unterstützt von AWS. Sie können sehen, dass es sich bei dem Herausgeber um einen verifizierten Anbieter handelt AWS.

1. Um die Amazon EC2-Instance einzurichten, wählen Sie Amazon EC2 als Host-Plattform im Abschnitt Plattformoptionen des Workflows aus. Anweisungen zur Konfiguration der Amazon EC2 EC2-Instance finden Sie unter Bereitstellen einer Amazon EC2 EC2-Instance zum Hosten Ihres Amazon S3 File Gateways File Gateways.
2. Wählen Sie Launch Instance aus, um die AWS Storage Gateway AMI-Vorlage in der Amazon EC2 EC2-Konsole zu öffnen und zusätzliche Einstellungen wie Instance-Typen, Netzwerkeinstellungen und Speicher konfigurieren anzupassen.
3. Optional können Sie in der Storage-Gateway-Konsole die Option Standardeinstellungen verwenden auswählen, um eine Amazon-EC2-Instance mit der Standardkonfiguration bereitzustellen.

   Die Amazon-EC2-Instance, die mit Standardeinstellungen verwenden erstellt wurde, hat die folgenden Standardspezifikationen:

   - Instance-Typ – m5.xlarge
   - Netzwerkeinstellungen
     - Wählen Sie unter VPC die VPC aus, in der Ihre EC2-Instanz ausgeführt werden soll.
     - Geben Sie für Subnet das Subnetz an, in dem Ihre EC2-Instance gestartet werden soll.

     > **Note**
     >
     > VPC-Subnetze werden nur dann in der Drop-down-Liste angezeigt, wenn für sie die Einstellung zur automatischen Zuweisung öffentlicher IP-Adressen in der VPC-Managementkonsole aktiviert ist.

     - Öffentliche IP automatisch zuweisen – Aktiviert
     - Eine EC2-Sicherheitsgruppe wird erstellt und der EC2-Instance zugeordnet. Die Sicherheitsgruppe hat die folgenden eingehenden Regeln:

     > **Note**
     >
     > Während der Gateway-Aktivierung muss Port 80 geöffnet sein. Der Port wird unmittelbar nach der Aktivierung geschlossen. Danach kann auf Ihre EC2-Instance nur über die anderen Ports von der ausgewählten VPC aus zugegriffen werden. Auf die Dateifreigaben auf Ihrem Gateway kann nur von den Hosts aus zugegriffen werden, die sich in derselben VPC wie das Gateway befinden. Wenn auf die

Dateifreigaben von Hosts außerhalb der VPC zugegriffen werden muss, sollten Sie die entsprechenden Sicherheitsgruppenregeln aktualisieren.
Sie können Sicherheitsgruppen jederzeit bearbeiten, indem Sie zur Detailseite der Amazon-EC2-Instances navigieren, Sicherheit auswählen, zu Sicherheitsgruppendetails navigieren und die Sicherheitsgruppen-ID auswählen.

Port	Protocol (Protokoll)	Dateisystem-Protokoll
80	TCP	HTTP-Zugriff zur Aktivierung
111	TCP, UDP	NFSv3
139	TCP, UDP	SMB
445	TCP	SMB
2049	TCP, UDP	NFS
20048	TCP, UDP	NFSv3

- Speicher konfigurieren

Standardeinstellungen	AMI-Root-Volume	Volume 2 Cache				
Gerätename		/dev/sdf				
Größe	80 GiB	250 GiB				
Volume-Typ	gp3	gp3				
E/A\Sek	3000	3000				
Beim Beenden löschen	Ja	Ja				
Verschlüsselt	Nein	Nein				
Durchsatz	125	125				

Stellen Sie einen benutzerdefinierten Amazon EC2 EC2-Host für S3 File Gateway bereit

Sie können ein Amazon S3 File Gateway Amazon FSx File Gateway Elastic Compute Cloud (Amazon EC2) -Instance bereitstellen und aktivieren. Das AWS Storage Gateway Amazon Machine Image (AMI) ist als Community-AMI verfügbar.

> **Note**
>
> AMIs Die Storage Gateway Gateway-Community wird veröffentlicht und vollständig unterstützt von AWS. Sie können sehen, dass es sich bei dem Herausgeber um einen verifizierten Anbieter handelt AWS.
> S3 File Gateway FSx AMIs verwendet die folgende Namenskonvention. Die an den AMI-Namen angehängte Versionsnummer ändert sich mit jeder Versionsversion.

```
aws-storage-gateway-FILE_S3-1.25.0
```

So stellen Sie eine Amazon EC2 EC2-Instance zum Hosten Ihres Amazon S3 File Gateways bereit

1. Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter Ein Amazon S3 File Gateway einrichten. Wenn Sie den Bereich Plattformoptionen erreichen, wählen Sie Amazon EC2 als Host-Plattform aus und führen Sie dann die folgenden Schritte aus, um die Amazon EC2 EC2-Instance zu starten, die Ihr File Gateway hostet.
2. Wählen Sie Launch instance, um die AWS Storage Gateway AMI-Vorlage in der Amazon EC2 EC2-Konsole zu öffnen, wo Sie zusätzliche Einstellungen konfigurieren können.

   Verwenden Sie Schnellstart, um die Amazon-EC2-Instance mit Standardeinstellungen zu starten. Weitere Informationen zu den Standardspezifikationen von Amazon EC2 Quicklaunch finden Sie unter Schnellstart-Konfigurationsspezifikationen für Amazon EC2 für Amazon EC2.
3. Geben Sie unter Name einen Namen für die Amazon-EC2-Instance ein. Nachdem die Instance bereitgestellt wurde, können Sie nach diesem Namen suchen, um Ihre Instance auf Listenseiten in der Amazon-EC2-Konsole zu finden.
4. Für Instance-Typ können Sie aus der Liste Instance-Typ die Hardware-Konfiguration für Ihre Instance auswählen. Die Hardwarekonfiguration muss bestimmte Mindestanforderungen erfüllen, um Ihr Gateway zu unterstützen. Wir empfehlen, mit dem Instance-Typ m4.xlarge zu beginnen, der die Mindestanforderungen erfüllt, damit das Gateway korrekt funktioniert. Weitere Informationen finden Sie unter Anforderungen für Amazon-EC2-Instance-Typen.

   Sie können die Größe der Instance nach dem Start bei Bedarf ändern. Weitere Informationen finden Sie unter Größenänderung Ihrer Instance im Amazon EC2 EC2-Benutzerhandbuch.

   > **Note**
   >
   > Bestimmte Instance-Typen, insbesondere i3 EC2, verwenden NVMe SSD-Festplatten. Diese können zu Problemen beim Starten oder Stoppen von File Gateway führen. Sie können beispielsweise Daten aus dem Cache verlieren. Überwachen Sie die `CachePercentDirty` CloudWatch Amazon-Metrik und starten oder stoppen Sie Ihr System nur, wenn dieser Parameter aktiviert ist`0`. Weitere Informationen zu Monitoring-Metriken für Ihr Gateway finden Sie in der CloudWatch Dokumentation unter Storage Gateway Gateway-Metriken und -Dimensionen.

5. Wählen Sie im Abschnitt Schlüsselpaar (Anmeldung) für Schlüsselpaarname – erforderlich das Schlüsselpaar aus, das Sie für die sichere Verbindung mit Ihrer Instance verwenden möchten. Bei Bedarf können Sie ein neues Schlüsselpaarname erstellen. Weitere Informationen dazu finden Sie unter Erstellen eines Schlüsselpaares im Amazon-Elastic-Compute-Cloud-Benutzerhandbuch für Linux-Instances.
6. Überprüfen Sie im Abschnitt Netzwerkeinstellungen die vorkonfigurierten Einstellungen und wählen Sie Bearbeiten, um Änderungen an den folgenden Feldern vorzunehmen:
   a. Wählen Sie für VPC — erforderlich die VPC aus, auf der Sie Ihre Amazon-EC2-Instance starten möchten. Weitere Informationen zur Funktionsweise von Amazon VPC finden Sie im Amazon Virtual Private Cloud-Benutzerhandbuch.
   b. (Optional) Wählen Sie unter Subnetz das Subnetz aus, in dem Sie Ihre Amazon-EC2-Instance starten möchten.
   c. Wählen Sie für Öffentlche IP automatisch zuweisen Aktivieren aus.
7. Überprüfen Sie im Unterabschnitt Firewall (Sicherheitsgruppen) die vorkonfigurierten Einstellungen. Sie können den Standardnamen und die Beschreibung der neuen Sicherheitsgruppe, die für Ihre Amazon-EC2-Instance erstellt werden soll, ändern, wenn Sie möchten, oder sich dafür entscheiden, stattdessen Firewallregeln aus einer vorhandenen Sicherheitsgruppe anzuwenden.
8. Fügen Sie im Unterabschnitt Eingehende Sicherheitsgruppenregeln Firewallregeln hinzu, um die Ports zu öffnen, über die Clients eine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances.

> **Note**
>
> Amazon S3 File Gateway erfordert, dass der TCP-Port 80 für eingehenden Datenverkehr und einmaligen HTTP-Zugriff während der Gateway-Aktivierung geöffnet ist. Nach der Aktivierung können Sie diesen Port schließen.
> Wenn Sie NFS-Dateifreigaben erstellen möchten, müssen Sie TCP/UDP Port 2049 für den NFS-Zugriff, Port 111 für den Zugriff und TCP/UDP TCP/UDP Port 20048 für NFSv3 den Zugriff öffnen. NFSv3
> Wenn Sie SMB-Dateifreigaben erstellen möchten, müssen Sie den TCP-Port 445 für den SMB-Zugriff öffnen.

9. Überprüfen Sie im Unterabschnitt Erweiterte Netzwerkkonfiguration die vorkonfigurierten Einstellungen und nehmen Sie gegebenenfalls Änderungen vor.
10. Wählen Sie im Abschnitt Speicher hinzufügen die Option Neues Volume hinzufügen, um der Gateway-Instance Speicher hinzuzufügen.

    > **Important**
    >
    > Sie müssen zusätzlich zum vorkonfigurierten Root-Volume mindestens ein Amazon EBS-Volume mit mindestens 150 GiB Kapazität für den Cache-Speicher hinzufügen. Für eine höhere Leistung empfehlen wir, mehrere EBS-Volumes für den Cache-Speicher mit jeweils mindestens 150 GiB zuzuweisen.

11. Überprüfen Sie im Abschnitt Erweiterte Details die vorkonfigurierten Einstellungen und nehmen Sie gegebenenfalls Änderungen vor.
12. Wählen Sie Instance starten, um Ihre neue Amazon-EC2-Gateway-Instance mit den konfigurierten Einstellungen zu starten.
13. Um zu überprüfen, ob Ihre neue Instance erfolgreich gestartet wurde, navigieren Sie zur Seite Instances in der Amazon-EC2-Konsole und suchen Sie anhand des Namens nach Ihrer neuen Instance. Stellen Sie sicher, dass der Instance-Status mit einem grünen Häkchen als Wird ausgeführt angezeigt wird und dass die Statusprüfung abgeschlossen ist und dass ein grünes Häkchen angezeigt wird.
14. Wählen Sie Ihre Instance auf der Detailseite aus. Kopieren Sie die öffentliche IP-Adresse aus dem Abschnitt Instance-Zusammenfassung und kehren Sie dann zur Seite Gateway einrichten in der Storage Gateway Gateway-Konsole zurück, um mit der Einrichtung Ihres Amazon S3 File Gateway fortzufahren.

Sie können die AMI-ID ermitteln, die für den Start eines File Gateways verwendet werden soll, indem Sie die Storage Gateway Gateway-Konsole verwenden oder den AWS Systems Manager Parameterspeicher abfragen.

Um die AMI-ID zu ermitteln, führen Sie einen der folgenden Schritte aus:

- Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter Ein Amazon S3 File Gateway einrichten. Wenn Sie den Bereich Plattformoptionen erreichen, wählen Sie Amazon EC2 als Host-Plattform und dann Launch Instance aus, um die AWS Storage Gateway AMI-Vorlage in der Amazon EC2 EC2-Konsole zu öffnen.

Sie werden zur AMI-Seite der EC2-Community weitergeleitet, auf der Sie die AMI-ID für Ihre AWS Region in der URL sehen können.

- Führen Sie eine Abfrage des Systems Manager-Parameterspeichers durch. Sie können die AWS CLI oder Storage Gateway Gateway-API verwenden, um den öffentlichen Parameter von Systems Manager unter dem Namespace `/aws/service/storagegateway/ami/FILE_S3/latest` abzufragen. Wenn Sie beispielsweise den folgenden CLI-Befehl verwenden, wird die ID des aktuellen AMI in der von AWS-Region Ihnen angegebenen zurückgegeben.

```
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"
    }
}
```

Metadatenoptionen Amazon EC2 EC2-Instances ändern

Der Instance-Metadaten-Service (IMDS) ist eine On-Instance-Komponente, die sicheren Zugriff auf Amazon EC2 EC2-Instance-Metadaten bietet. Eine Instance kann so konfiguriert werden, dass sie eingehende Metadatenanfragen akzeptiert, die IMDS Version 1 (IMDSv1) verwenden, oder verlangt, dass alle Metadatenanfragen IMDS Version 2 verwenden (). IMDSv2 IMDSv2 verwendet sitzungsorientierte Anfragen und behebt verschiedene Arten von Sicherheitslücken, die beim Versuch, auf das IMDS zuzugreifen, genutzt werden könnten. Weitere Informationen dazu IMDSv2 finden Sie unter So funktioniert Instance Metadata Service Version 2 im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Wir empfehlen, dass Sie IMDSv2 für alle Amazon EC2 EC2-Instances benötigen, die Storage Gateway hosten. IMDSv2 ist standardmäßig für alle neu gestarteten Gateway-Instances erforderlich. Wenn Sie über bestehende Instances verfügen, die noch so konfiguriert sind, dass sie IMDSv1 Metadatenanfragen akzeptieren, finden Sie unter Verwendung von erforderlich IMDSv2 im Amazon Elastic Compute Cloud-Benutzerhandbuch Anweisungen, wie Sie Ihre Instance-Metadatenoptionen so ändern können, dass sie die Verwendung von erfordern IMDSv2. Für die Anwendung dieser Änderung ist kein Neustart der Instance erforderlich.

Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Host-Zeit

Für ein Gateway, das auf bereitgestellt wird VMware ESXi, reicht es aus, die Hypervisor-Host-Zeit einzustellen und die Zeit der virtuellen Maschine mit dem Host zu synchronisieren, um Zeitabweichungen zu vermeiden. Weitere Informationen finden Sie unter Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit. Für ein Gateway, das auf Microsoft Hyper-V oder Linux KVM bereitgestellt wird, empfehlen wir, die Uhrzeit der virtuellen Maschine regelmäßig mit dem unten beschriebenen Verfahren zu überprüfen.

Um die Uhrzeit einer virtuellen Hypervisor-Gateway-Maschine anzuzeigen und mit einem NTP-Server (Network Time Protocol) zu synchronisieren

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

   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Greifen Sie mit Microsoft auf die lokale Gateway-Konsole zu Hyper-V.
   - Weitere Informationen zur Anmeldung an der lokalen Konsole für Linux Kernel-based Virtual Machine (KVM) finden Sie unter. Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
2. Geben Sie auf dem Hauptmenübildschirm der Storage Gateway Gateway-Konfiguration die entsprechende Zahl ein, um System Time Management auszuwählen.
3. Geben Sie auf dem Menübildschirm System Time Management die entsprechende Ziffer ein, um Systemzeit anzeigen und synchronisieren auszuwählen.

   Die lokale Gateway-Konsole zeigt die aktuelle Systemzeit an und vergleicht sie mit der vom NTP-Server gemeldeten Zeit. Anschließend wird die genaue Abweichung zwischen den beiden Zeiten in Sekunden gemeldet.
4. Wenn die Zeitabweichung mehr als 60 Sekunden beträgt, geben Sie ein, um die Systemzeit mit der NTP-Zeit **y** zu synchronisieren. Geben Sie andernfalls **n** ein.

Die Zeitsynchronisierung kann einige Augenblicke dauern.

Synchronisieren Sie die VM-Zeit mit der VMware 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. Klicken Sie im vSphere-Client im Bereich auf der linken Seite des Anwendungsfensters mit der rechten Maustaste auf den Namen Ihrer Gateway-VM, um das Kontextmenü für die VM zu öffnen, und wählen Sie dann Einstellungen bearbeiten.

      Das Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) wird geöffnet.

   b. Wählen Sie die Registerkarte Optionen und dann in der Optionsliste VMware Tools aus.

   c. Aktivieren Sie im Bereich „Erweitert“ auf der rechten Seite des Dialogfelds „Eigenschaften der virtuellen Maschine“ die Option „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 im linken Bereich den vSphere-Hostknoten und dann die Registerkarte Konfiguration aus.

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. Stellen Sie unter Datum und Uhrzeit Datum und Uhrzeit für Ihren vSphere-Host ein.

d. Konfigurieren Sie den Host so, dass seine Zeit automatisch mit einem NTP-Server synchronisiert wird.

   i. Wählen Sie im Dialogfeld „Zeitkonfiguration“ die Option „Optionen“ und wählen Sie dann im linken Bereich im Dialogfeld „NTP-Daemon (ntpd) -Optionen“ die Option „NTP-Einstellungen“ aus.

   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 es `pool.ntp.org` als Domainnamen verwenden.

   iv. Wählen Sie im Dialogfeld mit den Optionen für NTP Daemon (ntpd) im linken Bereich die Option Allgemein aus.

   v. Wählen Sie unter Dienstbefehle die Option Start aus, um den Dienst 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.

Netzwerkadapter für Ihr Gateway konfigurieren

Storage Gateway verwendet standardmäßig einen einzigen Netzwerkadapter VMXNET3 (10 GbE). Sie können Ihr Gateway jedoch so konfigurieren, dass es mehr als einen Netzwerkadapter verwendet, sodass über mehrere IP-Adressen darauf zugegriffen werden kann. Dies kann in den folgenden Situationen wünschenswert sein:

- Maximierung des Durchsatzes — Möglicherweise möchten Sie den Durchsatz zu einem Gateway maximieren, wenn Netzwerkadapter einen Engpass darstellen.
- Anwendungstrennung – Möglicherweise müssen Sie trennen, wie Ihre Anwendungen in Gateway-Volumes schreiben. Sie können beispielsweise festlegen, dass eine kritische Speicheranwendung ausschließlich einen bestimmten Adapter verwendet, der für Ihr Gateway definiert ist.
- Netzwerkeinschränkungen — Ihre Anwendungsumgebung erfordert möglicherweise, dass Sie Ihre Dateifreigaben und die Initiatoren, die eine Verbindung zu ihnen herstellen, in einem isolierten Netzwerk aufbewahren. Dieses Netzwerk unterscheidet sich von dem Netzwerk, über das das Gateway mit AWS kommuniziert.

In einem typischen Anwendungsfall mit mehreren Adaptern wird ein Adapter als Route konfiguriert, mit der das Gateway kommuniziert AWS (d. h. als Standard-Gateway). Mit Ausnahme dieses einen Adapters müssen sich die Initiatoren im selben Subnetz befinden wie der Adapter, der die Dateifreigaben enthält, mit denen sie eine Verbindung herstellen. Andernfalls ist die Kommunikation mit den vorgesehenen Zielen vielleicht nicht möglich. Wenn ein Ziel auf demselben Adapter konfiguriert ist, mit dem kommuniziert wird AWS, fließt der Dateifreigabeverkehr für dieses Ziel und der AWS Datenverkehr über denselben Adapter.

In einigen Fällen können Sie einen Adapter für die Verbindung mit der Storage Gateway Gateway-Konsole konfigurieren und dann einen zweiten Adapter hinzufügen. In einem solchen Fall konfiguriert Storage Gateway die Routing-Tabelle automatisch so, dass der zweite Adapter als bevorzugte Route verwendet wird. Anweisungen zur Konfiguration mehrerer Adapter finden Sie in den folgenden Themen:

Themen

- Konfiguration Ihres Gateways für mehrere NICs auf einem VMware ESXi Host
- Konfiguration Ihres Gateways für mehrere NICs in Microsoft Hyper-V Host

Konfiguration Ihres Gateways für mehrere NICs auf einem VMware ESXi Host

Im folgenden Verfahren wird davon ausgegangen, dass für Ihre Gateway-VM bereits ein Netzwerkadapter definiert ist, und es wird beschrieben, wie ein Adapter hinzugefügt wird VMware ESXi.

So konfigurieren Sie Ihr Gateway für die Verwendung eines zusätzlichen Netzwerkadapters im VMware ESXi Host

1. Fahren Sie das Gateway herunter.
2. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM aus.

   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, den VMXNET3 Netzwerkadapter mit Storage Gateway zu verwenden. Weitere Informationen zu den Adaptertypen, die möglicherweise in der Adapterliste erscheinen, finden Sie unter Netzwerkadaptertypen in der ESXi und der 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 Übersicht der VM und anschließend Alle anzeigen neben dem Kontrollkästchen IP-Adresse. Das Fenster 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.

7. Schalten Sie in der Storage-Gateway-Konsole das Gateway ein.
8. Wählen Sie im Fenster Navigation der Storage-Gateway-Konsole 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.

> **Note**
>
> Die Beispiel-Mountingbefehle auf der Informationsseite für eine Dateifreigabe in der Storage-Gateway-Konsole enthalten immer die IP-Adresse des Netzwerkadapters, der zuletzt zum zugehörigen Gateway der Dateifreigabe hinzugefügt wurde.

Informationen zu Aufgaben auf lokalen Konsolen VMware, die bei Hyper-V- und KVM-Hosts häufig vorkommen, finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine

Konfiguration Ihres Gateways für mehrere NICs in 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 in der Storage-Gateway-Konsole das Gateway aus.
2. Wählen Sie im Microsoft Hyper-V Manager Ihre Gateway-VM im Bereich Virtuelle Maschinen aus.
3. Wenn die Gateway-VM noch nicht ausgeschaltet ist, klicken Sie mit der rechten Maustaste auf den VM-Namen, um das Kontextmenü zu öffnen, und wählen Sie dann Ausschalten.
4. Klicken Sie mit der rechten Maustaste auf den Namen der Gateway-VM, um das Kontextmenü zu öffnen, und wählen Sie dann Einstellungen.
5. Wählen Sie im Dialogfeld Einstellungen unter Hardware die Option Hardware hinzufügen aus.
6. Wählen Sie im Bereich „Hardware hinzufügen“ auf der rechten Seite des Dialogfelds „Einstellungen“ die Option „Netzwerkadapter“ und dann „Hinzufügen“, um ein Gerät hinzuzufügen.

7. Konfigurieren Sie den Netzwerkadapter, und wählen Sie dann Apply (Anwenden), um die Einstellungen anzuwenden.
8. Vergewissern Sie sich im Dialogfeld Einstellungen unter Hardware, dass der neue Netzwerkadapter zur Hardwareliste hinzugefügt wurde, und klicken Sie dann auf OK.
9. Schalten Sie das Gateway über die Storage Gateway Gateway-Konsole ein.
10. Wählen Sie im Navigationsbereich der Storage Gateway Gateway-Konsole Gateways und dann das Gateway aus, zu dem Sie den Adapter hinzugefügt haben. Vergewissern Sie sich, dass auf der Registerkarte Details eine zweite IP-Adresse aufgeführt ist.

> **Note**
>
> Die Beispiel-Mountingbefehle auf der Informationsseite für eine Dateifreigabe in der Storage-Gateway-Konsole enthalten immer die IP-Adresse des Netzwerkadapters, der zuletzt zum zugehörigen Gateway der Dateifreigabe hinzugefügt wurde.

Informationen zu Aufgaben auf lokalen Konsolen VMware, die bei Hyper-V- und KVM-Hosts häufig auftreten, finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine

Verwenden von VMware vSphere High Availability mit Storage Gateway

Storage Gateway bietet Hochverfügbarkeit VMware durch eine Reihe von Integritätsprüfungen 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.

Mit dieser Integration erholt sich ein Gateway, das in einer lokalen VMware Umgebung oder in einer VMware Cloud bereitgestellt wird, AWS automatisch nach den meisten Dienstunterbrechungen. Dies geschieht dies in der Regel in weniger als 60 Sekunden ohne Datenverlust.

> **Note**
>
> Wir empfehlen, Folgendes zu tun, wenn Sie Storage Gateway in einem VMware HA-Cluster bereitstellen:
>
> - Stellen Sie das herunterladbare VMware ESX .ova-Paket, das die Storage Gateway Gateway-VM enthält, auf nur einem Host in einem Cluster bereit.

- Wählen Sie bei der Bereitstellung des .ova-Pakets einen Datenspeicher aus, der nicht lokal auf einem Host gespeichert ist. 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.
- Wenn Sie beim Clustering das .ova-Paket im Cluster bereitstellen, wählen Sie einen Host aus, wenn Sie dazu aufgefordert werden. Alternativ können Sie direkt auf einem Host in einem Cluster bereitstellen.

In den folgenden Themen wird beschrieben, wie Storage Gateway in einem VMware HA-Cluster bereitgestellt wird:

Themen

Konfigurieren Sie Ihren vSphere VMware HA-Cluster

Wenn Sie noch keinen VMware Cluster erstellt haben, erstellen Sie zunächst einen. Informationen zum Erstellen eines VMware Clusters finden Sie in der VMware Dokumentation unter Erstellen eines vSphere HA-Clusters.

Als Nächstes konfigurieren Sie Ihren VMware Cluster so, dass er mit Storage Gateway funktioniert.

Um Ihren VMware Cluster zu konfigurieren

1. Stellen Sie auf der Seite Clustereinstellungen bearbeiten in VMware vSphere sicher, dass die VM-Überwachung für die VM- und Anwendungsüberwachung konfiguriert ist. Stellen Sie dazu für jede Option die folgenden Werte ein:

   - Antwort auf einen Hostfehler: Neustart VMs

- Reaktion auf die Hostisolierung: Herunterfahren und neu starten VMs
- Datastore with PDL (Datenspeicher mit PDL): Disabled (Deaktiviert)
- Datastore with APD (Datenspeicher mit APD): Disabled (Deaktiviert)
- VM Monitoring (VM-Überwachung): VM and Application Monitoring (VM- und Anwendungsüberwachung)

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.
   - Mindestbetriebszeit: Der Cluster wartet so lange nach dem Start einer VM, bevor mit der Überwachung des Heartbeat von VM-Tools begonnen wird.
   - Maximale Zurücksetzungen pro VM: Der Cluster startet die VM innerhalb des Zeitfensters für maximale Zurücksetzungen höchstens so viele Male.
   - Zeitfenster für maximale Zurücksetzungen: 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 andere auf dem Cluster VMs ausgeführt werden, sollten Sie diese Werte möglicherweise 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) Fügen Sie in Ihrem Cluster Überschreibungsoptionen für andere VMs Optionen hinzu.

Richten Sie Ihren Gateway-Typ ein

Gehen Sie wie folgt vor, um das Gateway einzurichten

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 — Erstellen und Aktivieren eines Amazon S3 File Gateways

Bereitstellen des Gateways

Stellen Sie das OVA-Image in Ihrem konfigurierten Cluster auf einem der Cluster-Hosts bereit. Anweisungen finden Sie unter Bereitstellen einer OVF- oder OVA-Vorlage in der VMware vSphere-Online-Dokumentation.

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) Fügen Sie in Ihrem Cluster Überschreibungsoptionen für andere VMs Optionen hinzu

Wenn andere auf Ihrem Cluster VMs ausgeführt werden, möchten Sie die Clusterwerte möglicherweise speziell für jede VM festlegen. Anweisungen finden Sie unter Anpassen einer einzelnen virtuellen Maschine in der VMware vSphere-Online-Dokumentation.

Um Optionen zum Außerkraftsetzen für andere Optionen VMs in Ihrem Cluster hinzuzufügen

1. Wählen Sie auf der Übersichtsseite in VMware vSphere Ihren Cluster aus, um die Clusterseite zu öffnen, und wählen Sie dann Configure aus.
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.

   Legen Sie die folgenden Werte für jede Option unter vSphere HA — VM-Überwachung fest:

   - VM-Überwachung: Override Enabled — VM- und Anwendungsüberwachung
   - Empfindlichkeit der VM-Überwachung: Override aktiviert — VM- und Anwendungsüberwachung
   - VM-Überwachung: Benutzerdefiniert
   - Ausfallintervall: **30** Sekunden

- Minimale Betriebszeit: Sekunden **120**
- Maximum per-VM resets (Maximale Zurücksetzungen pro VM): **5**
- Zeitfenster für maximale Rücksetzungen: Innerhalb von Stunden **1**

Aktivieren des Gateways

Nachdem die .ova in Ihrer VMware Umgebung bereitgestellt wurde, aktivieren Sie Ihr Gateway über die Storage Gateway Gateway-Konsole. Anweisungen finden Sie unter Einstellungen überprüfen und Ihre Amazon S3 File Gateway-Einstellungen aktivieren.

Testen Sie Ihre VMware Hochverfügbarkeitskonfiguration

Testen Sie Ihre Konfiguration, nachdem Sie Ihr Gateway aktiviert haben.

Um Ihre VMware HA-Konfiguration zu testen

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, das Sie auf VMware HA testen möchten.
3. Wählen Sie für Aktionen die Option Verify VMware HA aus.
4. Wählen Sie im daraufhin angezeigten Feld „ VMware Hochverfügbarkeitskonfiguration überprüfen“ die Option OK aus.

   > **Note**
   >
   > Beim Testen Ihrer VMware HA-Konfiguration wird Ihre Gateway-VM neu gestartet und die Konnektivität 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 CloudWatch Amazon-Protokollgruppen. Weitere Informationen finden Sie unter Abrufen von S3 File Gateway FSx mit CloudWatch Protokollgruppen.

Abrufen eines Aktivierungsschlüssels für das Gateway

Um einen Aktivierungsschlüssel für Ihr Gateway zu erhalten, stellen Sie eine Webanforderung an die virtuelle Gateway-Maschine (VM). Die VM gibt eine Umleitung zurück, die den Aktivierungsschlüssel enthält, der als einer der Parameter für die `ActivateGateway`-API-Aktion zur Angabe der Konfiguration Ihres Gateways übergeben wird. Weitere Informationen finden Sie ActivateGatewayin der Storage Gateway API-Referenz.

> **Note**
>
> Gateway-Aktivierungsschlüssel laufen nach 30 Minuten ab, wenn sie nicht verwendet werden.

Die Anfrage, die Sie an die Gateway-VM stellen, umfasst die AWS Region, in der die Aktivierung erfolgt. Die URL, die von der Umleitung in der Antwort zurückgegeben wird, enthält einen Abfragezeichenfolgenparameter namens `activationkey`. Dieser Abfragezeichenfolge-Parameter ist Ihr Aktivierungsschlüssel. Das Format der Abfragezeichenfolge: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. Mit der Ausgabe dieser Abfrage werden sowohl die Aktivierungsregion als auch der Aktivierungsschlüssel zurückgegeben.

Die URL enthält auch `vpcEndpoint`, die VPC-Endpunkt-ID für Gateways, die über den VPC-Endpunkttyp eine Verbindung herstellen.

> **Note**
>
> Die AWS Storage Gateway Hardware-Appliance, VM-Image-Vorlagen und Amazon EC2 Amazon Machine Images (AMI) sind mit den HTTP-Diensten vorkonfiguriert, die für den Empfang und die Beantwortung der auf dieser Seite beschriebenen Webanfragen erforderlich sind. Es ist nicht erforderlich oder empfehlenswert, zusätzliche Dienste auf Ihrem Gateway zu installieren.

Themen

- Linux (curl)
- Linux (bash/zsh)
- Microsoft Windows PowerShell
- Verwenden der lokalen Konsole

Linux (curl)

In den folgenden Beispielen wird gezeigt, wie Sie mithilfe von Linux (curl) einen Aktivierungsschlüssel abrufen.

> **Note**
>
> Ersetzen Sie die hervorgehobenen Variablen durch tatsächliche Werte für Ihr Gateway. Zulässige Werte sind:
>
> - *`gateway_ip_address`*- Zum Beispiel die IPv4 Adresse Ihres Gateways `172.31.29.201`
> - *`gateway_type`*- Der Gateway-Typ, den Sie aktivieren möchten, z. B. `STOREDCACHED`,`VTL`,`FILE_S3`, oder`FILE_FSX_SMB`.
> - *`region_code`*- Die Region, in der Sie Ihr Gateway aktivieren möchten. Weitere Informationen finden Sie unter Regionale Endpunkte im Allgemeinen Referenzhandbuch zu AWS . Wenn dieser Parameter nicht angegeben ist oder wenn der angegebene Wert falsch geschrieben ist oder nicht mit einer gültigen Region übereinstimmt, verwendet der Befehl standardmäßig die `us-east-1` Region.
> - *`vpc_endpoint`*- Zum Beispiel `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com` der VPC-Endpunktname für Ihr Gateway.

Öffentlicher Endpunkt

Verwenden Sie einen der folgenden Befehle, um einen Aktivierungsschlüssel für einen öffentlichen Endpunkt zu erhalten:

Standard-Endpunkte

Um den Aktivierungsschlüssel für einen Standardendpunkt zu erhalten:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Dual-Stack-Endpunkte

Um den Aktivierungsschlüssel für einen Dual-Stack-Endpunkt zu erhalten:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

FIPS-Endpunkte

Um den Aktivierungsschlüssel für einen FIPS-Endpunkt zu erhalten:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

VPC-Endpunkte

So rufen Sie den Aktivierungsschlüssel für einen VPC-Endpunkt ab:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

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 "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

Das folgende Beispiel zeigt Ihnen, wie Sie Microsoft Windows verwenden, PowerShell um die HTTP-Antwort abzurufen, HTTP-Header zu analysieren und den Aktivierungsschlüssel abzurufen.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Verwenden der lokalen Konsole

Die folgenden Ihnen, wie Sie Ihre lokale Konsole verwenden, um einen Aktivierungsschlüssel zu generieren und anzuzeigen.

Auf Amazon Linux 2 (AL2) basierende Gateways

Sie können entweder Standard- oder FIPS-Endpunkte für Gateways auswählen, die auf basieren. AL2

> **Note**
>
> FIPS-Endpunkte sind nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter FIPS-Endpunkte nach Dienst.

Um einen Aktivierungsschlüssel für Ihr AL2 basiertes Gateway von Ihrer lokalen Konsole zu erhalten

1. Melden Sie sich bei Ihrer lokalen Konsole als Administrator an.
2. Wählen Sie im Hauptmenü AWS Appliance-Aktivierung — Konfiguration `0` die Option Aktivierungsschlüssel abrufen aus.
3. Wählen Sie die Option Storage Gateway für die Gateway-Produktreihe aus.
4. Geben Sie die AWS Region ein, in der Sie Ihr Gateway aktivieren möchten.
5. Geben Sie als Netzwerktyp 1 für Öffentlich oder 2 für VPC ein.
6. Geben Sie als Endpunkttyp 1 für Standard oder 2 für Federal Information Processing Standard (FIPS) ein.

Auf Amazon Linux 2023 (AL2023) basierende Gateways

Für Gateways, die auf basieren AL2023, sind die folgenden Endpunkte verfügbar:

- Standardendpunkte (nur Support) IPv4
- FIPS-Endpunkte (nur Support) IPv4
- Dual-Stack-Endpunkte (Unterstützung und) IPv4 IPv6
- Dual-Stack-FIPS-Endpunkte (Unterstützung und) IPv4 IPv6

Weitere Informationen finden Sie unter Endpunkttypen.

Um einen Aktivierungsschlüssel für Ihr AL2023 basiertes Gateway von Ihrer lokalen Konsole zu erhalten

1. Melden Sie sich bei der lokalen Konsole an. Wenn Sie auf einem Windows-Computer eine Verbindung mit Ihrer Amazon-EC2-Instance herstellen, melden Sie sich als admin an.
2. Wählen Sie im Hauptmenü AWS Appliance-Aktivierung — Konfiguration `0` die Option Aktivierungsschlüssel abrufen aus.
3. Wählen Sie die Option Storage Gateway für die Gateway-Produktreihe aus.
4. Geben Sie die AWS Region ein, in der Sie Ihr Gateway aktivieren möchten.
5. Geben Sie als Netzwerktyp 1 für Öffentlich oder 2 für VPC-Endpunkt ein.
6. Geben Sie für Endpunkttyp auswählen die Option FIPS aktivieren? , geben Sie ein, `Y` um FIPS zu aktivieren oder einen `N` Nicht-FIPS-Endpunkt zu verwenden.
7. Geben Sie als Endpunkttyp den Wert 1 für Standardendpunkt oder 2 für Dual-Stack-Endpunkt ein.

    - Geben Sie für einen Dual-Stack-Endpunkt für Select IP version or exit: 1 for IPv4 oder 2 for ein. IPv6

Support für Dateiattribute in Amazon S3 File Gateway

Amazon S3 File Gateway unterstützt standardmäßig DOS- oder Windows-Dateiattribute. Mit S3 File Gateway können Sie Dateidaten und Metadaten beibehalten und Einstellungen aktualisieren — z. B. Elemente als archiviert markieren, wenn sie in Amazon S3 abgelegt werden. Weitere Informationen zu DOS- und Windows-Dateiattributen finden Sie im Artikel Dateiattribute-Konstanten auf der Dokumentationswebsite für die Entwicklung von Windows-Apps.

S3 File Gateway unterstützt die folgenden Attribute:

- ReadOnly— Das S3 File Gateway verhindert Änderungen an Dateien, für die das ReadOnly Attribut gesetzt ist.
- Archiv — Das S3 File Gateway legt dieses Attribut fest, wenn Dateien zum ersten Mal zum Gateway hinzugefügt werden.

> **Note**
>
> Backup-Anwendungen sichern in der Regel Dateien, für die das Archiv-Bit gesetzt ist, und löschen das Bit nach erfolgreicher Sicherung.

- Versteckt — SMB-Clients (Server Message Block) verstecken Dateien, die diesen Bitsatz verwenden.
- System — Dieses Attribut bleibt bestehen, sobald Sie es festgelegt haben.

Wenn Sie eine Datei mit den festgelegten Attributen auf das S3 File Gateway kopieren, bleiben die DOS- oder Windows-Attribute der Datei auf dem S3 File Gateway und in Amazon S3 erhalten. Sie können diese Attribute für Dateien auf dem Gateway aktualisieren, und diese Aktualisierungen gelten auch für das Objekt in Amazon S3. Wenn eine Datei vom Gateway entfernt wird, ruft das Gateway die Datei, ihre Metadaten und ihre persistenten Attribute auf Anfrage von Amazon S3 ab.

> **Note**
>
> DOS-Attribute werden nur auf SMB-Shares unterstützt und wenn der Zugriff durch Windows-Zugriffskontrolllisten gesteuert wird.

Verwendung Direct Connect mit Storage Gateway

Direct Connect verbindet Ihr internes Netzwerk mit der Amazon Web Services Cloud. Durch die Verwendung Direct Connect mit Storage Gateway können Sie eine Verbindung für Workload-Anforderungen mit hohem Durchsatz herstellen und so eine dedizierte Netzwerkverbindung zwischen Ihrem lokalen Gateway und bereitstellen. AWS

Storage Gateway verwendet öffentliche Endpunkte. Wenn eine Direct Connect Verbindung besteht, können Sie eine öffentliche virtuelle Schnittstelle erstellen, über die der Datenverkehr an die Storage Gateway Gateway-Endpunkte weitergeleitet werden kann. Die öffentliche virtuelle Schnittstelle umgeht Internetdienstanbieter in Ihrem Netzwerkpfad. Der öffentliche Endpunkt des Storage Gateway Gateway-Dienstes kann sich in derselben AWS Region wie der Direct Connect Standort oder in einer anderen AWS Region befinden.

Die folgende Abbildung zeigt ein Beispiel für die Direct Connect Funktionsweise mit Storage Gateway.

Netzwerkarchitektur, die zeigt, dass Storage Gateway über AWS Direct Connect mit der Cloud verbunden ist.

In der folgenden Vorgehensweise wird davon ausgegangen, dass Sie bereits ein funktionsfähiges Gateway erstellt haben.

Zur Verwendung Direct Connect mit Storage Gateway

1. Erstellen und stellen Sie eine AWS Direct Connect Verbindung zwischen Ihrem lokalen Rechenzentrum und Ihrem Storage Gateway Gateway-Endpunkt her. Weitere Informationen zum Erstellen einer Verbindung finden Sie unter Erste Schritte mit Direct Connect im Benutzerhandbuch zu Direct Connect .
2. Connect Sie Ihre lokale Storage Gateway Gateway-Appliance mit dem Direct Connect Router.
3. Erstellen Sie eine öffentliche virtuelle Schnittstelle und konfigurieren Sie Ihren lokalen Router entsprechend. Weitere Informationen finden Sie unter Erstellen einer virtuellen Schnittstelle im Benutzerhandbuch zu Direct Connect .

Einzelheiten dazu finden Sie Direct Connect unter Was ist Direct Connect? im Direct Connect Benutzerhandbuch.

Berechtigungsanforderungen für das Active Directory-Dienstkonto

Wenn Sie Microsoft Active Directory verwenden möchten, um benutzerauthentifizierten Zugriff auf die auf Ihrem Computer bereitzustellen AWS Storage Gateway, müssen Sie sicherstellen, dass Sie über ein Active Directory-Dienstkonto verfügen und dass das Dienstkonto über delegierte Berechtigungen verfügt, um Computer zu Ihrer Domäne hinzuzufügen. Ein Dienstkonto ist ein Active Directory-Benutzerkonto, dem die Berechtigung zur Ausführung bestimmter Aufgaben delegiert wurde. Sie geben den Benutzernamen und das Passwort für dieses Konto an, wenn Sie ein Storage Gateway zu Ihrer Active Directory-Domäne hinzufügen.

Dem Active Directory-Dienstkonto müssen die folgenden Berechtigungen in der Organisationseinheit, der Sie Ihr Gateway beitreten, delegiert werden:

- Fähigkeit, Computerobjekte zu erstellen und zu löschen
- Fähigkeit, Passwörter zurückzusetzen
- Möglichkeit, Berechtigungen zu ändern
- Möglichkeit, Konten am Lesen und Schreiben von Daten zu hindern

- Bestätigte Fähigkeit zum Lesen und Schreiben von Kontoeinschränkungen
- Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service
- Überprüfte Fähigkeit zum Schreiben in den DNS-Hostnamen

Dabei handelt es sich um die Mindestanzahl an Berechtigungen, die erforderlich sind, um Computerobjekte mit Ihrem Active Directory zu verknüpfen. Weitere Informationen finden Sie in der Microsoft Windows Server-Dokumentation zum Thema Fehler: Zugriff wird verweigert, wenn Benutzer ohne Administratorrechte, denen die Steuerung delegiert wurde, versuchen, Computer mit einem Domänencontroller zu verbinden.

Abrufen der IP-Adresse für Ihr Gatewaygerät

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. Im Fall von Amazon-EC2-Gateways können Sie die IP-Adresse Ihrer Amazon-EC2-Instance auch aus der Amazon-EC2-Management-Konsole abrufen. Informationen zum Abrufen der IP-Adresse des Gateways finden unter:

- VMware Gastgeber: Zugreifen auf die lokale Konsole mit VMware ESXi
- Hyper-V-Host: Greifen Sie mit Microsoft auf die lokale Gateway-Konsole zu Hyper-V
- Linux kernelbasierte virtuelle Maschine (KVM)-Host: Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
- EC2-Host: Abrufen einer IP-Adresse von einem Amazon-EC2-Host

Wenn Sie die IP-Adresse gefunden haben, notieren Sie sie. Kehren Sie dann zur Storage-Gateway-Konsole zurück und geben Sie die IP-Adresse in der Konsole ein.

Abrufen einer IP-Adresse von einem Amazon-EC2-Host

Um die IP-Adresse der Amazon-EC2-Instance abzurufen, auf der das Gateway bereitgestellt wird, melden Sie sich bei der lokalen Konsole der EC2-Instance an. Rufen Sie dann die IP-Adresse am oberen Rand der Konsolenseite ab. Detaillierte 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.

Verfahren 1: Herstellen einer Verbindung mit dem Gateway über die öffentliche IP-Adresse

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich 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-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.

Verfahren 2: Herstellen einer Verbindung mit dem Gateway über die Elastic IP-Adresse

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich 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-Konsole zurück und geben Sie die Elastic IP-Adresse ein.

IPv6 Unterstützung

IPv6 Unterstützung ist nur für Gateway-Appliance-Versionen 2.x oder höher verfügbar. Gateway-Appliance-Version 1.x kann nicht auf Version 2.x aktualisiert werden. Sie müssen Ihr Gateway-Gerät, Version 1.x, migrieren oder ersetzen, um Support zu erhalten. IPv6

Die folgenden Dual-Stack-Endpunkte sind erforderlich für. IPv6

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

```
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
s3.dualstack.region.amazonaws.com
```

Grundlegendes zu Storage Gateway Gateway-Ressourcen und -Ressourcen IDs

In Storage Gateway ist die primäre Ressource ein Gateway, aber andere Ressourcentypen sind Dateifreigaben. Dateifreigaben werden als Unterressourcen bezeichnet und existieren nur, wenn sie einem Gateway zugeordnet sind.

Diesen Ressourcen und Unterressourcen sind eindeutige Amazon-Ressourcennamen (ARNs) zugeordnet, wie in dieser Tabelle dargestellt.

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`*

Mit Ressourcen arbeiten 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.

Ressourcen-IDs von Storage Gateway werden in Großbuchstaben geschrieben. Wenn Sie diese Ressourcen-IDs jedoch 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. In Storage Gateway könnte die ID für ein Gateway beispielsweise lautensgw-12A3456B. Wenn Sie diese ID mit der EC2-API verwenden, müssen Sie sie in ändern. `sgw-12a3456b` Andernfalls verhält sich die EC2-API möglicherweise nicht wie erwartet.

Tagging von Storage Gateway Gateway-Ressourcen

In Storage Gateway können Sie Tags verwenden, um Ihre Ressourcen zu verwalten. Mit Tags können Sie den Ressourcen Metadaten hinzufügen und sie so kategorisieren, dass 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.

Beispiel: Sie können Tags verwenden, um zu erkennen, von welcher Abteilung Storage-Gateway-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 File Gateway können Sie Tags verwenden, um den Zugriff auf Ressourcen zu steuern. Weitere Informationen über die entsprechende Vorgehensweise finden Sie unter Verwenden Sie Tags, um den Zugriff auf Ihr Gateway und Ihre Ressourcen zu kontrollieren.

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 zur Verwendung in AWS reserviert.
- Gültige Zeichen der Schlüsseleigenschaft sind UTF-8-Buchstaben und Zahlen, Leerzeichen und die Sonderzeichen + - = . _ : / und @.

Mit Tags arbeiten

Sie können mit Tags in der Storage-Gateway-Konsole, der Storage-Gateway-API oder der Befehlszeilenschnittstelle (CLI) für Storage Gateway arbeiten. 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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
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 Stiftsymbol neben dem Tag, 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-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
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).

Arbeiten mit Open-Source-Komponenten für AWS Storage Gateway

In diesem Abschnitt werden die Tools und Lizenzen von Drittanbietern beschrieben, auf die wir für die Bereitstellung von AWS Storage 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

Verschiedene Tools und Lizenzen von Drittanbietern werden verwendet, um Funktionen für Volume Gateway, Tape Gateway und Amazon S3 File Gateway bereitzustellen.

Verwenden Sie die folgenden Links, um den Quellcode für bestimmte Open-Source-Softwarekomponenten herunterzuladen, die in der AWS Storage Gateway Software enthalten sind:

- Für Storage Gateway Gateway-Appliances, die bereitgestellt werden auf VMware ESXi: sources.tar
- Für Storage Gateway Gateway-Geräte, die auf Microsoft Hyper-V bereitgestellt werden: sources_hyperv.tar

- Für Storage Gateway Gateway-Appliances, 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/) entwickelt wurde. Die entsprechenden Lizenzen für alle abhängigen Drittanbieter-Tools finden Sie unter Lizenzen von Drittanbietern.

Open-Source-Komponenten für Amazon S3 File Gateway

Für die Bereitstellung der Funktionen von Amazon S3 File Gateway (S3 File Gateway) werden mehrere Tools und Lizenzen von Drittanbietern verwendet.

Verwenden Sie die folgenden Links, um den Quellcode für bestimmte Open-Source-Softwarekomponenten herunterzuladen, die in der S3 File Gateway-Software enthalten sind:

- Für Amazon S3 File Gateway: sgw-file-s3-open-source.tgz

Dieses Produkt enthält Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL-Toolkit (http://www.openssl.org/) entwickelt wurde. Die entsprechenden Lizenzen für alle abhängigen Drittanbieter-Tools finden Sie unter Lizenzen von Drittanbietern.

Beschränkungen und Kontingente für Amazon S3 File Gateway

Kontingente für Dateifreigaben

In der folgenden Tabelle sind Kontingente für Dateifreigaben aufgeführt.

Description	Limit
Maximale Anzahl von Dateifreigaben pro Gateway **Note** Jede Dateifreigabe kann nur eine Verbindung zu einem S3-Bucket herstellen, aber mehrere Fileshares können eine Verbindung zu demselben	50

Description	Limit
Bucket herstellen. Wenn Sie mehr als eine Dateifreigabe mit demselben Bucket verbinden, müssen Sie jede Dateifreigabe so konfigurieren, dass sie einen eindeutigen, sich nicht überschne idenden Präfixnamen verwendet, um Konflikte zu vermeiden read/write . Die Anzahl der von einem Gateway verwalteten Dateifreigaben kann sich auf die Leistung des Gateways auswirken. Weitere Informationen finden Sie unter Leistungsanleitung für Gateways mit mehreren Dateifreigaben.	

Description	Limit
Die maximale Anzahl von Dateien, für die ein Gateway gleichzeitig Metadaten zwischens peichern kann **Note** Da S3 File Gateway von Amazon S3 unterstützt wird, gibt es keine maximale Ordnergröße oder Beschränkung für die Anzahl der Dateien, die Sie über ein Gateway speichern oder auf die Sie zugreifen können. Jedes Gateway hat ein konfiguri erbares Limit, das die Anzahl der Dateien bestimmt, für die es gleichzei tig Metadaten zwischenspeichern kann. Sie können die UpdateGatewayInfor mationAPI-Aktion verwenden, um GatewayCapacityauf `SmallMedium`, oder zu setzen`Large`. Diese Einstellu ng wirkt sich auf die Gateway-Leistung und die Hardwareempfehlungen aus. Weitere Informationen finden Sie unter Leistungsanleitung für Gateways mit mehreren Dateifreigaben.	Gateway-Kapazität: Klein — 5 Millionen Dateien Mittel — 10 Millionen Dateien Groß — 20 Millionen Dateien

Description	Limit
Die maximale Größe einer einzelnen Datei **Note** Wenn Sie versuchen, Dateien, die die Größenbeschränkung überschre iten, Stück für Stück zu schreiben, werden nur die ersten 5 TiB hochgelad en. Wenn Sie versuchen, Dateien, die die Größenbeschränkung überschre iten, auf einmal zu schreiben, wird auf Windows-Clients keine Datei und auf Linux-Clients eine Datei mit der Größe Null erstellt.	5 TiB
Maximale Pfadlänge **Note** Clients dürfen keinen Pfad erstellen , der diese Länge überschreitet. Dies würde zu einem Fehler führen. Diese Beschränkung gilt für beide von File Gateways unterstützten Protokolle, NFS und SMB. Die Pfadlänge in Byte wird anhand von Zeichenbitwerten in UTF-8-Kodierung berechnet.	1024 Bytes

Description	Limit
Maximale Länge des Dateinamens **Note** File Gateway unterstützt keine Dateinamen, die diese Länge überschreiten. Die Länge des Dateinamens in Byte wird anhand von Zeichenbitwerten in UTF-8-Kodierung berechnet.	255 Byte

Empfohlene Kapazität für die lokalen Datenträger des Gateways

In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt.

Gateway-Typ	Cache (Minimum)	Cache (Maximum)
S3 File Gateway	150 GiB	64 TiB

Note

Sie können ein oder mehrere lokale Laufwerke für Ihren Cache bis zur maximalen Kapazität konfigurieren.
Wenn Sie einem vorhandenen Gateway Cache hinzufügen, ist es wichtig, neue Festplatten auf Ihrem Host (Hypervisor oder Amazon EC2 EC2-Instance) zu erstellen. Ändern Sie nicht die Größe vorhandener Festplatten, wenn die Festplatten zuvor als Cache zugewiesen wurden.

Verwendung von Speicherklassen

Amazon S3 File Gateway unterstützt die Speicherklassen Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 One Zone-Infrequent Access, Amazon S3 Intelligent-Tiering und Amazon Glacier. Weitere Informationen zu Speicherklassen finden Sie unter Amazon S3 S3-Speicherklassen im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> S3 File Gateway unterstützt derzeit nicht die Speicherklasse Amazon S3 Glacier Instant Retrieval.

Themen

Verwenden von Speicherklassen mit einem File Gateway

Wenn Sie eine Dateifreigabe erstellen oder aktualisieren, können Sie eine Speicherklasse für Ihre Objekte auswählen. Sie können die Amazon S3 Standard-Speicherklasse oder eine der Speicherklassen S3 Standard-IA, S3 One Zone-IA oder S3 Intelligent-Tiering wählen. Objekte, die in einer dieser Speicherklassen gespeichert sind, können mithilfe einer Lebenszyklusrichtlinie auf GLACIER übertragen werden.

Amazon S3 S3-Speicherklasse	Überlegungen
Standard	Wählen Sie Standard aus, um Ihre häufig aufgerufenen Dateien redundant in mehreren Availability Zones zu speichern, die geografisch voneinander getrennt sind. Dies ist die Standardspeicherklasse. Weitere Informationen finden Sie unter Amazon S3 S3-Preise.
S3 Intelligent-Tiering	Wählen Sie Intelligent-Tiering, um die Speicherkosten zu optimieren, indem Sie Daten

Amazon S3 S3-Speicherklasse	Überlegungen
	automatisch in die kostengünstigste Speicherz ugriffsstufe verschieben. Objekte, die kleiner als 128 KB sind, kommen für Auto-Tiering in der Intelligent-Tiering-Speicherklasse nicht in Frage. Für diese Objekte gelten die Tarife für den häufigen Zugriff, und es fällt nicht die Überwachu ngsgebühr an, die für Objekte mit automatis cher Zuweisung erhoben wird. S3 Intelligent-Tiering unterstützt jetzt die Stufen Archive Access und Deep Archive Access. S3 Intelligent-Tiering verschiebt Objekte, auf die 90 Tage lang nicht zugegriffen wurde, automatisch in die Archive Access-Stufe und nach 180 Tagen ohne Zugriff in die Deep Archive Access-Stufe. Immer wenn ein Objekt in einer der Archivzugriffsebenen wiederher gestellt wird, wird das Objekt innerhalb weniger Stunden in die Stufe für häufigen Zugriff verschoben und kann abgerufen werden. Dies führt zu Timeoutfehlern für Benutzer oder Anwendungen, die versuchen, über eine Dateifreigabe auf Dateien zuzugreifen, wenn das Objekt nur in einer der beiden Archivsch ichten vorhanden ist. Verwenden Sie die Archivstufen nicht mit S3 Intelligent-Tiering, wenn Ihre Anwendungen über die vom File Gateway bereitgestellten Dateifreigaben auf Dateien zugreifen. Wenn Dateioperationen, die Metadaten aktualisieren (wie Besitzer, Zeitstempel, Berechtigungen und ACLs), für Dateien ausgeführt werden, die vom File Gateway

Amazon S3 S3-Speicherklasse	Überlegungen
	verwaltet werden, wird das bestehende Objekt gelöscht und eine neue Version des Objekts wird in dieser Amazon S3 S3-Speicherklasse erstellt. Überprüfen Sie, wie sich Dateioperationen auf die Objekterstellung auswirken, bevor Sie diese Speicherklasse in der Produktion verwenden. Weitere Informationen finden Sie unter Amazon S3 S3-Preise.

Amazon S3 S3-Speicherklasse	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. Für Objekte, die in der Standard-IA-Speich erklasse gespeichert sind, können zusätzliche Gebühren anfallen, wenn Objekte innerhalb von 30 Tagen überschrieben, gelöscht, angeforde rt, abgerufen oder zwischen Speicherklassen übertragen werden. Es gibt eine Mindestsp eicherdauer von 30 Tagen. Für Objekte, die vor 30 Tagen gelöscht wurden, fällt eine anteilige Gebühr an, die der Speichergebühr 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. Für Objekte, die kleiner als 128 KB sind, werden 128 KB berechnet, und es fallen Gebühren für vorzeitiges Löschen an. Wenn Dateioperationen, die Metadaten aktualisieren (wie Besitzer, Zeitstempel, Berechtigungen und ACLs), für Dateien ausgeführt werden, die vom File Gateway verwaltet werden, wird das bestehende Objekt gelöscht und eine neue Version des Objekts wird in dieser Amazon S3 S3-Speich erklasse erstellt. Sie sollten überprüfen, wie sich Dateioperationen auf die Objekterstellung auswirken, bevor Sie diese Speicherklasse in der Produktion verwenden, da Gebühren für vorzeitiges Löschen anfallen. Weitere Informati onen finden Sie unter Amazon S3 S3-Preise.

Amazon S3 S3-Speicherklasse	Überlegungen
S3 One Zone-IA	Wählen Sie One Zone-IA, um Ihre selten aufgerufenen Dateien in einer einzigen Availability Zone zu speichern. Für Objekte, die in der Speicherklasse One Zone-IA gespeichert sind, können zusätzliche Gebühren anfallen, wenn Objekte innerhalb von 30 Tagen überschrieben, gelöscht, angefordert, abgerufen oder zwischen Speicherklassen übertragen werden. Es gibt eine Mindestspeicherdauer von 30 Tagen, und für Objekte, die vor 30 Tagen gelöscht wurden, fällt eine anteilige Gebühr an, die der Speichergebühr 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. Für Objekte, die kleiner als 128 KB sind, werden 128 KB berechnet, und es fallen Gebühren für vorzeitiges Löschen an. Wenn Dateioperationen, die Metadaten aktualisieren (wie Besitzer, Zeitstempel, Berechtigungen und ACLs), für Dateien ausgeführt werden, die vom File Gateway verwaltet werden, wird das bestehende Objekt gelöscht und eine neue Version des Objekts wird 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 Gebühren für vorzeitiges Löschen anfallen. Weitere Informationen finden Sie unter Amazon S3 S3-Preise.

Sie können Objekte zwar direkt von einer Dateifreigabe in die Speicherklasse S3-Standard-IA, S3-One Zone-IA oder S3 Intelligent-Tiering schreiben, wir empfehlen jedoch, für die Übertragung Ihrer Objekte eine Lebenszyklusrichtlinie zu verwenden, anstatt direkt aus der Dateifreigabe zu schreiben, insbesondere wenn Sie das Objekt voraussichtlich innerhalb von 30 Tagen nach der Archivierung aktualisieren oder löschen. Informationen zur Lebenszyklusrichtlinie finden Sie unter Verwaltung des Objektlebenszyklus.

Verwendung der GLACIER-Speicherklasse mit File Gateway

Wenn Sie eine Datei mithilfe von Amazon S3-Lebenszyklusrichtlinien zu Amazon Glacier übertragen und die Datei für Ihre Fileshare-Clients über den Cache sichtbar ist, treten beim Aktualisieren der Datei I/O Fehler auf. Wir empfehlen Ihnen, CloudWatch Events so einzurichten, dass Sie bei Auftreten dieser I/O Fehler eine Benachrichtigung erhalten und anhand der Benachrichtigung entsprechende Maßnahmen ergreifen können. Sie können beispielsweise Maßnahmen ergreifen, um das archivierte Objekt in Amazon S3 wiederherzustellen. Nachdem das Objekt in S3 wiederhergestellt wurde, können Ihre Dateifreigabe-Clients über die Dateifreigabe darauf zugreifen und es aktualisieren.

Informationen zum Wiederherstellen archivierter Objekte finden Sie unter Wiederherstellen archivierter Objekte im Amazon Simple Storage Service-Benutzerhandbuch.

> **Important**
>
> S3 File Gateway unterstützt die Speicherklasse S3 Glacier Instant Retrieval offiziell nicht. Sie können Objekte in einem Fileshare-Bucket zwar mithilfe von Lebenszyklusrichtlinien oder direkten PUT Anfragen für S3 Glacier Instant Retrieval festlegen, aber S3 File Gateway kann nicht erkennen, welche Dateien sich in dieser Speicherklasse befinden, und führt Dateioperationen mit ihnen wie mit jedem anderen Objekt aus. Da S3 Glacier Instant Retrieval höhere Zugriffskosten verursacht als andere Amazon S3 S3-Speicherklassen, können Massendateivorgänge wie Virenscans und Umbenennungen zu hohen Amazon S3 S3-Rechnungen führen, wenn sie nicht sorgfältig verwaltet werden. `rsync` Aus diesem Grund empfehlen wir nicht, S3 Glacier Instant Retrieval mit S3 File Gateway zu verwenden.

Verwendung von Kubernetes Container Storage Interface-Treibern

Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen. In einer Kubernetes-Umgebung ähnelt ein Container

einer VM, aber ein Container verfügt über lockere Isolationseigenschaften, um das Betriebssystem (OS) für alle Anwendungen gemeinsam zu nutzen. Daher gelten Container als leichter als. VMs Ähnlich wie eine virtuelle Maschine hat ein Container sein eigenes Dateisystem, einen Anteil an zugewiesener CPU, Arbeitsspeicher, Prozessraum und mehr. Da sie von der zugrunde liegenden Infrastruktur entkoppelt sind, sind sie über Clouds und Betriebssystemverteilungen hinweg portabel. Wenn Sie über einen Kubernetes-Cluster verfügen, können Sie Kubernetes Container Storage Interface (CSI) -Treiber für alle Instances in Ihrem Cluster installieren und konfigurieren, damit sie ein vorhandenes Amazon S3 File Gateway als Speicher verwenden können.

Nachdem Sie die CSI-Treiber für den Typ der Dateifreigabe installiert haben, den Sie verwenden möchten, müssen Sie ein oder mehrere Speicherobjekte erstellen. Abhängig von der Art der Bereitstellung, die Kubernetes verwenden soll, wenn Ihre Pods Speicher anfordern, müssen Sie entweder ein einzelnes *`StorageClass`* Kubernetes-Objekt oder sowohl ein Objekt als auch ein *`PersistentVolume`* Objekt erstellen, um Ihre Kubernetes-Compute-Pods mit Ihrer Dateifreigabe zu verbinden. `PersistentVolumeClaim` Weitere Informationen finden Sie in der Kubernetes-Online-Dokumentation unter. https://kubernetes.io/docs/concepts/storage/

Themen

- Arbeiten mit SMB-CSI-Treibern
- Arbeiten mit NFS-CSI-Treibern

Arbeiten mit SMB-CSI-Treibern

Folgen Sie den Verfahren in diesem Abschnitt, um die CSI-Treiber zu installieren, zu konfigurieren oder zu löschen, die für die Verwendung einer SMB-Dateifreigabe auf einem Amazon S3 File Gateway für die Speicherung in Ihrem Kubernetes-Cluster erforderlich sind. Weitere Informationen finden Sie in der Open-Source-Dokumentation zum SMB-CSI-Treiber unter. GitHub https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md

> **Note**
>
> Wenn Sie ein `PersistentVolume` Objekt oder ein `StorageClass` Objekt erstellen, können Sie einen `ReclaimPolicy` Parameter angeben, um zu bestimmen, was mit dem externen Speicher passiert, wenn Objekte gelöscht werden. Der SMB-CSI-Treiber unterstützt die `Recycle` Optionen `Retain` und, unterstützt derzeit jedoch keine `Delete` Option.

Installieren Sie die Treiber

So installieren Sie die Kubernetes SMB CSI-Treiber:

1. Führen Sie in einem Befehlszeilenterminal mit Zugriff auf Ihren Kubernetes-Cluster den folgenden Befehl aus: `kubectl`

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. Warten Sie, bis der vorherige Befehl abgeschlossen ist, und stellen Sie dann mithilfe der folgenden Befehle sicher, dass die CSI-Treiber-Pods ausgeführt werden:

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
NAME                                 READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-smb-controller-56bfddd689-dh5tk  4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4  4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                   3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                   3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Erstellen Sie ein SMB-Objekt StorageClass

Um ein neues StorageClass SMB-Objekt für Ihren Kubernetes-Cluster zu erstellen:

1. Erstellen Sie eine Konfigurationsdatei `storageclass.yaml` mit einem Namen, der dem folgenden Beispiel ähnelt. Ersetzen Sie die angezeigten Informationen durch Ihre eigenen bereitstellungsspezifischen Informationen. *`ExampleValues`*

```
---
```

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub
 directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. Führen Sie in einem Befehlszeilenterminal mit Zugriff auf `kubectl` und den folgenden `storageclass.yaml` Befehl aus:

   kubectl apply -f storageclass.yaml

   > **Note**
   >
   > Sie können den auch erstellen, StorageClass indem Sie den `.yaml` Konfigurationstext aus dem vorherigen Schritt für die meisten Kubernetes-Verwaltungs- und Containerisierungsplattformen von Drittanbietern bereitstellen.

3. Konfigurieren Sie die Pods in Ihrem Kubernetes-Cluster so, dass sie die von Ihnen erstellten Pods verwenden. StorageClass Weitere Informationen finden Sie in der Kubernetes-Online-Dokumentation unter. https://kubernetes.io/docs/concepts/storage/

SMB und Objekte PersistentVolume erstellen PersistentVolumeClaim

Um neue SMBs PersistentVolume und PersistentVolumeClaim Objekte zu erstellen:

1. Erstellen Sie zwei Konfigurationsdateien. Eine benannte `persistentvolume.yaml` und eine benannte`persistentvolumeclaim.yaml`.
2. Fügen Sie für Inhalte hinzu`persistentvolume.yaml`, die dem folgenden Beispiel ähneln. Ersetzen Sie die angezeigten Informationen durch Ihre eigenen einsatzspezifischen Informationen. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
        driver: smb.csi.k8s.io
        readOnly: false
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. Fügen Sie für Inhalte hinzu`persistentvolumeclaim.yaml`, die dem folgenden Beispiel ähneln. Ersetzen Sie die angezeigten Informationen durch Ihre eigenen einsatzspezifischen Informationen. *`ExampleValues`*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
 name of the PersistentVolume you created
        storageClassName: ""
```

4. Führen Sie in einem Befehlszeilenterminal mit Zugriff auf `kubectl` und beide von Ihnen erstellten `.yaml` Dateien die folgenden Befehle aus:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > Sie können die PersistentVolumeClaim Objekte PersistentVolume und auch erstellen, indem Sie den `.yaml` Konfigurationstext aus dem vorherigen Schritt für die meisten Kubernetes-Verwaltungs- und Containerisierungsplattformen von Drittanbietern bereitstellen.

5. Konfigurieren Sie die Pods in Ihrem Kubernetes-Cluster so, dass sie die von Ihnen erstellten Pods verwenden. PersistentVolumeClaim Weitere Informationen finden Sie in der Kubernetes-Online-Dokumentation unter. https://kubernetes.io/docs/concepts/storage/

Treiber deinstallieren

So deinstallieren Sie die Kubernetes SMB CSI-Treiber:

- Führen Sie in einem Befehlszeilenterminal mit Zugriff auf Ihren Kubernetes-Cluster den folgenden Befehl aus: `kubectl`

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

Arbeiten mit NFS-CSI-Treibern

Folgen Sie den Verfahren in diesem Abschnitt, um die CSI-Treiber zu installieren, zu konfigurieren oder zu löschen, die für die Verwendung einer NFS-Dateifreigabe auf einem Amazon S3 File Gateway für die Speicherung in Ihrem Kubernetes-Cluster erforderlich sind. Weitere Informationen finden Sie in der Open-Source-Dokumentation zum NFS-CSI-Treiber unter. GitHub https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md

Installieren Sie die Treiber

So installieren Sie Kubernetes NFS CSI-Treiber:

1. Führen Sie in einem Befehlszeilenterminal mit Zugriff auf Ihren Kubernetes-Cluster den folgenden Befehl aus: `kubectl`

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --
2. Warten Sie, bis der vorherige Befehl abgeschlossen ist, und stellen Sie dann mithilfe der folgenden Befehle sicher, dass die CSI-Treiber-Pods ausgeführt werden:

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
            NODE
```

```
csi-nfs-controller-56bfddd689-dh5tk       4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4       4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                        3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-dr4s4                        3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Erstellen Sie ein NFS-Objekt StorageClass

Um ein StorageClass NFS-Objekt für Ihren Kubernetes-Cluster zu erstellen:

1. Erstellen Sie eine Konfigurationsdatei `storageclass.yaml` mit einem Namen, der dem folgenden Beispiel ähnelt. Ersetzen Sie die angezeigten Informationen durch Ihre eigenen bereitstellungsspezifischen Informationen. *`ExampleValues`*

   ```
   ---
   apiVersion: storage.k8s.io/v1
   kind: StorageClass
   metadata:
       name: example-nfs-classname
       namespace: example-namespace
   provisioner: nfs.csi.k8s.io
   parameters:
       server: gateway-dns-name-or-ip-address
       share: /example-share-name
   reclaimPolicy: Retain
   volumeBindingMode: Immediate
   mountOptions:
       - hard
       - nfsvers=4.1
   ```

2. Führen Sie in einem Befehlszeilenterminal mit Zugriff auf `kubectl` und den folgenden `storageclass.yaml` Befehl aus:

   kubectl apply -f storageclass.yaml

> **Note**
>
> Sie können den auch erstellen, StorageClass indem Sie den `.yaml` Konfigurationstext aus dem vorherigen Schritt für die meisten Kubernetes-Verwaltungs- und Containerisierungsplattformen von Drittanbietern bereitstellen.

3. Konfigurieren Sie die Pods in Ihrem Kubernetes-Cluster so, dass sie das neue Objekt verwenden, das Sie erstellt haben. StorageClass Weitere Informationen finden Sie in der Kubernetes-Online-Dokumentation unter. https://kubernetes.io/docs/concepts/storage/

Erstellen Sie PersistentVolume NFS und Objekte PersistentVolumeClaim

Um neue NFS PersistentVolume und PersistentVolumeClaim Objekte zu erstellen:

1. Erstellen Sie zwei Konfigurationsdateien mit dem Namen `persistentvolume.yaml` und`persistentvolumeclaim.yaml`.
2. Fügen Sie für Inhalte hinzu`persistentvolume.yaml`, die dem folgenden Beispiel ähneln. Ersetzen Sie die angezeigten Informationen durch Ihre eigenen einsatzspezifischen Informationen. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
```

```
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
            share: /example-share-name
```

3. Fügen Sie für Inhalte hinzu`persistentvolumeclaim.yaml`, die dem folgenden Beispiel ähneln. Ersetzen Sie die angezeigten Informationen durch Ihre eigenen einsatzspezifischen Informationen. *ExampleValues*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name
 of the PersistentVolume you created
    storageClassName: ""
```

4. Führen Sie in einem Befehlszeilenterminal mit Zugriff auf `kubectl` und beide `.yaml` Dateien die folgenden Befehle aus:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

> **Note**
>
> Sie können die PersistentVolumeClaim Objekte PersistentVolume und auch erstellen, indem Sie den `.yaml` Konfigurationstext aus dem vorherigen Schritt für die meisten Kubernetes-Verwaltungs- und Containerisierungsplattformen von Drittanbietern bereitstellen.

5. Konfigurieren Sie die Pods in Ihrem Kubernetes-Cluster so, dass sie das neue Objekt verwenden, das Sie erstellt haben. PersistentVolumeClaim Weitere Informationen finden Sie in der Kubernetes-Online-Dokumentation unter. https://kubernetes.io/docs/concepts/storage/

Treiber deinstallieren

So deinstallieren Sie die Kubernetes NFS CSI-Treiber:

- Führen Sie in einem Befehlszeilenterminal mit Zugriff auf Ihren Kubernetes-Cluster den folgenden Befehl aus: `kubectl`

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/uninstall-driver.sh | bash -s master --

AWS Storage Gateway Terraform-Modul

HashiCorpTerraform ist eine Open-Source-Engine für Infrastructure as Code (IaC), die mit der HashiCorp Configuration Language (HCL) entwickelt wurde. Terraform bietet einen konsistenten CLI- (Command Line Interface) -Workflow, der in Verbindung mit Amazon S3 File Gateway für die Back-End-Infrastruktur Hunderte von Cloud-Diensten verwalten und die Cloud APIs in deklarative Konfigurationsdateien kodifizieren kann.

Sie können Terraform verwenden, um ein Amazon S3 File Gateway sicher als virtuelle Maschine (VM) in Ihrer lokalen virtuellen Infrastruktur bereitzustellen. Terraform bietet Automatisierung für die virtuelle Infrastruktur vor Ort. Informationen zur schnellen Bereitstellung eines Amazon S3 File Gateways VMware mithilfe von Terraform in einer lokalen virtuellen Umgebung finden Sie unter Automatisieren von HashiCorp Amazon S3 File Gateway-Bereitstellungen in mit Terraform von. VMware

> **Note**
>
> Möglicherweise müssen Sie Terraform konfigurieren, um die neueste Version des Computer-Images für Ihre bevorzugte Hypervisor-Plattform zu erhalten. AWS Storage Gateway Storage Gateway Gateway-Maschinen-Images gilt die folgende Namenskonvention. Die an den Imagenamen angehängte Versionsnummer ändert sich mit jeder Versionsversion. `aws-storage-gateway-FILE_S3-1.25.0`

Diese Automatisierung bietet Ihnen ein anpassbares Terraform-Modul, mit dem Sie ein Amazon S3 File Gateway mit allen Ressourcen und Abhängigkeiten bereitstellen können, die für die vollständige Bereitstellung des Gateways und der Dateifreigaben in Ihrer VM-Umgebung erforderlich sind. Das Terraform-Modul stellt die Gateway-VM bereit, aktiviert das Gateway, konfiguriert die Cache-Festplatte, verbindet das Gateway mit einer Domain, erstellt die Amazon S3 S3-Buckets, erstellt die Dateifreigaben und ordnet sie Buckets zu. Ein vollständiges Beispiel für ein Repository, das Terraform-Code enthält, um die Ressourcen zu erstellen, die für den lokalen Betrieb von Amazon S3 File Gateway erforderlich sind, finden Sie im Quellcode des Terraform Storage Gateway Gateway-Moduls unter. GitHub

> **Note**
>
> Das Amazon S3 File Gateway-Modul für Terraform ist ein von der Community unterstütztes Projekt. Es ist nicht Teil eines AWS Dienstes. Bestmöglicher Support wird von der AWS Storage-Community bereitgestellt.

Storage-Gateway-API-Referenz

Zusätzlich zur Verwendung der Konsole können Sie die AWS Storage Gateway API verwenden, um Ihre Gateways programmgesteuert zu konfigurieren und zu verwalten. In diesem Abschnitt werden die AWS Storage Gateway Vorgänge, das Signieren von Anfragen zur Authentifizierung und die Fehlerbehandlung beschrieben. Weitere Informationen zu den für Storage Gateway verfügbaren Endpunkte finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

> **Note**
>
> Sie können den auch verwenden AWS SDKs , wenn Sie Anwendungen mit Storage Gateway entwickeln. Die AWS SDKs für Java, .NET und PHP umschließen die zugrunde liegende Storage Gateway Gateway-API und vereinfachen so Ihre Programmieraufgaben. Weitere Informationen zum Herunterladen der SDK-Bibliotheken finden Sie unter Beispiel-Code-Bibliotheken.

Themen

AWS Storage Gateway Erforderliche Anforderungsheader

In diesem Abschnitt werden die erforderlichen Header beschrieben, die Sie bei jeder POST-Anfrage senden müssen. AWS Storage Gateway 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.

Das folgende Beispiel zeigt Header, die in der ActivateGatewayOperation 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
```

Im Folgenden sind die Header aufgeführt, die in Ihren POST-Anfragen an enthalten sein müssen. AWS Storage Gateway Die unten aufgeführten Header, die mit „x-amz“ beginnen, sind -spezifische Header. AWS Alle anderen aufgeführten Header sind allgemeine Header für HTTP-Transaktionen.

Header	Description
`Authorization`	Der Autorisierungsheader enthält mehrere Informationen über die Anfrage, anhand derer festgestellt werden kann, ob es sich bei der Anfrage AWS Storage Gateway um eine gültige Aktion für den Anfordere r handelt. Das Format dieses Headers lautet wie folgt (Zeilenumbrüche dienen besserer Lesbarkeit): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= CalculatedSignature` In der vorherigen Syntax geben Sie das Jahr YourAccessKey, den Monat und den Tag (yyyymmdd), die Region und die an. CalculatedSignature Das Format des Autorisierungsheaders wird durch die Anforderungen des V4-Signaturprozesses bestimmt. AWS Detaillierte Informationen zum Signieren finden Sie unter dem Thema Signieren von Anforderungen.
`Content-Type`	Verwenden Sie `application/x-amz-json-1.1` es als Inhaltstyp für alle Anfragen an AWS Storage Gateway.

Header	Description
	`Content-Type: application/x-amz-json-1.1`
`Host`	Verwenden Sie den Host-Header, um den AWS Storage Gateway Endpunkt anzugeben, an den Sie Ihre Anfrage senden. `storagegateway.us-east-2.amazonaws.com` steht beispielsweise für den Endpunkt der Region USA Ost (Ohio). Weitere Informationen zu den verfügbaren Endpunkten finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der. AWS Storage GatewayAllgemeine AWS-Referenz `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 vorhanden ist, AWS Storage Gateway ignoriert der alle `Date` Header während der Anforderungsauthentifizierung. Das `x-amz-date` Format muss ISO8601 Basic im Format YYYYMMDD'T'HHMMSS'Z' sein. Wenn sowohl der Header als auch verwendet werden, `Date` muss das Format des `x-amz-date` Date-Headers nicht verwendet werden. ISO8601 `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 OperationName-Wert (z. B. "ActivateGateway„) kann in der API-Liste gefunden werden. Storage-Gateway-API-Referenz

Signieren von Anforderungen

Storage Gateway erfordert, dass Sie jede gesendete Anforderung durch eine Signatur 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 mit der Signatur in der Anforderung übereinstimmt, verarbeitet Storage Gateway die Anforderung. Andernfalls wird die Anforderung abgelehnt.

Storage Gateway unterstützt die Authentifizierung mittels AWS Signature Version 4. 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 berechnet, indem Sie mit Ihrem

geheimen Zugriffsschlüssel beginnen und anhand der Zeichenfolge für den Gültigkeitsbereich der Anmeldeinformationen eine Reihe von Hash-basierten Nachrichtenauthentifizierungscodes () HMACs erstellen.

Signatur-Berechnungsbeispiel

Das folgende Beispiel macht Sie damit vertraut, wie Sie eine Signatur für ListGateways erstellen. Das Beispiel kann als Referenz verwendet werden, um Ihre Signaturberechnungsmethode zu überprüfen.

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. Dies liegt daran, dass es für diese API (oder ein Storage Gateway APIs) keine Abfrageparameter 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 (mit hinzugefügten Zeilenumbrüchen zur besseren Lesbarkeit) lautet der Header:

```
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

Dieser Abschnitt enthält Referenzinformationen zu AWS Storage Gateway Fehlern. 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 Fehlercode für den Vorgang `ActivationKeyInvalid` wird jedoch nur für die ActivateGatewayAPI 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

In der folgenden Tabelle sind AWS Storage Gateway API-Ausnahmen aufgeführt. Wenn ein AWS Storage Gateway Vorgang 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 Bad Request (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

Exception	Fehlermeldung	HTTP-Statuscode
`InvalidAction`	Die angeforderte Aktion oder Operation ist ungültig.	400 Bad Request (400 Ungültige Anfrage)
`InvalidClientTokenId`	Das angegebene X.509-Zertifikat oder die angegebene AWS Zugriffss chlüssel-ID ist in unseren Aufzeichn ungen nicht vorhanden.	403 Forbidden
`InvalidGatewayRequ estException`	Eine der Operationsfehlercode-Nachri chten in Operationsfehlercodes.	400 Bad Request (400 Ungültige Anfrage)
`InvalidSignatureEx ception`	Die berechnete Anforderungssignat ur entspricht nicht der angegebenen Signatur. Überprüfen Sie Ihren AWS Zugriffsschlüssel und Ihre Signaturm ethode.	400 Bad Request (400 Ungültige Anfrage)
`MissingAction`	In der Anforderung fehlt ein Aktions- oder Operationsparameter.	400 Bad Request (400 Ungültige Anfrage)
`MissingAuthenticat ionToken`	Die Anfrage muss entweder eine gültige (registrierte) AWS Zugriffss chlüssel-ID oder ein X.509-Zertifikat enthalten.	403 Forbidden
`RequestExpired`	Die Anforderung liegt nach dem Ablaufdatum oder dem Anforderu ngsdatum (jeweils in 15-Minute n-Schritten) oder das Anforderu ngsdatum liegt mehr als 15 Minuten in der Zukunft.	400 Bad Request (400 Ungültige Anfrage)

Exception	Fehlermeldung	HTTP-Statuscode
`SerializationException`	Fehler bei der Serialisierung. Stellen Sie sicher, dass Ihre JSON-Nutzdaten wohlgeformt sind.	400 Bad Request (400 Ungültige Anfrage)
`ServiceUnavailable`	Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.	503 Service Unavailable (503 Service nicht verfügbar)
`SubscriptionRequiredException`	Die AWS Access Key ID benötigt ein Abonnement für den Dienst.	400 Bad Request (400 Ungültige Anfrage)
`ThrottlingException`	Rate überschritten.	400 Bad Request (400 Ungültige Anfrage)
`TooManyRequests`	Zu viele Anfragen	429 Zu viele Anfragen
`UnknownOperationException`	Eine unbekannte Operation wurde angegeben. Gültige Operationen werden in API-Aktionen für Storage Gateway aufgeführt.	400 Bad Request (400 Ungültige Anfrage)
`UnrecognizedClientException`	Das Sicherheits-Token der Anfrage ist ungültig.	400 Bad Request (400 Ungültige Anfrage)
`ValidationException`	Der Wert des Parameters ist ungültig oder außerhalb des Bereichs.	400 Bad Request (400 Ungültige Anfrage)

Operationsfehlercodes

Die folgende Tabelle zeigt die Zuordnung zwischen AWS Storage Gateway Operationsfehlercodes und Fehlercodes APIs , die die Codes zurückgeben können. 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
`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

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		CreateStorediSCSIVolume
DiskDoesNotExist	Der angegebene Datenträger ist nicht vorhanden.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	Der angegebene Datenträger ist nicht für Gigabyte ausgerichtet.	CreateStorediSCSIVolume
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 bestehende Konfiguration des Dateisystemzuordnungs-Endpunkts steht in Konflikt mit der angegebenen Konfiguration.	AssociateFileSystem

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
FileSystemAssociationEndpointIpAddressAlreadyInUse	Die angegebene Endpunkt-IP-Adresse wird bereits verwendet.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	Die IP-Adresse des Dateisystemzuordnungs-Endpunkts fehlt.	AssociateFileSystem
FileSystemAssociationNotFound	Die angegebene Dateisystemzuordnung wurde nicht gefunden.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
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:

- Inhaltstyp: Anwendung/ -1.1 x-amz-json
- 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.

Typ: Zeichenfolge

error

Enthält API-spezifische Fehlerdetails. Unter den allgemeinen Fehler (z. B. nicht spezifische Fehler für eine API) werden diese Fehlerinformationen nicht angezeigt.

Typ: Sammlung

errorCode

Einer der Operationsfehlercodes .

Typ: Zeichenfolge

errorDetails

Dieses Feld wird nicht in der aktuellen Version der API verwendet.

Typ: Zeichenfolge

message

Eine der Operationsfehlercode-Nachrichten .

Typ: Zeichenfolge

Beispielantwort auf einen Fehler

Der folgende JSON-Hauptteil wird zurückgegeben, wenn Sie die DescribeStoredi SCSIVolumes API verwenden und eine Gateway-ARN-Anforderungseingabe angeben, die nicht existiert.

```
{
  "__type": "InvalidGatewayRequestException",
```

```
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
}
```

Der folgende JSON-Text wird zurückgegeben, wenn ein 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."
}
```

API-Aktionen für Storage Gateway

Eine vollständige Liste der Storage-Gateway-Operationen finden Sie unter Aktionen in der AWS Storage Gateway -API-Referenz.

Dokumentenverlauf für das Amazon S3 File Gateway-Benutzerhandbuch

In der folgenden Tabelle werden wichtige Änderungen in den einzelnen Versionen dieses Benutzerhandbuchs nach April 2018 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
IPv6 Unterstützung	IPv6Support ist für Gateway-Appliance-Versionen 2.x oder höher verfügbar.	10. September 2025
Zusätzliche Hinweise zum Durchsatz und zur Optimierung	Das Kapitel Leistung und Optimierung enthält jetzt Empfehlungen und bewährte Methoden zur Maximierung des Durchsatzes Ihres S3 File Gateways und zur Optimierung Ihrer Bereitstellung für Anwendungsfälle mit SQL Server-Datenbanksicherungen. Weitere Informationen finden Sie unter Maximieren des S3 File Gateway-Durchsatzes und Optimieren von S3 File Gateway für SQL Server-Datenbanksicherungen.	13. Juni 2025
Funktion für Cache-Berichte hinzugefügt	S3 File Gateway kann jetzt einen Bericht mit den Metadaten für Dateien generieren, die sich derzeit im lokalen Upload-Cache für eine bestimmte Dateifreigabe befinden. Weitere Informati	31. März 2025

	onen finden Sie unter Erstellen eines Cache-Berichts für Ihr S3 File Gateway, Anzeigen und Verwalten von Cache-Berichten für Ihr S3 File Gateway und Grundlegendes zu den Informationen in den Cache-Berichten von S3 File Gateway.	
Unterstützung für serverseitige Dual-Layer-Verschlüsselung mit AWS KMS Schlüsseln (DSSE-KMS) wurde hinzugefügt	Sie können jetzt eine zweischichtige serverseitige Verschlüsselung mit AWS KMS Schlüsseln verwenden, um die Dateien zu verschlüsseln, die S3 File Gateway auf Amazon S3 hochlädt. Weitere Informationen zu DSSE-KMS finden Sie unter Verschlüsseln von Objekten, die von File Gateway in Amazon S3 gespeichert wurden.	13. September 2024

Option hinzugefügt, um Wartungsupdates ein- oder auszuschalten	Storage Gateway erhält regelmäßige Wartungsupdates, die Betriebssystem- und Software-Upgrades, Korrekturen zur Verbesserung der Stabilität, Leistung und Sicherheit sowie den Zugriff auf neue Funktionen beinhalten können. Sie können jetzt eine Einstellung konfigurieren, um diese Updates für jedes einzelne Gateway in Ihrer Bereitstellung ein- oder auszuschalten. Weitere Informationen finden Sie unter Gateway-Updates mit der AWS Storage Gateway Konsole verwalten.	6. Juni 2024
Neue SMB-Sicherheitsstufe hinzugefügt	S3 File Gateway unterstützt jetzt eine zusätzliche Sicherheitsstufe, mit der Sie die 256-Bit-AES-Verschlüsselung für SMB-Clientverbindungen erzwingen können. Weitere Informationen finden Sie unter Eine Sicherheitsstufe für Ihr Gateway festlegen.	23. Mai 2024

Versionsberichte und Versionshinweise zur Gateway-Appliance für S3 File Gateway	Es wurden Versionshinweise hinzugefügt, um die neuen und aktualisierten Funktionen, Verbesserungen und Korrekturen zu beschreiben, die in jeder Version der Amazon S3 File Gateway-Appliance enthalten sind. Sie können die Softwareversionsnummer eines Gateways über die Storage Gateway Gateway-Konsole oder mithilfe der ermitteln AWS CLI. Weitere Informationen finden Sie unter Versionshinweise — Gateway-Appliance-Software.	05. Oktober 2023
Die empfohlenen CloudWatch Alarme wurden aktualisiert	Der CloudWatch `HealthNotifications` Alarm gilt jetzt für alle Gateway-Typen und Hostplattformen und wird für diese empfohlen. Die empfohlenen Konfigurationseinstellungen wurden auch für `HealthNotifications` und `AvailabilityNotifications` aktualisiert. Weitere Informationen finden Sie unter Grundlegendes zu CloudWatch Alarmen Grundlegendes .	2. Oktober 2023

Die maximale Anzahl an Dateifreigaben pro Gateway wurde erhöht	S3 File Gateway unterstützt jetzt bis zu 50 Dateifreigaben pro Gateway, was gegenüber dem vorherigen Limit von 10 erhöht wurde. Auf diese Weise können Sie mehr Dateifreigaben auf einem einzigen Gateway erstellen und so die Anzahl der Gateways reduzieren, die Sie verwalten müssen. Weitere Informationen finden Sie unter Kontingente für Dateifreigaben.	18. Januar 2023
Unterstützung für DOS-Attribute hinzugefügt	S3 File Gateway unterstützt jetzt DOS-Attribute für in Amazon S3 gespeicherte Dateien. Auf diese Weise können Sie Windows-Dateiattribute wie „Schreibgeschützt“, „Versteckt“, „System“ und „Archiv“ beibehalten, wenn Dateien auf Amazon S3 hochgeladen werden. Weitere Informationen finden Sie unter Support für Dateiattribute in Amazon S3 File Gateway.	18. Januar 2023

Tipps GatewayClockOutOfSync zur Fehlerbehebung hinzugefügt	Der Abschnitt Problembehandlung: Probleme mit File Gateway enthält jetzt Richtlinien zur Problembehebung, die bei der Diagnose von Problemen helfen, die auftreten können, wenn Ihre Gateway-Systemuhr nicht mit der AWS Storage Gateway Gateway-Serverzeit synchronisiert ist. Weitere Informationen finden Sie unter Fehler: GatewayClockOutOfSync.	19. Oktober 2022
Zeitplanbasierte Drosselung der Netzwerkbandbreite hinzugefügt	S3 File Gateway unterstützt jetzt die zeitplanbasierte Drosselung der Netzwerkbandbreite für Datenuploads auf Amazon S3. Mit dieser Funktion können Sie die Netzwerkbandbreite begrenzen, die Ihr Gateway in bestimmten Zeiträumen verwendet, sodass Sie die Netzwerknutzung während der Hauptgeschäftszeiten besser verwalten können. Weitere Informationen finden Sie unter Bandbreite für Ihr S3 File Gateway verwalten.	18. Januar 2022

Aktualisierte Verfahren zur Gateway-Erstellung	Das Verfahren zum Erstellen eines neuen Gateways wurde aktualisiert, um Änderungen in der Storage Gateway Gateway-Konsole widerzuspiegeln. Weitere Informationen finden Sie unter Amazon S3 File Gateway erstellen und aktivieren.	12. Oktober 2021
Support für das erzwungene Schließen von Dateien auf SMB-Dateifreigaben	Sie können jetzt die Einstellungen für lokale Gruppen verwenden, um Gateway-Administratorberechtigungen zuzuweisen. Gateway-Administratoren können das Microsoft Management Console-Snap-In für gemeinsame Ordner verwenden, um das Schließen von Dateien zu erzwingen, die auf SMB-Dateifreigaben geöffnet und gesperrt sind. Weitere Informationen finden Sie unter Lokale Gruppen für Ihr Gateway konfigurieren.	12. Oktober 2021

Audit-Log-Unterstützung für NFS-Dateifreigaben	Sie können jetzt NFS-Dateifreigaben so konfigurieren, dass Auditprotokolle generiert werden, 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 unter Grundlegendes zu File Gateway-Auditprotokollen.	12. Oktober 2021
Unterstützung für Access Point-Alias	File Gateway-Dateifreigaben können jetzt über Access Point-Aliase im Bucket-Stil eine Verbindung zum Amazon S3 S3-Speicher herstellen. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	12. Oktober 2021
Unterstützung VPC VPC-Endpunkte und Access Points	File Gateway-Fileshares können jetzt über Access Points oder Schnittstellenendpunkte in Ihrer VPC Powered by eine Verbindung zu S3-Buckets herstellen. AWS PrivateLink Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	7. Juli 2021

Unterstützung für opportunistisches Sperren	File Gateway-Dateifreigaben können jetzt opportunistisches Sperren verwenden, um ihre Dateipufferungsstrategie zu optimieren, wodurch in den meisten Fällen die Leistung verbessert wird, insbesondere in Bezug auf Windows-Kontextmenüs. Weitere Informationen finden Sie unter Erstellen einer SMB-Dateifreigabe.	7. Juli 2021
FedRAMP-Compliance	Storage Gateway ist jetzt FedRAMP-konform. Weitere Informationen finden Sie unter Konformitätsprüfung für Storage Gateway.	24. November 2020
Benachrichtigung zum Datei-Upload für File Gateway	File Gateway bietet jetzt eine Datei-Upload-Benachrichtigung, die Sie benachrichtigt, wenn eine Datei vom File Gateway vollständig auf Amazon S3 hochgeladen wurde. Weitere Informationen finden Sie unter Benachrichtigung zum Hochladen von Dateien erhalten.	9. November 2020

Zugriffsbasierte Aufzählung für File Gateway	File Gateway bietet jetzt eine zugriffsbasierte Aufzählung, bei der die Aufzählung von Dateien und Ordnern auf einer SMB-Dateifreigabe auf der Grundlage der Freigabe gefiltert wird. ACLs Weitere Informationen finden Sie unter Erstellen einer SMB-Datei freigabe.	9. November 2020
File Gateway-Migration	File Gateway bietet jetzt einen dokumentierten Prozess zum Ersetzen eines vorhanden en File Gateways durch ein neues File Gateway. Weitere Informationen finden Sie unter Ersetzen eines File Gateways durch ein neues File Gateway.	30. Oktober 2020
Steigerung der Leseleist ung im Cold-Cache von File Gateway um das Vierfache	Storage Gateway hat die Cold-Cache-Leseleistung um das Vierfache erhöht. Weitere Informationen finden Sie unter Leistungsanleitung für File Gateways.	31. August 2020
Bestellen der Hardware-Appliance über die Konsole	Sie können die Hardware-Appliance jetzt über die AWS Storage Gateway Konsole bestellen. Weitere Informationen finden Sie unter Verwenden der AWS Storage Gateway Gateway-Hardware-Appliance.	12. August 2020

Support für FIPS-Endpunkte (Federal Information Processing Standard) in neuen Regionen AWS	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 (Zentral) aktivieren. Weitere Informationen finden Sie unter AWS Storage Gateway - Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	31. Juli 2020

Support für mehrere Dateifreigaben, die an einen einzelnen Amazon S3 S3-Bucket angehängt sind	File Gateway unterstützt jetzt das Erstellen mehrerer Dateifreigaben für einen einzelnen S3-Bucket und das Synchronisieren des lokalen Cache des File Gateways mit einem Bucket, basierend auf der Häufigkeit des Verzeichniszugriffs. Sie können die Anzahl der Buckets einschränken, die zur Verwaltung der Dateifreigaben erforderlich sind, die Sie auf Ihrem File Gateway erstellen. Sie können mehrere S3-Präfixe für einen S3-Bucket definieren und ein einzelnes S3-Präfix einer einzelnen Gateway-Dateifreigabe zuordnen. Sie können Gateway-Dateifreigabenamen auch so definieren, dass sie unabhängig vom Bucket-Namen sind, um der lokalen Namenskonvention für Dateifreigaben zu entsprechen. Weitere Informationen finden Sie unter Erstellen einer NFS-Dateifreigabe oder Erstellen einer SMB-Dateifreigabe.	7. Juli 2020

Erhöhung des lokalen Cache-Speichers von File Gateway um das Vierfache	Storage Gateway unterstützt jetzt einen lokalen Cache von bis zu 64 TB für File Gateway und verbessert so die Leistung für lokale Anwendungen, indem der Zugriff mit geringer Latenz auf größere Arbeitsdatensätze ermöglicht wird. Weitere Informationen finden Sie unter Empfohlene lokale Festplattengrößen für Ihr Gateway im Storage Gateway Gateway-Benutzerhandbuch.	7. Juli 2020
CloudWatch Amazon-Alarme in der Storage Gateway Gateway-Konsole anzeigen	Sie können jetzt CloudWatch Alarme in der Storage Gateway Gateway-Konsole anzeigen. Weitere Informationen finden Sie unter Grundlegendes zu CloudWatch Alarmen.	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 zur Auswahl eines FIPS-Endpunkts für ein File Gateway finden Sie unter Auswahl eines Service-Endpunkts.	22. Mai 2020

Neue Regionen AWS	Storage Gateway ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar. Weitere Informati onen finden Sie unter AWS Storage Gateway -Endpunkt e und -Kontingente in der Allgemeine AWS-Referenz.	7. Mai 2020
Unterstützung für die S3 Intelligent-Tiering-Speiche rklasse	Storage Gateway unterstützt jetzt die S3 Intelligent-Tierin g-Speicherklasse. Die S3 Intelligent-Tiering-Speiche rklasse optimiert die Speicherk osten, indem Daten automatis ch auf die kostengünstigste Zugriffsebene übertragen werden, ohne dass sich dies auf die Leistungsfähigkeit oder den Betriebsaufwand auswirkt. Weitere Informationen finden Sie unter Speicherklasse zum automatischen Optimieren häufig und selten aufgerufe ner Objekte im Amazon-Si mple-Storage-Service-Benutz erhandbuch.	30. April 2020
Neue AWS Region	Storage Gateway ist jetzt in der Region AWS GovCloud (USA-Ost) verfügbar. Weitere Informationen finden Sie unter AWS Storage Gateway - Endpunkte und -Kontingente in der Allgemeine AWS-Refer enz.	12. März 2020

Unterstützung für Linux KVM-Hypervisor (Kernel-basierte virtuelle Maschine)	Storage Gateway unterstützt jetzt die Bereitstellung eines On-Premises-Gateways auf der KVM-Virtualisierungsplattform. Gateways, die auf KVM bereitgestellt werden, verfügen über die gleiche Funktionalität und Funktionen wie die vorhandenen lokalen Gateways. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Hostanforderungen im Storage Gateway-Benutzerhandbuch.	4. Februar 2020
Support für VMware vSphere High Availability	Storage Gateway bietet jetzt Unterstützung für Hochverfügbarkeit, VMware um Storage-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen zu schützen. Weitere Informationen finden Sie unter Verwenden von VMware vSphere High Availability mit Storage Gateway im Storage Gateway Gateway-Benutzerhandbuch. Diese Version enthält auch Leistungsverbesserungen. Weitere Informationen finden Sie unter Leistung im Storage Gateway-Benutzerhandbuch.	20. November 2019

Support für Amazon CloudWatch Logs	Sie können jetzt File Gateways mit Amazon CloudWatch Log Groups konfigurieren, um über Fehler und den Zustand Ihres Gateways und seiner Ressourcen benachrichtigt zu werden. Weitere Informationen finden Sie unter Benachrichtigungen über Gateway-Integrität und Fehler bei Amazon CloudWatch Log Groups im Storage Gateway Gateway-Benutzerhandbuch.	4. September 2019
Neu AWS-Region	Storage Gateway ist jetzt in der Region Asien-Pazifik (Hongkong) verfügbar. Weitere Informationen finden Sie unter AWS Storage Gateway - Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	14. August 2019
Neu AWS-Region	Storage Gateway ist nun in der Region Mittlerer Osten (Bahrain) verfügbar. Weitere Informationen finden Sie unter AWS Storage Gateway - Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	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
SMB-Dateifreigabeunterstützung für Microsoft Windows ACLs	Für File Gateways können Sie jetzt Microsoft Windows-Zugriffskontrolllisten (ACLs) verwenden, um den Zugriff auf SMB-Dateifreigaben (Server Message Block) zu steuern. Weitere Informationen finden Sie unter Steuern des Zugriffs auf eine SMB-Dateifreigabe mithilfe von Microsoft Windows ACLs .	8. Mai 2019

File Gateway-Unterstützung für tagbasierte Autorisierung	File Gateway unterstützt jetzt die Tag-basierte Autorisierung. Sie können den Zugriff auf File Gateway-Ressourcen anhand der Tags auf diesen Ressourcen steuern. 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 der AWS Storage Gateway Hardware-Appliance in Europa	Die AWS Storage Gateway Hardware Appliance ist jetzt in Europa erhältlich. Weitere Informationen finden Sie unter AWS Storage Gateway - Hardware-Appliance-Regionen in der Allgemeine AWS-Referenz. Darüber hinaus können Sie jetzt den nutzbaren Speicher auf der AWS Storage Gateway Hardware Appliance von 5 TB auf 12 TB erhöhen und die installierte Kupfer-Netzwerkkarte durch eine 10-Gigabit-Glasfaser-Netzwerkkarte ersetzen. Weitere Informationen finden Sie unter Einrichten Ihrer Hardware-Appliance.	25. Februar 2019

Support für AWS Storage Gateway Hardware Appliance	Die AWS Storage Gateway Hardware Appliance enthält die Storage Gateway Gateway-Software, die auf einem Drittanbieter-Server vorinstalliert ist. Sie können die Appliance in der AWS-Managementkonsole verwalten. Die Appliance kann Datei-, Band- und Volume Gateways hosten. Weitere Informationen finden Sie unter Verwenden der Storage Gateway-Hardware-Appliance.	18. September 2018
Support für Server Message Block (SMB)-Protokolle	File Gateways bieten jetzt Unterstützung für Server Message Block (SMB)-Pro tokolle bei Dateifreigaben. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	20. Juni 2018

Frühere Aktualisierungen

In der folgenden Tabelle werden wichtige Änderungen in den einzelnen Versionen des AWS Storage Gateway -Benutzerhandbuchs beschrieben, die vor Mai 2018 veröffentlicht wurden.

Änderungen	Beschreibung	Änderungsdatum
Support für die Speicherklasse S3 One Zone-IA	Für File Gateways können Sie jetzt S3 One Zone-IA als Standardspeicherklasse für Ihre Dateifreigaben wählen. Diese Speicherklasse ermöglicht Ihnen das Speichern Ihrer Objektdaten in einer einzelnen Availability Zone in Amazon S3. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	4. April 2018

Änderungen	Beschreibung	Änderungsdatum
Neu AWS-Region	Tape Gateway ist jetzt in der Region Asien-Pazifik (Singapur) erhältlich. Weitere Informationen hierzu finden Sie unter AWS-Regionendie Storage Gateway unterstützen.	3. April 2018
Support für Cache-Aktualisierungsbenachrichtigungen, Requester Pays und vorgefertigte ACLs Amazon S3 S3-Buckets	Mit File Gateways können Sie nun eine Benachrichtigung erhalten, wenn ein Gateway die Aktualisierung des Caches für Ihren Amazon S3-Bucket abgeschlossen hat. Weitere Informationen finden Sie unter RefreshCache.html in der Storage Gateway API-Referenz. Für File Gateways können Sie jetzt angeben, dass der Anforderer oder Leser die Zugriffsgebühren bezahlt und nicht der Bucket-Besitzer. File Gateway kann nun dem Besitzer des S3-Buckets, der der NFS-Dateifreigabe zugeordnet ist, die volle Kontrolle über geschriebene Dateien geben. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	1. März 2018
Neu AWS-Region	Storage Gateway ist jetzt in der Region Europa (Paris) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionendie Storage Gateway unterstützen.	18. Dezember 2017

Änderungen	Beschreibung	Änderungsdatum
Support für Benachric htigungen zum Hochladen von Dateien und Erraten des MIME-Typs (Multipur pose Internet Mail Extension)	File Gateway kann jetzt Benachrichtigungen senden, wenn alle in Ihre NFS-Dateifreigabe geschriebenen Dateien auf Amazon S3 hochgeladen wurden. Weitere Informationen finden Sie NotifyWhenUploadedin der Storage Gateway API-Referenz. File Gateway kann jetzt den MIME-Typ für hochgelad ene Objekte anhand von Dateierweiterungen erraten. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	21. November 2017
Support für VMware ESXi Hypervisor Version 6.5	AWS Storage Gateway unterstützt jetzt VMware ESXi Hypervisor Version 6.5. Diese Version wird zusätzlic h zu den Versionen 4.1, 5.0, 5.1, 5.5 und 6.0 unterstüt zt. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	13. September 2017
Unterstützung für den Hypervisor Microsoft Hyper-V in der File Gateway-K onfiguration	Es ist nun möglich, ein File Gateway auf dem Hypervisor Microsoft Hyper-V bereitzustellen. Weitere Informationen finden Sie unter Unterstützte Hyperviso ren und Host-Anforderungen.	22. Juni 2017
Neu AWS-Region	Storage Gateway ist jetzt in der Region Asien-Paz ifik (Mumbai) erhältlich. Weitere Informationen hierzu finden Sie unter AWS-Regionendie Storage Gateway unterstützen.	02. Mai 2017

Änderungen	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 einer Dateifreigabe. In der File-Gateway-Konfiguration lassen sich nun alle Objekte im Amazon-S3-Bucket finden, die hinzugefügt oder entfernt wurden, seit das Gateway letztmals die Inhalte des Buckets aufgelistet und die Ergebnisse zwischengespeichert hat. Weitere Informationen finden Sie RefreshCachein der API-Referenz.	28. März 2017
Unterstützung für File Gateways in Amazon EC2	AWS Storage Gateway bietet jetzt die Möglichkeit, ein File Gateway in Amazon EC2 bereitzustellen. Sie können in Amazon EC2 einen File Gateway auf der Basis des Storage Gateway-Amazon Machine Image (AMI) starten, das nun als Community-AMI verfügbar ist. Informationen darüber, wie Sie ein File Gateway erstellen und es auf einer EC2-Instance bereitstellen, finden Sie unter. Erstellen und Aktivieren eines Amazon S3 File Gateways Informationen zum Starten eines File Gateway-AMI finden Sie unterStellen Sie einen Amazon EC2 EC2-Standardhost für S3 File Gateway bereit. Darüber hinaus unterstützt File Gateway jetzt die HTTP-Proxykonfiguration. Weitere Informationen finden Sie unter Routing Ihres auf Amazon EC2 bereitgestellten Gateways über einen HTTP-Proxy.	08. Februar 2017

Änderungen	Beschreibung	Änderungsdatum
Neu AWS-Region	Storage Gateway ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionendie Storage Gateway unterstützen.	13. Dezember 2016
Neu AWS-Region	Storage Gateway ist jetzt in der Region Kanada (Zentral) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionendie Storage Gateway unterstützen.	08. Dezember 2016
Unterstützung für File Gateway	Zusätzlich zu Volume Gateways und Tape Gateway bietet Storage Gateway jetzt File Gateway. File Gateway kombiniert einen Service und eine virtuelle Software-Appliance. So können Sie Objekte in Amazon S3 mit Dateiprotokollen nach Branchens tandard wie beispielsweise NFS (Network File System) speichern und abrufen. Das Gateway stellt Objekte in Amazon S3 als Dateien auf einem NFS-Mounting-Punkt bereit.	29. November 2016

Migrationskampagne von Storage Gateway AL2 zu AL2023

AWSstellt das Betriebssystem (OS) der Storage Gateway Gateway-Appliance von Amazon Linux 2 auf AL2023 um, um neue Hybrid-Cloud-Speicherfunktionen zu ermöglichen und optimale Leistungs- und Sicherheitsstandards aufrechtzuerhalten. Dieser Übergang wird sich auf alle AL2-based Storage Gateway Gateway-Appliance-Versionen S3 File Gateway Version 1.x, Tape Gateway Version 2.x und Volume Gateway Version 2.x auswirken. Sie müssen die Migration vor dem 30. Juni 2026 abschließen, da der Support für AWS diese Systeme danach eingestellt wird.

Sie können anhand mehrerer Methoden feststellen, ob Ihre Gateways migriert werden müssen. Die AWS Konsole zeigt auf der Registerkarte „Details“ des Gateways für die betroffenen Gateways eine Meldung über eine veraltete Version an. Darüber hinaus bietet die `DescribeGatewayInformation`API programmatischen Zugriff, um das Feld mit dem Verfallsdatum zu überprüfen. Das AWS Health Dashboard listet die betroffenen Gateways auf der Registerkarte Betroffene Ressourcen auf. Die Liste wird jedoch nicht unmittelbar nach der Migration eines Gateways aktualisiert. Der Migrationsprozess selbst ist so konzipiert, dass die Datensicherheit oberste Priorität hat. AWS Vor Beginn der Migration wird eine Kopie der lokalen Gateway-VM-Daten gespeichert, um bei Bedarf eine einfache Wiederherstellung zu ermöglichen.

AWSbietet umfassende Migrationsleitfäden, die für jeden Gateway-Typ spezifisch sind. Nach Abschluss der Migration sollten Sie überprüfen, ob die Migration erfolgreich war, indem Sie überprüfen, ob auf der Registerkarte Gateway-Details der AWS Konsole keine Verfallswarnungen mehr angezeigt werden, oder indem Sie die `DescribeGatewayInformation`API verwenden, um zu bestätigen, dass das Feld für das Verfallsdatum nicht vorhanden ist. Entscheidend ist, dass Sie nach erfolgreicher Migration auf AL2023 nicht zu Ihrem AL2-Gateway zurückkehren dürfen, da eine Wiederherstellung zu Betriebsproblemen führen kann.

Während des gesamten Migrationszeitraums AWS erhalten Sie monatliche Erinnerungsbenachrichtigungen per E-Mail und die Registerkarte Geplante Änderungen im AWS Health Dashboard, um Sie bei der Planung und Durchführung Ihrer Migrationen zu unterstützen. Wenn Sie während der Migration auf Probleme stoßen, wenden Sie sich an den AWSSupport, um Unterstützung und Anleitungen zur Fehlerbehebung zu erhalten.

Schnelllinks und Ressourcen

Referenz zur Migration von Gateway-Versionen

Anhand der Versionsnummer der Gateway-Software ist es einfach zu verstehen, welche Gateways migriert werden müssen. Es ist wichtig zu beachten, dass selbst kürzlich aktivierte Gateways, die auf dem Betriebssystem Amazon Linux 2 basieren, noch bis zum 30. Juni 2026 migriert werden müssen.

Gateway-Typ	AL2-Version (erfordert Migration)	AL2023 Version (Ziel)
S3-Dateigateway	Version 1.x	Ausführung 2.x
Tape Gateway	Ausführung 2.x	Ausführung 3.x
Volume Gateway	Ausführung 2.x	Ausführung 3.x

Zeitplan für die Migration

Der Zeitplan für die Migration umfasst mehrere wichtige Meilensteine:

- 28. Oktober 2025: Alle neuen Gateway-Bereitstellungen, die über die Storage Gateway Gateway-Konsole initiiert werden, verwenden standardmäßig AL203-Images.
- 5. Januar 2026: AWS beginnt mit der Einschränkung neuer AL2-Gateway-Aktivierungen.
- 30. Juni 2026: AL2-based Gateways erhalten keine Softwareupdates mehr und der Support wird eingestellt. AWS Nach diesem Datum können Sie die AL2-based Appliances zwar weiterhin verwenden, sie erhalten jedoch keine neuen Softwareupdates, Sicherheitspatches oder Bugfixes. Die Wartung dieser Systeme liegt in Ihrer alleinigen Verantwortung.

Pre-migration Checkliste

> **Important**
>
> Bevor Sie mit dem Migrationsprozess beginnen, überprüfen Sie die folgenden Anforderungen, um eine erfolgreiche Migration sicherzustellen.

- Verwenden Sie das neueste Gateway-Image. Gehen Sie beim Erstellen der neuen Storage Gateway Gateway-VM wie folgt vor:
  - Verwenden Sie für Amazon EC2 EC2-Gateways das neueste AMI aus dem öffentlichen SSM-Parameter oder verwenden Sie die Storage Gateway Gateway-Konsole.
  - Laden Sie für lokale Gateways das neueste VM-Image von der Storage Gateway Gateway-Konsole herunter.
- Passen Sie die Hardwarekonfiguration an. Stellen Sie sicher, dass die neue Gateway-VM dieselbe CPU, denselben Arbeitsspeicher und denselben Netzwerkdurchsatz verwendet wie das vorhandene Gateway. Verwenden Sie für EC2-Gateways denselben Instanztyp.
- Überprüfen Sie die Größe der Root-Festplatte. Die Stammfestplatte der neuen Gateway-VM muss mindestens dieselbe Größe wie die Stammfestplatte des vorhandenen Gateways haben. Wenn auf der vorhandenen Root-Festplatte weniger als 20 GB verfügbarer Speicherplatz zur Verfügung stehen, passen Sie die Größe der neuen Root-Festplatte wie folgt an: (Größe der vorhandenen Root-Festplatte) + (20 GB abzüglich des verfügbaren Speicherplatzes auf der vorhandenen Root-Festplatte).
- Wenden Sie ausstehende Softwareupdates an. Bevor Sie mit der Migration beginnen, wenden Sie alle ausstehenden Softwareupdates auf dem vorhandenen Gateway an. Öffnen Sie die Storage Gateway Gateway-Konsole, wählen Sie Ihr Gateway aus und wählen Sie Jetzt aktualisieren, falls verfügbar.
- Überprüfen Sie die Netzwerkkonnektivität vom neuen Gateway aus. Bevor Sie mit der Migration beginnen, stellen Sie sicher, dass die neue Gateway-VM Folgendes erreichen kann:
  - Storage Gateway Gateway-Dienstendpunkte (oder Ihre VPC-Endpunkte).
  - Amazon S3 S3-Endpunkte.
  - Active Directory-/DNS-Server (wenn Ihr Gateway in eine Domäne eingebunden ist).
  - Verwenden Sie den Netzwerkverbindungstest der lokalen Gateway-Konsole, um zu überprüfen, ob alle Endgeräte erfolgreich sind.
- Beheben Sie fehlgeschlagene Datei-Uploads. Stellen Sie sicher, dass die `FilesFailingUpload` CloudWatch Metrik Ihres Gateways Null ist, bevor Sie mit der Migration beginnen. Dateien in einem fehlerhaften Zustand weisen auf ungelöste Fehler hin, die zuerst behoben werden sollten. Um die betroffenen Dateien zu identifizieren, erstellen Sie einen Cache-Bericht und beheben Sie dann die zugrunde liegenden Probleme, bevor Sie fortfahren.
- Warten Sie, bis der Cache synchronisiert ist. Stellen Sie sicher, dass die `CachePercentDirty` Metrik auf der Registerkarte Überwachung des Gateways 0 ist. Dadurch wird bestätigt, dass alle zwischengespeicherten Daten auf S3 hochgeladen wurden.

Leitfäden zur Migration

- Leitfaden zur Migration von S3 File Gateway
- Leitfaden zur Migration von Tape Gateway
- Leitfaden zur Migration von Volume Gateway

Support und Überwachung

- Storage Gateway Gateway-Konsole
- AWSPersonal Health Dashboard
- AWSSupport kontaktieren

Häufig gestellte Fragen

Was passiert mit meinen Daten während der Migration?

Ihre Daten bleiben während des AWS gesamten Migrationsprozesses dauerhaft gespeichert. Das Migrationsverfahren umfasst das Speichern einer Kopie Ihrer lokalen Gateway-VM-Daten AWS zur einfachen Wiederherstellung, falls erforderlich.

Wird es während der Migration zu Ausfallzeiten kommen?

Der Zeitpunkt der Migration und mögliche Serviceunterbrechungen hängen vom Typ und der Konfiguration Ihres Gateways ab. Ausführliche Informationen finden Sie im Gateway-spezifischen Migrationsleitfaden für Ihre Bereitstellung.

Was passiert, wenn ich nicht bis zum 30. Juni 2026 migriere?

Ihr Gateway wird weiterhin normal funktionieren und die Daten werden sicher gespeichertAWS, aber Sie müssen die betroffenen Gateways bis zum 30. Juni 2026 migrieren, um weiterhin Updates und Support zu erhalten.

Kann ich mein AL2-basiertes Gateway nach der Migration weiter verwenden?

Nein, Sie sollten Ihr AL2-Gateway nach erfolgreicher Migration nicht zusammen mit Ihrem AL2023 AL2023-Gateway verwenden. Verwenden Sie in Zukunft nur noch Ihr neues AL2023-based Gateway. Die gleichzeitige Verwendung von AL2- und AL203-Gateways kann zu Betriebsproblemen führen.

Ich habe Probleme bei der Migration. Was soll ich tun?

Wenden Sie sich an den AWSSupport, um Unterstützung zu erhalten Unser Support-Team kann Ihnen bei der Behebung von Migrationsproblemen helfen und Sie durch den Prozess führen.

Versionshinweise für Gateway-Appliance-Software

In diesen Versionshinweisen werden die neuen und aktualisierten Funktionen, Verbesserungen und Korrekturen beschrieben, die in jeder Version der Amazon S3 File Gateway enthalten sind. Jede Softwareversion wird durch ihr Veröffentlichungsdatum und eine eindeutige Versionsnummer identifiziert.

Sie können die Softwareversionsnummer eines Gateways ermitteln, indem Sie die Seite „Details“ in der Storage Gateway Gateway-Konsole überprüfen oder die DescribeGatewayInformationAPI-Aktion mit einem AWS CLI Befehl aufrufen, der dem folgenden ähnelt:

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

Die Versionsnummer wird im `SoftwareVersion` Feld der API-Antwort zurückgegeben.

> **Note**
>
> Unter den folgenden Umständen meldet ein Gateway keine Informationen zur Softwareversion:
>
> - Das Gateway ist offline.
> - Auf dem Gateway wird ältere Software ausgeführt, die keine Versionsberichterstattung unterstützt.
> - Der Gateway-Typ ist nicht S3 File Gateway.

Weitere Informationen zu S3 File Gateway , einschließlich der Änderung des standardmäßigen automatischen Wartungs- und Aktualisierungszeitplans für ein Gateway, finden Sie unter Gateway-Updates mit der AWS Storage Gateway Console verwalten.

Weitere Informationen zur Migration von S3 File Gateway von Amazon Linux 2 auf AL2023 finden Sie unter. Migration von AL2 nach AL2023

Gateways auf Basis von Amazon Linux 2023 (AL2023)

In der folgenden Tabelle sind die Versionshinweise für Gateways aufgeführt, die auf AL2023 basieren.

> **Note**
>
> Die Gateway-Versionen 1.x.x können nicht auf 2.x.x aktualisiert werden.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-06-16	2.1.8	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-05-21	2.1.7	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-05-14	2.1.6	Wartungsupdates: • Verbesserungen bei der Migration von 1.x auf 2.x (AL2 auf AL2023). • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-04-16	2.1.5	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-03-26	2.1.4	Wartungsupdates:

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		Note Diese Version führt eine stärkere Abhängigkeit vom DCE/RPC Endpoint Mapper-Dienst (TCP-Port 135) auf AD-Domänencontrollern ein. Wenn Ihre Umgebung ausgehenden Datenverkehr an diesem Port blockiert, entsperren Sie ihn, um Verbindungsprobleme zu vermeiden. Einzelheiten finden Sie unter Port-Anforderungen für File Gateway. • NTLM für Interaktionen zwischen Active Directory-Domänencontrollern und dem Gateway wird weiterhin als veraltet eingestuft. • Verbesserte Resilienz des SMB-Stacks bei Netzwerkunterbrechungen.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-03-16	2.1.3	Wartungsupdates: • Verbesserte Widerstan dsfähigkeit von DNS gegenüber SMB-Verkehr. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-03-02	2.0.7	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-02-12	2.1.2	Wartungsupdates: **Note** Der Rollout wurde angehalten. Diese Version wurde für eine begrenzte Anzahl von Gateways eingeführt. • Behebt ein Problem mit fehlenden Sicherheits- und Kontingent-Tabs bei der Verwendung von Windows Explorer auf einer SMB-Freigabe. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-02-02	2.1.1	Wartungsupdates: **Note** Der Rollout wurde angehalten. Diese Version wurde für eine begrenzte Anzahl von Gateways eingeführt. • Problem mit SMB beim Dateizugriff ohne Berücksichtigung von Groß- und Kleinschreibung behoben. • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.
2026-01-21	2.0.6	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-01-16	2.1.0	Wartungsupdates: **Note** Der Rollout wurde angehalten. Diese Version wurde für eine begrenzte Anzahl von Gateways eingeführt. • Der SMB-Stack wurde aktualisiert. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-12-15	2.0.5	Wartungsupdates: • Ein Problem mit der Metrik zur Root-Disc-Größe wurde behoben. • Betriebssystem und Softwareelemente wurden aktualisiert, um Sicherheit und Leistung zu verbessern.
2025-11-12	2.0.4	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-11-12	2.0.4	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-10-15	2.0.3	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
15.09.2025	2.0.2	Wartungsupdates: • Es wurde ein Problem behoben, das eine Änderung der Gateway-K apazität verhinderte. • Ein Problem mit der `UpdateSMBLocalGrou ps` API wurde behoben. • Betriebssystem und Softwareelemente wurden aktualisiert, um Sicherheit und Leistung zu verbessern.
2025-08-29	2.0.1	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung. • Erste Version für lokale Gateways.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-08-21	2.0.0	Features: • Erste Veröffentlichung des neuen Betriebssystems. • IPv6-Unterstützung hinzugefügt.

Amazon Linux 2 (AL 2) basierte Gateways

In der folgenden Tabelle sind die Versionshinweise für Gateways aufgeführt, die auf basieren. AL2

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-06-16	1,28,8	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-05-26	1,28,7	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-05-18	1.28.6	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2026-04-16	1,28,5	Wartungsupdates:

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-03-26	1.28.4	Wartungsupdates: **Note** Diese Version ist nur für Gateways verfügbar, die bereits auf Version 1.28 installiert sind. * **Note** Diese Version führt eine stärkere Abhängigkeit vom DCE/RPC Endpoint Mapper-Dienst (TCP-Port 135) auf AD-Domänencontroll ern ein. Wenn Ihre Umgebung ausgehend en Datenverkehr an diesem Port blockiert, entsperren Sie ihn, um Verbindungsproblem e zu vermeiden. Einzelheiten finden Sie unter Port-Anfo rderungen für File Gateway. • NTLM für Interaktionen zwischen Active Directory

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		-Domänencontrollern und dem Gateway wird weiterhin als veraltet eingestuft. • Verbesserte Resilienz des SMB-Stacks bei Netzwerkunterbrechungen.
2026-03-16	1,27,21	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.
2026-03-16	1,28,3	Wartungsupdates: **Note** Diese Version ist nur für Gateways verfügbar, die bereits auf Version 1.28 installiert sind. * • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.
2026-02-27	1,27,20	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-02-11	1.28.2	Wartungsupdates: **Note** Der Rollout wurde angehalten. Diese Version wurde für eine begrenzte Anzahl von Gateways eingeführt. • Behebt ein Problem mit fehlenden Sicherheits- und Kontingent-Tabs bei der Verwendung von Windows Explorer auf einer SMB-Freigabe. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-02-02	1,28,1	Wartungsupdates: **Note** Der Rollout wurde angehalten. Diese Version wurde für eine begrenzte Anzahl von Gateways eingeführt. • Problem mit SMB beim Dateizugriff ohne Berücksichtigung von Groß- und Kleinschreibung behoben. • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.
2026-01-21	1,27,19	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-01-16	1.28.0	Wartungsupdates: **Note** Der Rollout wurde angehalten. Diese Version wurde für eine begrenzte Anzahl von Gateways eingeführt. • Der SMB-Stack wurde aktualisiert. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-12-15	1,27,18	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-11-17	1,27,17	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-10-15	1,27,16	Wartungsupdates: • Ein Problem im Protokoll „Upload Rename Order“ wurde behoben. • Betriebssystem und Softwareelemente wurden aktualisiert, um Sicherheit und Leistung zu verbessern.
2025-09-22	1,27,15	Wartungsupdates: • Ein Problem im Protokoll „Upload Rename Order“ wurde behoben.
15.09.2025	1,27,14	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-08-21	1,27,13	Wartungsupdates: • Systemstatistiken und Metriken wurden hinzugefü gt, um tiefere Einblicke in die Gateway-Leistung zu erhalten.
2025-08-18	1,27,12	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-08-11	1,27,11	Wartungsupdates: • Es wurde ein Problem behoben, das sich auf S3 Metadaten-Updates bei bestimmten Dateioperationen für einige Gateways auswirkte.
2025-07-15	1,27,10	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung. • Probleme mit dem Upload Rename Order Log für Gateways wurden behoben.
2025-06-23	1,27,9	Wartungsupdates: • Probleme mit dem Upload Rename Order Log für Gateways wurden behoben. • Das Hochladen des Protokolls zur Umbenennung von Bestellungen für neue Gateways wurde aktiviert. • Das Problem wurde behoben, sodass das Gateway Löschvorgänge für Dateien, die nicht erfolgreich hochgeladen wurden, jetzt korrekt verarbeitet.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-06-16	1,27,8	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-05-26	1,27,7	Wartungsupdates: • Probleme bei der Bestellun g von Umbenennungen wurden behoben. Note Dieses Problem betrifft nur einige Gateways. Sie werden benachric htigt, wenn Ihr Gateway aktualisiert werden muss. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
15.05.2025	1,27,6	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-04-28	1,27,5	Wartungsupdates: • Probleme im Zusammenh ang mit dem Upload-Pr otokoll zur Umbenennung von Bestellungen wurden behoben. • Es wurden Debug-Too ls hinzugefügt, um die Ursachen von Upload-Pr oblemen zu ermitteln. • Es wurden Systemsta tistiken und Metriken hinzugefügt, um einen tieferen Einblick in die Gateway-Leistung zu erhalten. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-04-14	1.27.4	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2025-04-01	1,27,3	Wartungsupdates: • Update für die Konfigura tion der Gateway-Protokolli erung. Es ist kein Eingreifen des Kunden erforderlich.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-03-17	1,27,2	Wartungsupdates: • Es wurde eine API-Aktion hinzugefügt, die zwischengespeicherte Dateifreigabedaten und Metadaten für Dateien entfernt, die nicht von Ihrem Gateway zu Amazon S3 hochgeladen werden konnten. Sie AWS-Konto müssen auf der Zulassungsliste stehen, um diese Funktion nutzen zu können. Wenn Ihr Gateway Probleme mit Dateien hat, die beim Hochladen fehlschlagen, AWS Support kann er die Funktion entsperren und Ihnen Hinweise zur Verwendung geben. • Neue Gateways haben jetzt die Möglichkeit, die Reihenfolge der Upload-Vorgänge beim Umbenennen von Objekten zu protokollieren. Dadurch wird verhindert, dass Dateien nach wiederholten oder sich überschneidenden Umbenennungsvorgängen nicht auf Amazon S3 hochgeladen werden können.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		• Ein Problem im Zusammenhang mit dem unbeabsichtigten Öffnen von Ports durch SMB wurde behoben. • Betriebssystem und Softwareelemente wurden aktualisiert, um Sicherheit und Leistung zu verbessern.
2025-02-17	1,27,1	Wartungsupdates: • Java 11 wurde entfernt. • Cache-Funktion zur Support Verwendung hinzugefügt. • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-01-17	1.27.0	Features: • Cache-Berichte (demnächst verfügbar) — Die Gateway-Software wurde aktualisiert, um die Einführung einer neuen Funktion zur Generierung von Berichten über die Dateimetadaten zu unterstützen, die derzeit von einem S3 File Gateway zwischengespeichert werden. Sie können diese Berichte verwenden, um Probleme zu beheben, wenn Sie Dateien haben, die nicht von Ihrem Gateway zu Amazon S3 hochgeladen werden können. Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.
2025-01-09	1,26,9	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-12-18	1,26,8	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2024-11-18	1,26,7	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2024-10-17	1,26,6	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2024-09-30	1,26,5	Wartungsupdates: • Es wurde ein Problem behoben, bei dem lokale Gateways keine Supportka näle zuließen • Betriebssystem und Softwareelemente wurden aktualisiert, um Sicherheit und Leistung zu verbessern.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-09-16	1.26.3	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2024-08-21	1,26,1	Wartungsupdates: • Ein Problem im Zusammenh ang mit der Protokollierung wurde behoben.
2024-08-19	1,26,0	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2024-07-16	1.25.2	Wartungsupdates: • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.
2024-06-17	1.25.1	Wartungsupdates: • Es wurde ein Problem mit Upgrades behoben, wenn ein Proxy verwendet wurde und DNS deaktiviert war. • Betriebssystem und Softwareelemente wurden aktualisiert, um Sicherheit und Leistung zu verbessern.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-05-15	1,25,0	Features: • Es wurde die Möglichkeit hinzugefügt, eine AES-128 AES-256 Mindestve rschlüsselung festzulegen. Dies ist nur eine Gateway-Änderung und wird in einer kommenden Version in der Storage Gateway Gateway-Konsole verfügbar sein. • Erhöhte Rotation der Systemprotokolle, wenn der Festplattenspeicher knapp wird. Bisher führte das Schreiben von Protokoll en, die die Root-Festplatte füllten, dazu, dass das Gateway gestoppt wurde. Jetzt, da der Speicherp latz abnimmt, schafft das Gateway mehr Platz für neuere Protokolle, indem ältere Protokolle gelöscht werden. • S3-Pfad in Statusmel dungen für Fehler beim Hochladen von Dateien hinzugefügt. Bisher wurde in Gesundheitsbenachr ichtigungen nur der Pfad zur Datei auf dem Gateway angezeigt. Benachric htigungen zeigen jetzt den

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		Pfad an, damit Benutzer die Datei in S3 leichter finden können. • Der Dienst ignoriert jetzt Backend-Blocker beim erzwungenen Löschen von Dateifreigaben. Bisher wurden erzwungene Löschungen ohne Angabe von Gründen gestoppt, wenn auf Blockierer gestoßen wurde. In diesen Szenarien werden erzwungene Löschungen jetzt ohne Unterbrechung fortgesetzt. Wartungsupdates: • Der NFS-Stack wurde aktualisiert. • Java 17 JRE wurde aktualisiert. • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.
2024-04-15	1,24,5	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-04-01	1,24,4	Wartungsupdates: • Fehlende NTP-Komponente (Network Time Protocol) behoben.
2024-03-18	1,24,3	Wartungsupdates: • Es wurde ein Problem im Zusammenhang mit der Leistung bei der Suche nach Groß- und Kleinschreibung behoben. • Es wurde ein Problem behoben, das zum Absturz von Prozessen führte. • Betriebssystem und Softwareelemente wurden aktualisiert, um Sicherheit und Leistung zu verbessern.
2024-01-12	1,24,2	Wartungsupdates: • Das Problem mit der SMB-Protokollierung wurde behoben.
2023-12-27	1.24.1	Wartungsupdates: • Das SMB-Stabilitätsproblem wurde behoben.

Veröffentlichungsdatum	Softwareversion	Versionshinweise

2023-12-01	1,24,0	Features:
		• SMB-Stack aktualisiert.
		  • Unterstützung für AES-256 Verschlüsselung sowie sicherere Varianten der AES-128 Verschlüsselung und Signierung hinzugefügt, wenn ein SMB 3.1.1-Client verwendet wird, der dies anfordert.
		  • Die Funktionen für serverseitiges Kopieren und serverseitige Wildcard-Erweiterung von SMBv1 (LANMAN/CIFS) wurden entfernt. (SMBv2 und SMBv3 sind nicht betroffen.) Dies kann sich negativ auf die Leistung bestimmter SMBv1-Workloads auswirken. Wenn Sie SMBv1 verwenden, sollten Sie zu SMBv2 oder SMBv3 migrieren.
		
		Wartungsupdates:
		• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2023-10-24	1.23.2	Wartungsupdates: • Es wurde ein Problem behoben, das darauf zurückzuführen war, dass der Support-Kanal für bestimmte Benutzer nicht richtig verbunden war.
2023-08-14	1,23,1	Wartungsupdates: • Der NTP-Server wurde aktualisiert, um den Synchronisierungsserver für neue Gateways zu verwenden.
2023-06-12	1,23,0	Features: • Anzahl der Upload-Threads für einige AWS Konten. Wartungsupdates: • Ein Problem mit der Zugriffsverletzung bei großen Kopien wurde behoben. • Ein NFS-Problem wurde behoben. • Java 8 wurde entfernt. • Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2023-04-19	1,22,1	Wartungsupdates: • Ein Problem im Zusammenhang mit dem Umbenennen von Ordnern und Dateien wurde behoben.
2023-01-18	1,22,0	Features: • Unterstützung für DOS-Attribute hinzugefügt. • Die Anzahl der unterstützten Dateifreigaben pro Gateway wurde von 10 auf 50 erhöht. • Es wurde ein Mechanismus zur Erkennung von Zeitversatz implementiert, um festzustellen, wann ein Gateway und ein Dienst nicht synchron sind. Wartungsupdates: • Der SMB-Stack wurde aktualisiert.
06.07.2022	1,21.2	Wartungsupdates: • Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung von Sicherheit und Leistung.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
16.02.2022	1.21.1	Features: • Neue Metriken zum Umbenennen und Löschen im Cache hinzugefügt. Wartungsupdates: • Verschiedene Probleme wurden behoben.
18.01.2022	1,21,0	Features: • Neue CloudWatch Metriken hinzugefügt. • Bandbreitendrosselung für Datenuploads hinzugefügt.
2021-12-12	1,20,0	***URGENT UPDATE***: • Die Log4j-Sicherheitslücke wurde behoben.

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.