Amazon FSx File Gateway-Benutzerhandbuch

AWS Storage Gateway

API-Version 2021-03-31

AWS Storage Gateway: Amazon FSx File Gateway-Benutzerhandbuch

Table of Contents

Amazon FSx File Gateway ist für Neukunden nicht mehr verfügbar. Bestandskunden von FSx File Gateway können den Service weiterhin normal nutzen. Informationen zu Funktionen, die FSx File Gateway ähneln, finden Sie in diesem Blogbeitrag.

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.

Was ist Amazon FSx File Gateway

Amazon FSx File Gateway (FSx File Gateway) ist ein neuer File Gateway-Typ, der geringe Latenz und effizienten Zugriff auf Dateifreigaben in der Cloud FSx für Windows File Server von Ihrer lokalen Einrichtung aus bietet. Wenn Sie aufgrund von Latenz- oder Bandbreitenanforderungen einen lokalen Dateispeicher verwenden, können Sie stattdessen FSx File Gateway für den nahtlosen Zugriff auf vollständig verwaltete, äußerst zuverlässige und praktisch unbegrenzte Windows-Dateifreigaben verwenden, die in der AWS Cloud von FSx for Windows File Server bereitgestellt werden.

Vorteile der Verwendung von Amazon FSx File Gateway

FSx File Gateway bietet die folgenden Vorteile:

- Hilft dabei, lokale Dateiserver zu eliminieren und konsolidiert all ihre Daten AWS , um die Vorteile des Skalierens und der Wirtschaftlichkeit von Cloud-Speichern zu nutzen.
- Bietet Optionen, die Sie für all Ihre Datei-Workloads verwenden können, einschließlich solcher, die einen lokalen Zugriff auf Cloud-Daten erfordern.
- Anwendungen, die lokal bleiben müssen, können jetzt dieselbe niedrige Latenz und hohe Leistung wie bei anderen aufweisen AWS, ohne Ihre Netzwerke zu belasten oder die Latenzen Ihrer anspruchsvollsten Anwendungen zu beeinträchtigen.

So funktioniert Amazon FSx File Gateway

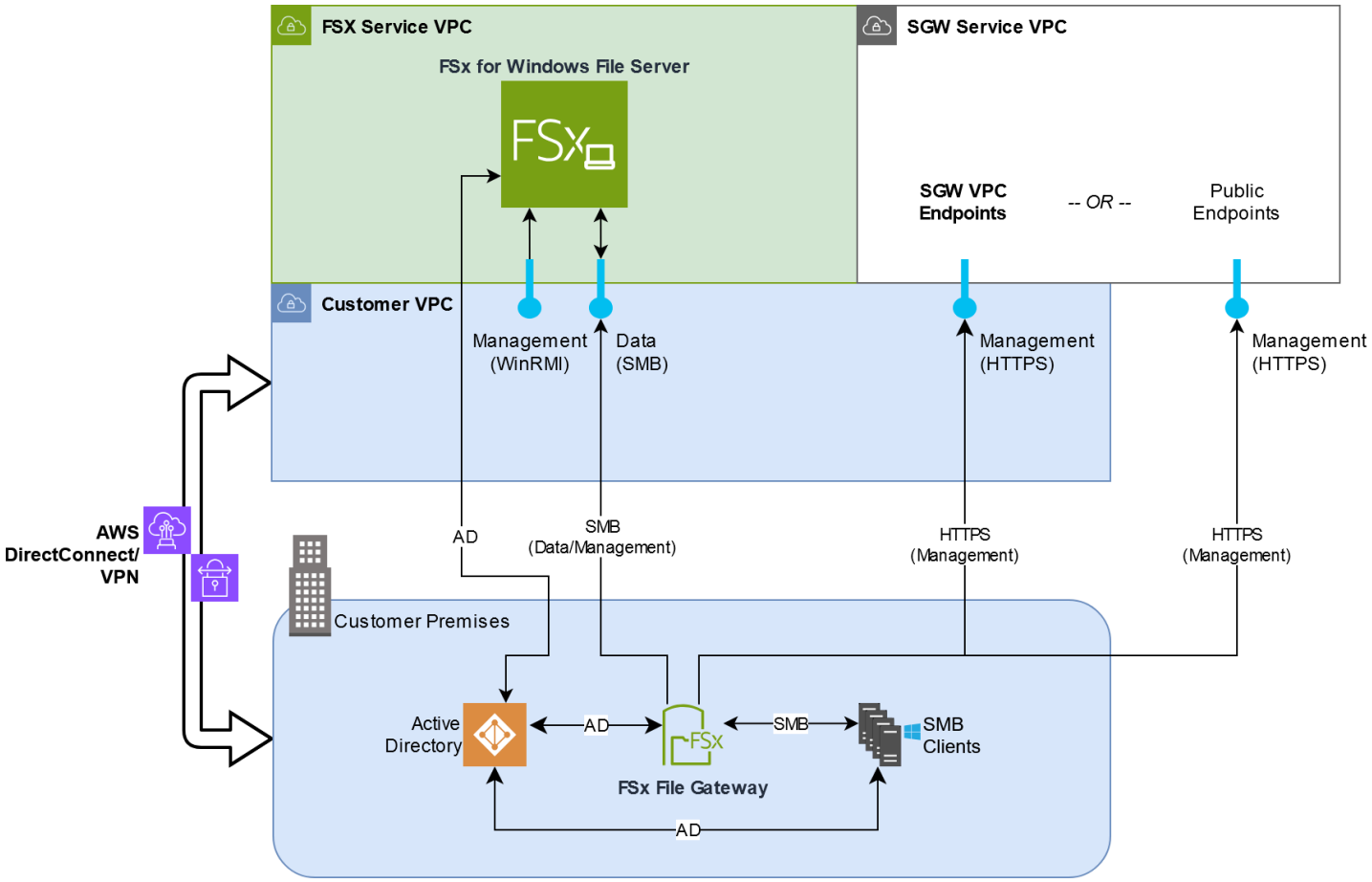
Um Amazon FSx File Gateway (FSx File Gateway) verwenden zu können, benötigen Sie mindestens ein Amazon FSx for Windows File Server-Dateisystem. Sie benötigen außerdem lokalen Zugriff auf den FSx Windows File Server, entweder über ein VPN oder über eine Direct Connect Verbindung. Weitere Informationen zur Verwendung von FSx Amazon-Dateisystemen finden Sie unter Was ist Amazon FSx for Windows File Server?

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. Nach der Bereitstellung Ihrer Appliance aktivieren Sie das FSx File Gateway über die Storage Gateway Gateway-Konsole oder über die Storage Gateway Gateway-API.

Nachdem Amazon FSx File Gateway aktiviert ist und auf Windows File Server zugreifen FSx kann, verwenden Sie die Storage Gateway Gateway-Konsole, um es mit Ihrer Microsoft Active Directory-Domain zu verbinden. Nachdem das Gateway erfolgreich einer Domäne beigetreten ist, verwenden Sie die Storage Gateway Gateway-Konsole, um das Gateway an einen vorhandenen Dateiserver FSx für Windows anzuhängen. FSx für Windows File Server stellt alle Shares auf dem Server als Shares auf Ihrem Amazon FSx File Gateway zur Verfügung. Sie können dann einen Client verwenden, um die Dateifreigaben auf FSx File Gateway zu durchsuchen und eine Verbindung zu ihnen herzustellen, die dem ausgewählten FSx File Gateway entsprechen.

Wenn die Dateifreigaben verbunden sind, können Sie Ihre Dateien lokal lesen und schreiben und gleichzeitig alle Funktionen nutzen, die FSx für Windows File Server verfügbar sind. FSx File Gateway ordnet lokale Dateifreigaben und deren Inhalt Dateifreigaben zu, die remote in FSx Windows File Server gespeichert sind. Es besteht eine 1:1 -Korrespondenz zwischen den remote und lokal sichtbaren Dateien und ihren Freigaben.

Das folgende Diagramm bietet einen Überblick über die Bereitstellung von Dateispeichern für Storage Gateway.



Beachten Sie im Diagramm Folgendes:

- Direct Connect oder ein VPN ist erforderlich, damit das FSx File Gateway über SMB auf die FSx Amazon-Dateifreigabe zugreifen kann und damit der Dateiserver FSx für Windows Ihrer lokalen Active Directory-Domäne beitreten kann.
- Amazon Virtual Private Cloud (Amazon VPC) wird benötigt, um über private Endpunkte eine Verbindung mit dem Service VPC FSx für Windows File Server und dem Storage Gateway Service VPC herzustellen. Das FSx File Gateway kann auch eine Verbindung zu den öffentlichen Endpunkten herstellen.

Sie können Amazon FSx File Gateway in allen AWS Regionen verwenden, in denen FSx Windows File Server verfügbar ist.

Erste Schritte mit AWS Storage Gateway

Dieser Abschnitt enthält Anweisungen für die ersten Schritte mit AWS. Sie benötigen ein AWS Konto, bevor Sie mit der Nutzung beginnen können AWS 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

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

Bei Amazon Web Services registrieren

An AWS-Konto ist eine grundlegende Voraussetzung für den Zugriff auf AWS Dienste. Ihr AWS-Konto ist der Basiscontainer für alle AWS Ressourcen, die Sie als AWS Benutzer erstellen. Ihre AWS-Konto ist auch die grundlegende Sicherheitsgrenze für Ihre AWS Ressourcen. Alle Ressourcen, die Sie in Ihrem Konto erstellen, stehen Benutzern zur Verfügung, die über Anmeldeinformationen für das Konto verfügen. Bevor Sie mit der Nutzung beginnen können AWS Storage Gateway, müssen Sie sich für einen registrieren AWS-Konto.

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

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

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Wir empfehlen außerdem, dass Sie von Ihren Benutzern verlangen, dass sie beim Zugriff temporäre Anmeldeinformationen verwenden AWS. Um temporäre Anmeldeinformationen bereitzustellen, können Sie den Verbund und einen Identitätsanbieter wie AWS IAM Identity Center verwenden. Wenn Ihr Unternehmen bereits einen Identitätsanbieter verwendet, können Sie ihn zusammen mit dem Verbund verwenden, um den Zugriff auf die Ressourcen in Ihrem AWS Konto zu vereinfachen.

Erstellen Sie einen IAM-Benutzer mit Administratorrechten

Nachdem Sie Ihr AWS Konto erstellt haben, gehen Sie wie folgt vor, um einen AWS Identity and Access Management (IAM-) Benutzer für sich selbst zu erstellen, und fügen Sie diesen Benutzer dann einer Gruppe hinzu, die über Administratorrechte verfügt. Weitere Informationen zur Verwendung des AWS Identity and Access Management Dienstes zur Steuerung des Zugriffs auf Storage Gateway Gateway-Ressourcen finden Sie unterIdentitäts- und Zugriffsmanagement für AWS Storage Gateway.

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
Im IAM Identity Center (Empfohlen)	Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.	Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center - Benutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff, indem Sie den AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch konfigurieren.
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Folgen Sie den Anleitungen unter IAM-Benutzer für den Notfallzugriff erstellen im IAM-Benutzerhandbuch.	Sie konfigurieren den programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch.

> **Warning**
>
> IAM-Benutzer verfügen über langfristige Anmeldeinformationen, die ein Sicherheitsrisiko darstellen. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

Zugreifen AWS Storage Gateway

Sie können die AWS Storage Gateway Konsole 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 , Anhängen, Verwalten und Trennen von 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 AWS CLI Command Reference.

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

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

AWS-Regionen die 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.

Amazon FSx File Gateway speichert Dateidaten in der AWS Region, in der sich Ihr FSx Amazon-Dateisystem befindet. Bevor Sie mit der Bereitstellung Ihres Gateways beginnen, wählen Sie in der oberen rechten Ecke der Storage Gateway Gateway-Konsole eine Region aus.

- Amazon FSx File Gateway — Unterstützte AWS Regionen und eine Liste der AWS Service-Endpunkte, die Sie mit Amazon FSx File Gateway verwenden können, finden Sie unter Amazon File Gateway-Endpunkte und Kontingente in der. FSx Allgemeine AWS-Referenz
- Storage Gateway — Unterstützte AWS Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte 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 Gateway Hardware-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 in AWS 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 FSx File Gateway (FSx File Gateway) einrichten, müssen Sie die folgenden Voraussetzungen erfüllen:

- Erstellen und konfigurieren Sie ein Dateisystem FSx für Windows File Server. Anweisungen finden Sie unter Schritt 1: Erstellen Sie Ihr Dateisystem im Amazon FSx for Windows File Server-Benutzerhandbuch.
- Konfigurieren Sie Microsoft Active Directory (AD) und erstellen Sie ein Active Directory-Dienstkonto mit den erforderlichen Berechtigungen. Weitere Informationen finden Sie unter Berechtigungsvoraussetzungen für für Active Directory-Dienstkonten.
- Stellen Sie sicher, dass zwischen dem Gateway und ausreichend Netzwerkbandbreite vorhanden ist AWS. 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 sowie zur Mindestmenge an Festplattenspeicher, die für den erforderlichen Speicher zugewiesen werden muss.

Hardwareanforderungen für lokale Umgebungen 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 zuweisen 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

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-basierte Instances, die Graviton-Prozessoren verwenden, werden nicht unterstützt.

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

Für File Gateway-Typen empfohlen

- Instance-Familie für allgemeine Zwecke — Instance-Typ m5, m6 oder m7. Wählen Sie die Xlarge-Instance-Größe oder höher, um die Prozessor- und RAM-Anforderungen von Storage Gateway zu erfüllen.
- Für die Datenverarbeitung optimierte 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.
- Speicheroptimierte 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.
- Speicheroptimierte 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.

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.

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

FSx File Gateway setzt voraus, dass 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 VPC-Endpunkten.

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

Sie können die auch verwenden Directory 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 FSx File Gateway

Netzwerkelement	Aus	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-Aktivierun

Netzwerkelement	Aus	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								gsschlüssel zu erhalten. Port 80 wird nur während der Aktivierung einer Storage-Gateway-Appliance verwendet. Für eine Storage-Gateway-VM ist es nicht erforderlich, dass Port 80 öffentlich zugänglich ist. Die erforderliche

Netzwerkelement	Aus	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie Ihr Gateway von der Storage Gateway Management Console aus aktivieren, muss der Host, von dem aus Sie eine Verbindung zur Konsole herstellen,

Netzwerkelement	Aus	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								Zugriff auf den Port 80 Ihres Gateways haben.
Webbrowser	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓	AWS Management-Konsole (alle anderen Operationen)

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

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

Netzwerkelement	Aus	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	UDP NetBIOS	137	✓	✓	✓	Benennen Sie den Dienst
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	UDP NetBIOS	138	✓	✓	✓	Datagram Service
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	TCP- und UDP-LDAP	389	✓	✓	✓	Client-Verbindung zum Directory System Agent (DSA)
Microsoft Active Directory	Storage-Gateway-VM	Active-Directory-Server	TCP- und UDP-Kerberos	88	✓	✓	✓	Kerberos

Netzwerkelement	Aus	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
FSx Amazon-Verbindung	Storage-Gateway-VM	FSx für Windows-Dateiserver	TCP oder UDP SMBv3	445	✓	✓	✓	Sitzungsdienst für die gemeinsame Nutzung von Daten

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

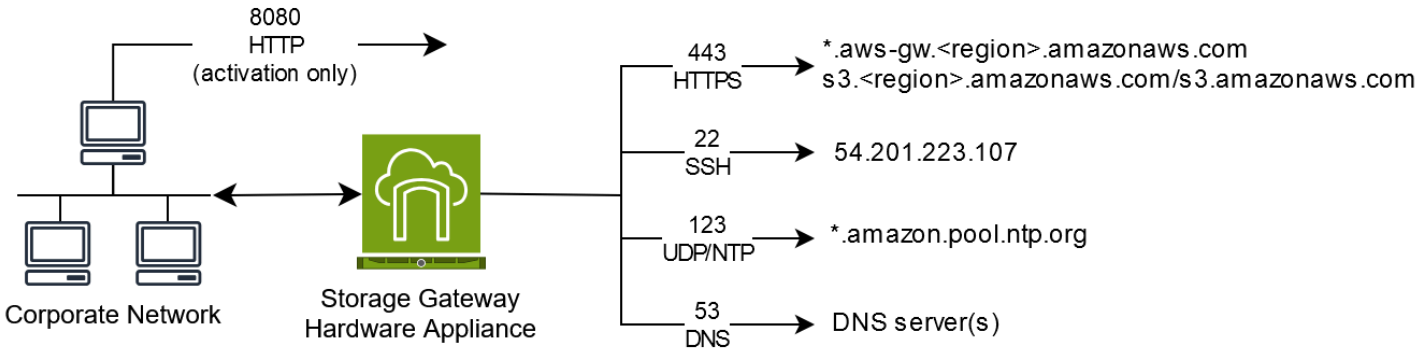
Jedes Storage-Gateway-Hardwaregerät benötigt die folgenden Netzwerkdienste:

- 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 Adresse 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

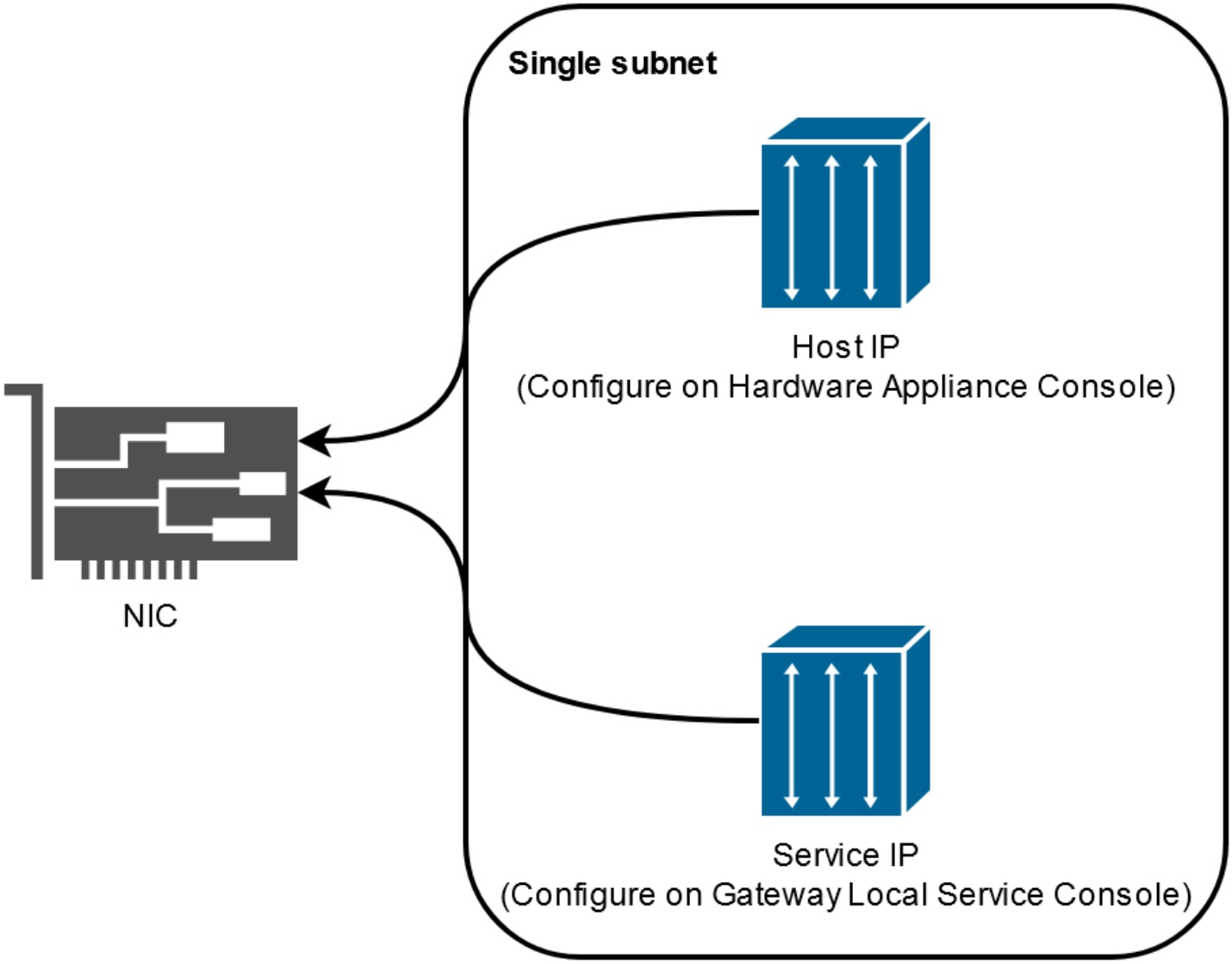
Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Usage
HTTPS	443	Ausgehend	Hardware-Appliance	`*.amazonaws.com`	Datenübertragung
HTTP	8080	Eingehend	AWS	Hardware-Appliance	Aktivierung (nur kurz)

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

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

Zulassen des AWS Storage Gateway Zugriffs 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 zur Verbindung und Datenübertragung von und zu konfigurieren AWS, 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 den 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 (`dp-1`) benötigt.

```
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
```

Zusätzlich zu den Service-Endpunkten Storage Gateway und Amazon S3 benötigt Storage 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.

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 bereitgestellt.

Storage Gateway unterstützt die folgenden Hypervisor-Versionen und Hosts:

- VMware ESXi Hypervisor (Version 7.0 oder 8.0) — Für dieses Setup benötigen Sie auch 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 kernelbasierte virtuelle Maschine (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 .xml-Datei finden Sie empfohlene Startkonfigurationen. aws-storage-gateway 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 KVM-basierte Virtualisierungsplattform, die in die Nutanix Hyper-Converged Infrastructure (HCI) -Lösung integriert ist.

- 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 FSx 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 SMB-Clients für File Gateway

File Gateway unterstützt die folgenden SMB-Clients (Service Message Block):

- Microsoft Windows Server 2008 R2 und höher
- Windows Desktop-Versionen: 10, 8 und 7.
- Windows Terminal Server, der auf Windows Server 2008 und höher ausgeführt wird

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

Unterstützte Dateisystemoperationen für File Gateway

Ihr SMB-Client kann Dateien schreiben, lesen, löschen und kürzen. Wenn Clients Schreibvorgänge an Storage Gateway senden, wird synchron in den lokalen Cache geschrieben. Dann schreibt es

FSx asynchron über optimierte Übertragungen an Amazon. Lesevorgänge werden zunächst über den lokalen Cache ausgeliefert. Wenn Daten nicht verfügbar sind, werden sie über Amazon FSx als Durchlese-Cache abgerufen.

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

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 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 bereitstellen, sollten Sie berücksichtigen, wie viel Cache-Laufwerk Sie zuweisen möchten. verwendet einen Algorithmus, der zuletzt verwendet wurde, um Daten automatisch aus dem Cache zu entfernen. Der Cache auf einem 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 der 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 eine bestimmte Arbeitslast benötigen, sollten Sie beachten, dass Sie Ihrem Gateway jederzeit eine Cache-Festplatte hinzufügen können (bis zu den aktuellen Kontingenten auf 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 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**
>
> Die zugrunde liegenden physischen Speicherressourcen werden als Datenspeicher in dargestellt VMware. 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 es sich bei dem Backup um eine weniger leistungsstarke RAID-Konfiguration handelt, z. B. RAID1

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 https://console.aws.amazon.com/storagegateway/zu Hause.
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.
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

Wir empfehlen nicht, kurzlebige Festplatten für den Cache-Speicher auf FSx File Gateways zu verwenden.

Ephemere Festplatten bieten temporären Speicher auf Blockebene für Ihre Amazon EC2 EC2-Instance. 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 für 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 verloren gehen, die noch nicht auf für Windows File Server hochgeladen wurden.

> **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.

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:

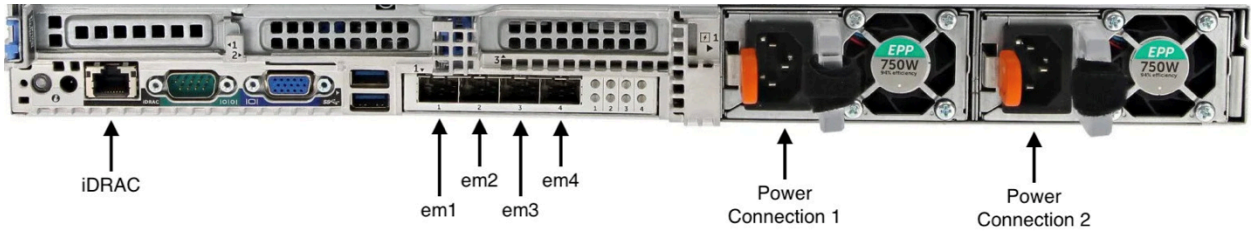
- Stromkabel: Benötigt wird ein Stromkabel. empfohlen werden zwei Stromkabel.
- Unterstützte Netzwerkverkabelung (abhängig davon, welche Netzwerkschnittstellenkarte (NIC) in der Hardware-Appliance enthalten ist). Twinax Copper DAC, optisches SFP+-Modul (Intel-kompatibel) oder SFP-Base-T-Kupfer-Transceiver.
- 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 Sie Ihr Amazon FSx File Gateway.

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 gehosteten Gateway zu beheben.

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

> **Important**
>
> Amazon FSx File Gateway ist für Neukunden nicht mehr verfügbar. Bestandskunden von FSx File Gateway können den Service weiterhin normal nutzen. Informationen zu Funktionen, die FSx File Gateway ähneln, finden Sie in diesem Blogbeitrag.

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 Sie ein Dateisystem FSx für Amazon für Windows File Server

Um ein Amazon FSx File Gateway in zu erstellen AWS Storage Gateway, müssen Sie zunächst ein Amazon FSx for Windows File Server-Dateisystem erstellen. Wenn Sie bereits ein FSx Amazon-Dateisystem erstellt haben, fahren Sie mit dem nächsten Schritt fortErstellen und aktivieren Sie ein Amazon FSx File Gateway.

> **Note**
>
> Beim Schreiben von einem File Gateway in ein FSx Amazon-Dateisystem gelten die folgenden Einschränkungen: FSx
>
> - Ihr FSx Amazon-Dateisystem und Ihr FSx File Gateway müssen demselben AWS Konto gehören und sich in derselben AWS Region befinden.
> - Jedes Gateway kann fünf angehängte Dateisysteme unterstützen. Wenn Sie ein Dateisystem anhängen, benachrichtigt Sie die Storage Gateway Gateway-Konsole, wenn das ausgewählte Gateway ausgelastet ist. In diesem Fall müssen Sie ein anderes Gateway wählen oder ein Dateisystem trennen, bevor Sie ein anderes anhängen können.
> - FSx File Gateway unterstützt weiche Speicherkontingente (es werden Warnungen ausgegeben, wenn Benutzer ihre Datenlimits überschreiten), unterstützt jedoch keine festen Kontingente (Durchsetzung von Datenlimits durch Verweigerung des Schreibzugriffs). Soft-Quotas werden für alle Benutzer außer dem FSx Amazon-Admin-Benutzer unterstützt. Weitere Informationen zur Einrichtung von Speicherkontingenten finden Sie unter Speicherkontingente im Amazon FSx for Windows File Server-Benutzerhandbuch.
> - Wir empfehlen nicht, Microsoft Distributed File System (DFS) zu verwenden, um Benutzer über FSx File Gateway zu Ihrem FSx Amazon-Dateisystem weiterzuleiten. Konfigurieren Sie DFS stattdessen so, dass es direkt zum FSx Amazon-Dateisystem umleitet, AWS Cloud wie unter Gruppieren mehrerer Dateisysteme mit DFS-Namespaces im Amazon FSx for Windows File Server-Benutzerhandbuch beschrieben.
> - Einige Dateioperationen auf dem FSx File Gateway, wie z. B. das Umbenennen von Ordnern auf oberster Ebene oder Änderungen von Berechtigungen, können zu mehreren Dateivorgängen führen, die zu einer hohen I/O Belastung Ihres Dateisystems für Windows File Server führen. FSx Wenn Ihr Dateisystem nicht über genügend Leistungsressourcen für Ihre Arbeitslast verfügt, löscht das Dateisystem möglicherweise Schattenkopien, da

es der kontinuierlichen I/O Verfügbarkeit Vorrang vor der Aufbewahrung historischer Schattenkopien einräumt.

Überprüfen Sie in der FSx Amazon-Konsole auf der Seite Überwachung und Leistung, ob Ihr Dateisystem nicht ausreichend bereitgestellt ist. Ist dies der Fall, können Sie zu SSD-Speicher wechseln, die Durchsatzkapazität erhöhen oder die SSD-IOPS erhöhen, um Ihre Arbeitslast zu bewältigen.

Um ein Dateisystem FSx für Windows File Server zu erstellen

1. Öffnen Sie AWS-Managementkonsole at https://console.aws.amazon.com/fsx/home/ und wählen Sie die Region aus, in der Sie Ihr Gateway erstellen möchten.
2. Folgen Sie den Anweisungen unter Erste Schritte mit Amazon FSx im Amazon FSx for Windows File Server-Benutzerhandbuch.

Erstellen und aktivieren Sie ein Amazon FSx File Gateway

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

Themen

- Richten Sie ein Amazon FSx File Gateway ein
- Connect Sie Ihr Amazon FSx File Gateway mit AWS
- Überprüfen Sie die Einstellungen und aktivieren Sie Ihr Amazon FSx File Gateway
- Konfigurieren Sie Ihr Amazon FSx File Gateway

Richten Sie ein Amazon FSx File Gateway ein

Um ein neues FSx 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 FSx 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.
- 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 für Einrichten des Gateways bestätigen das entsprechende 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. Jetzt, da Ihr Gateway eingerichtet ist, müssen Sie auswählen, wie es eine Verbindung herstellen und mit der es kommunizieren soll AWS. Wählen Sie Weiter aus, um fortzufahren.

Connect Sie Ihr Amazon FSx File Gateway mit AWS

Um ein neues FSx File Gateway zu verbinden AWS

1. Falls Sie dies noch nicht getan haben, führen Sie das unter Amazon FSx 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 Endpunktoptionen für Service-Endpunkt den Endpunkttyp aus, mit dem Ihr Gateway kommunizieren soll 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-kompatiblen 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.
3. 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.

- 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.

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 FSx File Gateway

Um ein neues FSx File Gateway zu aktivieren

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

   - Richten Sie ein Amazon FSx File Gateway ein
   - Connect Sie Ihr Amazon FSx 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 Sie Ihr Amazon FSx File Gateway

Um die Erstkonfiguration auf einem neuen FSx File Gateway durchzuführen

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

   - Richten Sie ein Amazon FSx File Gateway ein
   - Connect Sie Ihr Amazon FSx File Gateway mit AWS
   - Überprüfen Sie die Einstellungen und aktivieren Sie Ihr Amazon FSx 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, um über die Messwerte Ihres Gateways informiert zu werden. 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 — Verwenden Sie keine CloudWatch Alarme, um über die Messwerte Ihres Gateways informiert zu werden.

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 ein Dateisystem anhängen, damit es verwendet werden kann. Anweisungen finden Sie unter Anhängen eines Dateisystems von Amazon FSx für Windows.

Wenn Sie kein vorhandenes FSx Amazon-Dateisystem zum Anhängen haben, müssen Sie eines erstellen. Anweisungen finden Sie unter Erste Schritte mit Amazon FSx.

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 zu erstellen und die VPC-Endpunkt-ID abzurufen. Geben Sie dann diese VPC-Endpunkt-ID an, wenn Sie das Gateway erstellen und aktivieren. Weitere Informationen finden Sie unter Ihr Amazon FSx File Gateway mit zu AWS Connect AWS.

Um Ihr FSx File Gateway für die Übertragung von Daten über die VPC zu konfigurieren, müssen Sie ein VPN oder eine AWS DirectConnect Verbindung zwischen der Amazon FSx for Windows File Server-VPC und dem Netzwerk einrichten, in dem Ihr Gateway bereitgestellt wird.

> **Note**
>
> Sie müssen Ihr Gateway in derselben Region aktivieren, in der Sie den VPC-Endpunkt für Storage Gateway 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 erstellen und aktivieren Amazon FSx File Gateway erstellen und aktivieren.

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

Konfigurieren Sie die Einstellungen für den Microsoft Active Directory-Domänenzugriff

In diesem Schritt konfigurieren Sie die Zugriffseinstellungen, um Ihr Amazon FSx File Gateway mit einer Microsoft Active Directory-Domain zu verbinden.

Um die Active Directory-Einstellungen zu konfigurieren

1. Wählen Sie in der Storage Gateway Gateway-Konsole im Navigationsmenü FSx Dateisysteme aus.
2. Wählen Sie FSx Dateisystem anhängen.
3. Wählen Sie auf der Seite „Gateway bestätigen“ aus dem Dropdownmenü das Gateway aus, das Sie Ihrer Active Directory-Domäne hinzufügen möchten.

   Wenn Sie kein Gateway haben, müssen Sie eines erstellen. Stellen Sie sicher, dass Ihr Gateway den Namen Ihres Active Directory-Domänencontrollers auflösen kann. Weitere Informationen finden Sie unter Voraussetzungen.
4. Geben Sie Werte für die Active Directory-Einstellungen ein:

   > **Note**
   >
   > Wenn Ihr Gateway bereits mit einer Domäne verbunden ist, müssen Sie nicht erneut beitreten. Fahren Sie mit dem nächsten Schritt fort.

   - Geben Sie unter Domänenname den Domänennamen des Active Directory ein, das Sie verwenden möchten.
   - Geben Sie unter Domänenbenutzer den Benutzernamen des Active Directory-Benutzers ein, den Sie verwenden möchten, um das Gateway mit der Domäne zu verbinden. Dieser Benutzer muss über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter Berechtigungsanforderungen für für Active Directory-Dienstkonten.
   - Geben Sie unter Domänenkennwort das Kennwort für den Benutzer ein.
   - Unter Organisationseinheit — optional können Sie eine Organisationseinheit angeben, zu der das Active Directory gehört.

> **Note**
>
> Wenn Sie dieses Feld leer lassen, wird beim Beitritt zu einer Domäne 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.

- Geben Sie einen Wert für Domänencontroller ein — optional.

5. Wählen Sie Weiter, um die Seite „ FSx Dateisystem anhängen“ zu öffnen.

Nächster Schritt

Hängen Sie ein Amazon FSx for Windows File Server-Dateisystem an

Hängen Sie ein Amazon FSx for Windows File Server-Dateisystem an

Sie müssen über ein Dateisystem FSx für Windows File Server verfügen, bevor Sie es an ein FSx File Gateway anhängen können. Wenn Sie kein Dateisystem haben, müssen Sie eines erstellen. Anweisungen finden Sie unter Schritt 1: Erstellen Sie Ihr Dateisystem im Amazon FSx for Windows File Server-Benutzerhandbuch.

Der nächste Schritt besteht darin, ein FSx Amazon-Dateisystem an das Gateway anzuhängen. Wenn Sie ein FSx Amazon-Dateisystem anhängen, werden alle Dateifreigaben auf dem Dateisystem Amazon File Gateway (FSx FSx File Gateway) zur Verfügung gestellt, sodass Sie es mounten können.

> **Note**
>
> Beim Schreiben von Amazon File Gateway in ein FSx Amazon-Dateisystem gelten die folgenden Einschränkungen: FSx
>
> - Ihr FSx Amazon-Dateisystem und Ihr FSx File Gateway müssen demselben gehören AWS-Konto und sich in demselben befinden AWS-Region.
> - Jedes Gateway kann bis zu fünf angehängte Dateisysteme unterstützen. Wenn Sie ein Dateisystem anhängen, benachrichtigt Sie die Storage Gateway Gateway-Konsole, wenn das ausgewählte Gateway ausgelastet ist. In diesem Fall müssen Sie ein anderes Gateway wählen oder ein Dateisystem trennen, bevor Sie ein anderes anhängen können.
> - FSx File Gateway unterstützt weiche Speicherkontingente (die Sie warnen, wenn Benutzer ihre Datenlimits überschreiten), unterstützt jedoch keine festen Kontingente (die Datenlimits durchsetzen, indem sie den Schreibzugriff verweigern). Soft-Quotas werden für alle Benutzer außer dem FSx Amazon-Admin-Benutzer unterstützt. Weitere Informationen zur Einrichtung von Speicherkontingenten finden Sie unter Speicherkontingente im FSx Amazon-Benutzerhandbuch.
> - Wir empfehlen nicht, Microsoft Distributed File System (DFS) zu verwenden, um Benutzer über FSx File Gateway zu Ihrem FSx Amazon-Dateisystem weiterzuleiten. Konfigurieren Sie DFS stattdessen so, dass es direkt zum FSx Amazon-Dateisystem umleitet, AWS Cloud wie unter Gruppieren mehrerer Dateisysteme mit DFS-Namespaces im Amazon FSx for Windows File Server-Benutzerhandbuch beschrieben.

Um ein FSx Amazon-Dateisystem anzuhängen

1. Füllen Sie in der Storage Gateway Gateway-Konsole auf der Seite FSx FSx Dateisysteme > Dateisystem anhängen die folgenden Felder im Abschnitt FSx Dateisystemeinstellungen aus:

   - Wählen Sie als FSx Dateisystemname das Dateisystem, das Sie anhängen möchten, aus der Dropdownliste aus.
   - Geben Sie für Local Endpoint IP address die Gateway-IP-Adresse ein, die Clients zum Durchsuchen von Dateifreigaben im FSx Dateisystem verwenden werden.

   > **Note**
   >
   > - Sie müssen für jedes Dateisystem, das an das Gateway angeschlossen ist, eine IP-Adresse angeben.
   > - Für EC2 Amazon-Gateways können Sie die private IP-Adresse der EC2 Instance angeben, es sei denn, sie wird bereits von einem anderen Dateisystem verwendet. In diesem Fall müssen Sie dem Gateway eine neue private Adresse hinzufügen und es dann neu starten. Weitere Informationen finden Sie unter Mehrere IP-Adressen im EC2 Amazon-Benutzerhandbuch.
   > - Für lokale Gateways können Sie die IP-Adresse der primären Netzwerkschnittstelle (statisch oder DHCP) angeben, sofern sie nicht bereits von einem anderen Dateisystem verwendet wird. In diesem Fall müssen Sie eine andere IP-Adresse aus demselben Subnetz wie die primäre Schnittstelle angeben, die als virtuelle IP zur Verfügung gestellt wird. Verwenden Sie keine IP-Adresse, die einer anderen Netzwerkschnittstelle als der primären zugewiesen ist.

2. Geben Sie im Abschnitt Einstellungen für das Servicekonto die Anmeldeinformationen für das Servicekonto ein, die mit dem FSx Amazon-Dateisystem verknüpft sind.

   > **Note**
   >
   > Dieses Dienstkonto muss über Backup Operator-Rechte des Active Directory-Dienstes verfügen, der mit Ihren FSx Amazon-Dateisystemen verknüpft ist, oder über gleichwertige Berechtigungen verfügen.

> **Important**
>
> Um ausreichende Berechtigungen für Dateien, Ordner und Dateimetadaten sicherzustellen, empfehlen wir, dass Sie das Servicekonto zu einem Mitglied der Gruppe der Dateisystemadministratoren machen.
> Wenn Sie AWS Directory Service für Microsoft Active Directory mit Amazon FSx for Windows File Server verwenden, muss das Dienstkonto Mitglied der Gruppe AWS Delegated FSx Administrators sein.
> Wenn Sie ein selbstverwaltetes Active Directory mit Amazon FSx for Windows File Server verwenden, empfehlen wir, dass das Servicekonto Mitglied der benutzerdefinierten Gruppe delegierter Dateisystemadministratoren ist, die Sie bei der Erstellung Ihres Amazon-Dateisystems für die FSx Dateisystemadministration angegeben haben.
> Wenn Sie sich bei der Erstellung des Amazon-Dateisystems dafür entschieden haben, keine benutzerdefinierte Gruppe delegierter FSx Dateisystemadministratoren zu erstellen, ist die Standardgruppe Domain-Admins. Sie können das Servicekonto zwar stattdessen zu einem Mitglied dieser Gruppe machen, dies wird jedoch nicht als bewährte Methode empfohlen.
> Weitere Informationen finden Sie unter Delegieren von Rechten an Ihr FSx Amazon-Servicekonto im Amazon FSx for Windows File Server-Benutzerhandbuch.

3. Wählen Sie im Abschnitt Audit-Logs die Option Existierende Protokollgruppen und wählen Sie das Protokoll aus, das Sie zur Überwachung des Zugriffs auf Ihr FSx Amazon-Dateisystem verwenden möchten. Sie können ein neues erstellen. Wenn Sie Ihr System nicht überwachen möchten, wählen Sie Protokollierung deaktivieren.
4. Wenn Sie möchten, dass Ihr Cache automatisch aktualisiert wird, wählen Sie für die Einstellung Automatische Cacheaktualisierung die Option Aktualisierungsintervall festlegen und geben Sie ein Intervall zwischen 5 Minuten und 30 Tagen an.
5. (Optional) Wählen Sie im Abschnitt „Tags“ die Option Neues Tag hinzufügen aus, um einen oder mehrere Schlüssel und einen Wert für die Kennzeichnung Ihrer Einstellungen hinzuzufügen.
6. Wählen Sie Weiter aus und überprüfen Sie die Einstellungen. Um Ihre Einstellungen zu ändern, können Sie in jedem Abschnitt „Bearbeiten“ wählen.
7. Wenn Sie fertig sind, wählen Sie Finish aus.

Nächster Schritt

Mounten und verwenden Sie Ihre FSx Amazon-Dateifreigabe

Mounten und verwenden Sie Ihre FSx Amazon-Dateifreigabe

Warten Sie, bis sich der Status des Amazon-Dateisystems auf Verfügbar ändert, bevor Sie Ihre FSx Dateifreigabe auf dem Client bereitstellen. Nachdem Ihre Dateifreigabe bereitgestellt wurde, können Sie Ihr Amazon FSx File Gateway (FSx File Gateway) verwenden.

Themen

Mounten Sie Ihre SMB-Dateifreigabe auf Ihrem Client

In diesem Schritt mounten Sie Ihre SMB-Dateifreigabe und ordnen sie einem Laufwerk zu, 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:

- Der `net use` Befehl — bleibt bei Systemneustarts nicht bestehen, es sei denn, Sie verwenden den `/persistent:(yes:no)` Switch.
- Das `CmdKey` Befehlszeilenprogramm — Stellt eine dauerhafte Verbindung zu einer bereitgestellten SMB-Dateifreigabe her, die auch nach einem Neustart bestehen bleibt.
- Ein im Datei-Explorer zugeordnetes Netzlaufwerk — Konfiguriert die bereitgestellte Dateifreigabe so, dass sie bei der Anmeldung erneut eine Verbindung herstellt und dass Sie Ihre Netzwerkanmeldedaten eingeben müssen.
- PowerShell Skript — Kann persistent sein und während der Installation entweder sichtbar oder unsichtbar für das Betriebssystem sein.

> **Note**
>
> Wenn Sie ein Microsoft Active Directory-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 bereitstellen.

Amazon FSx File Gateway unterstützt weder SMB-Sperren noch erweiterte SMB-Attribute.

Um eine SMB-Dateifreigabe für Active Directory-Benutzer mit dem Befehl net use bereitzustellen

1. Stellen Sie sicher, dass Sie Zugriff auf die SMB-Dateifreigabe haben, bevor Sie die Dateifreigabe auf Ihrem lokalen System mounten.
2. Geben Sie für Microsoft Active Directory-Clients an der Eingabeaufforderung den folgenden Befehl ein:

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

Um eine SMB-Dateifreigabe unter Windows zu mounten, verwenden Sie CmdKey

1. Drücken Sie die Windows-Taste und dann die Eingabetaste**cmd**, um das Menüelement der Befehlszeile anzuzeigen.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für die Befehlszeile und wählen Sie Als Administrator ausführen.
3. Geben Sie den folgenden Befehl ein:

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

> **Note**
>
> Beim Mounten von Dateifreigaben müssen Sie Ihre Dateifreigabe möglicherweise nach dem Neustart Ihres Clients 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 Windows suchen die Eingabe 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 Netzlaufwerk zuordnen einen Laufwerksbuchstaben für Laufwerk aus.

4. Geben Sie für Ordner den ***[File Gateway IP]**[SMB File Share Name]*** Suchbegriff ein, oder wählen Sie Durchsuchen, um Ihre SMB-Dateifreigabe aus dem 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 Verbinden mit anderen Anmeldeinformationen,, wenn Sie möchten, dass ein Benutzer die Active Directory-Anmeldung oder das Gastkonto-Benutzerpasswort eingibt.
7. Klicken Sie auf Finish (Beenden), um den Mounting-Punkt fertigzustellen.

Testen Sie Ihr FSx File Gateway

Sie können Dateien und Verzeichnisse auf Ihr zugeordnetes Laufwerk kopieren. Die Dateien werden automatisch in Ihr Dateisystem FSx für Windows File Server hochgeladen.

Um Dateien von Ihrem Windows-Client zu Amazon hochzuladen FSx

1. Navigieren Sie auf Ihrem Windows-Client zu dem Laufwerk, auf dem Sie Ihr Dateisystem bereitgestellt haben. Dem Namen des Laufwerks wird der Name Ihres Dateisystems vorangestellt.
2. Kopieren Sie Dateien oder ein Verzeichnis auf das Laufwerk.

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

Verwaltung Ihrer Amazon FSx File Gateway-Ressourcen

Die folgenden Abschnitte enthalten Informationen zur Verwaltung Ihrer Amazon FSx File Gateway (FSx File Gateway) -Ressourcen, einschließlich des Anhängen und Trennen von FSx Amazon-Dateisystemen und der Konfiguration von Microsoft Active Directory-Einstellungen.

Themen

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 weist der Status darauf hin, 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.

Status	Bedeutung
`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.

Grundlegendes zum Dateisystemstatus

Sie können den Zustand eines Dateisystems auf einen Blick überprüfen, indem Sie sich seinen Status ansehen. Wenn der Status anzeigt, dass das Dateisystem normal funktioniert, sind keine Maßnahmen Ihrerseits erforderlich. Wenn der Status anzeigt, dass ein Problem vorliegt, können Sie untersuchen, ob möglicherweise Maßnahmen erforderlich sind.

Sie können den Status eines Dateisystems auf der Storage Gateway Gateway-Konsole in der Spalte Status anzeigen. Ein Dateisystem, das 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	Das Dateisystem ist ordnungsgemäß konfiguriert und kann verwendet werden. Dies ist der Standardstatus für ein Dateisystem, das ordnungsg emäß funktioniert.
WIRD ERSTELLT	Das Dateisystem ist noch nicht vollständig erstellt und kann nicht verwendet werden. Der Status CREATING ist vorübergehend. Es ist keine Aktion erforderlich. Wenn das Dateisystem in diesem Status hängen bleibt, liegt das wahrscheinlich daran, dass die Gateway-VM die Verbindung zu verloren hat AWS.

Status	Bedeutung
WIRD AKTUALISIERT	Die Dateisystemkonfiguration wird gerade aktualisiert. Der Aktualisierungsstatus ist vorübergehend. Es ist keine Aktion erforderlich. Wenn ein Dateisystem in diesem Status hängen bleibt, liegt das wahrscheinlich daran, dass die Gateway-VM die Verbindung zu verloren hat AWS.
WIRD GELÖSCHT	Das Dateisystem wird gelöscht. Das Dateisystem wird erst gelöscht, wenn alle Daten hochgeladen wurden AWS. Der Status DELETING ist vorübergehend, und es ist keine Aktion erforderlich.
FORCE_DELETING	Das Dateisystem wird gewaltsam gelöscht. Das Dateisystem wird sofort gelöscht und es werden keine Daten hochgeladen. AWS Der Status FORCE DELETING ist vorübergehend, und es ist keine Aktion erforderlich.
ERROR	Das Dateisystem befindet sich in einem fehlerhaften Zustand. Es ist eine Aktion erforderlich. Zu den möglichen Ursachen gehören Probleme mit den Zugangsdaten oder -berechtigungen, Verbindungsprobleme oder unzureichender Speicherplatz im Dateisystem. Wenn das Problem, das den fehlerhaften Zustand verursacht hat, behoben ist, kehrt das Dateisystem in den Status AVAILABLE zurück.

Bearbeiten Sie grundlegende Informationen für ein FSx 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.

Legen Sie eine Sicherheitsstufe für Ihr Gateway fest

Sie können die SMB-Sicherheitsstufe für Ihr FSx File Gateway konfigurieren, um anzugeben, ob für das Gateway SMB-Signierung (Server Message Block) oder SMB-Verschlüsselung erforderlich sein soll.

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 Sicherheitsstufe kann die Leistung des Gateways beeinträchtigen.

- Obligatorische Verschlüsselung — Wenn Sie diese Option wählen, lässt FSx 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 vertrauliche Daten verarbeitet werden. Es funktioniert mit SMB-Clients unter Microsoft Windows 8, Windows Server 2012 oder höher.
- Verschlüsselung erzwingen — Wenn Sie diese Option wählen, lässt FSx File Gateway nur Verbindungen von SMBv3 Clients zu, 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 SMB-Clients unter Microsoft Windows 8, Windows Server 2012 oder höher.
- Signierung erzwingen — Wenn Sie diese Option wählen, lässt FSx File Gateway nur Verbindungen von SMBv2 oder SMBv3 Clients zu, bei denen die Signatur aktiviert ist. Diese Option funktioniert mit SMB-Clients unter Microsoft Windows Vista, Windows Server 2008 oder höher.

> **Note**
>
> Die Standardsicherheitsstufe für FSx File Gateway ist Encryption erzwingen.

5. Wählen Sie Speichern.

Active Directory-Einstellungen für ein FSx File Gateway bearbeiten

Um Ihr Microsoft Active Directory Ihres Unternehmens oder AWS Managed Microsoft AD für den benutzerauthentifizierten Zugriff auf Ihr FSx Amazon-Dateisystem zu verwenden, bearbeiten Sie die SMB-Einstellungen für Ihr Gateway und geben Sie Ihre Active Directory-Domänenanmeldedaten ein. Dadurch kann Ihr Gateway Ihrer Active Directory-Domain beitreten und Mitglieder der Domain können auf das Dateisystem zugreifen.

> **Note**
>
> Mithilfe Directory Service können Sie einen gehosteten Active Directory-Domänendienst in der erstellen AWS Cloud.
> Um sie AWS Managed Microsoft AD mit einem Amazon EC2 EC2-Gateway zu verwenden, 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.

Um die Active Directory-Authentifizierung zu aktivieren

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 für Active Directory-Dienstkonten.
> 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.

Einstellungen für ein FSx Amazon-Dateisystem bearbeiten

Nachdem Sie ein Dateisystem FSx für Amazon for Windows File Server erstellt haben, können Sie die Einstellungen für CloudWatch Protokolle, automatische Cache-Aktualisierung und Anmeldedaten für das FSx Amazon-Servicekonto bearbeiten.

Um die FSx Amazon-Dateisystemeinstellungen zu bearbeiten

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Dateisystem und dann das Dateisystem aus, dessen Einstellungen Sie bearbeiten möchten.
3. Wählen Sie unter Aktionen die Option Dateisystemeinstellungen bearbeiten aus.
4. Überprüfen Sie im Bereich Dateisystemeinstellungen das Gateway, den FSx Amazon-Standort und die IP-Adresse.

   > **Note**
   >
   > Sie können die IP-Adresse eines Dateisystems nicht bearbeiten, nachdem es an ein Gateway angehängt wurde. Um die IP-Adresse zu ändern, müssen Sie das Dateisystem trennen und erneut anhängen.

5. Wählen Sie im Abschnitt Audit-Logs eine Option zur Verwendung von CloudWatch Protokollgruppen zur Überwachung des Zugriffs auf FSx Amazon-Dateisysteme. Sie können eine bestehende Protokollgruppe verwenden.
6. Wählen Sie für die Einstellungen für die automatische Cacheaktualisierung eine Option aus. Wenn Sie „Aktualisierungsintervall festlegen“ wählen, legen Sie die Zeit in Tagen, Stunden und Minuten fest, zu der der Cache des Dateisystems mithilfe von Time To Live (TTL) aktualisiert werden soll.

   TTL ist die Zeitspanne seit der letzten Aktualisierung. Wenn nach dieser Zeit auf das Verzeichnis zugegriffen wird, aktualisiert File Gateway den Inhalt dieses Verzeichnisses aus dem FSx Amazon-Dateisystem.

   > **Note**
   >
   > Gültige Werte für das Aktualisierungsintervall liegen zwischen 5 Minuten und 30 Tagen.

7. Geben Sie im Abschnitt Dienstkontoeinstellungen — optional einen Benutzernamen und ein Passwort ein. Diese Anmeldeinformationen gelten für einen Benutzer, der die Rolle Backup-Administrator des Active Directory-Dienstes hat, der mit Ihren FSx Amazon-Dateisystemen verknüpft ist.

8. Wählen Sie Änderungen speichern aus.

Trennen eines FSx Amazon-Dateisystems

Durch das Trennen eines Dateisystems werden Ihre Daten in FSx Windows File Server nicht gelöscht. Daten, die vor dem Trennen in diese Dateisysteme geschrieben wurden, werden trotzdem auf Ihren FSx Windows-Dateiserver hochgeladen.

Um ein FSx Amazon-Dateisystem zu trennen

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie FSx Dateisysteme und anschließend ein oder mehrere Dateisysteme aus, die getrennt werden sollen.
3. Wählen Sie unter Aktionen die Option Dateisystem trennen aus. Das Bestätigungsdialogfeld wird angezeigt.
4. Vergewissern Sie sich, dass Sie die angegebenen Dateisysteme trennen möchten, geben Sie dann das Wort Trennen in das Bestätigungsfeld ein und wählen Sie Trennen aus.

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 File Gateway- 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 verwendet werden, finden Sie unter und Grundlegendes zu Dateifreigabe-Metriken zu Dateisystemmetriken. 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
- Dateisystemfehler: `FileSystem-ERROR` >= 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 konfigurieren Ihr Amazon FSx 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 File Gateway

Sie können Ihr 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 File Gateway-Integritätsprotokollen mit CloudWatch Protokollgruppen

Sie können Amazon CloudWatch Logs verwenden, um Informationen über den Zustand Ihres 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 FSx File Gateway keine Dateien in ein FSx Amazon-Dateisystem hochladen kann. Sie können die Gruppe entweder bei der Aktivierung des Gateways oder nachdem Ihr Gateway aktiviert und betriebsbereit ist, konfigurieren. Weitere Informationen zum Konfigurieren einer CloudWatch -Protokollgruppe während der Aktivierung eines Gateways finden Sie unter Konfigurieren Sie Ihr Amazon FSx File Gateway. Allgemeine

Informationen zu CloudWatch Protokollgruppen finden Sie unter Working with Log Groups and Log Streams im CloudWatch Amazon-Benutzerhandbuch.

Informationen zur Behebung von Fehlern, die möglicherweise von 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 File Gateway

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 File Gateway 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 , 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

Grundlagen zu Gateway-Metriken

In der folgenden Tabelle werden Metriken beschrieben, die FSx File Gateways abdecken. Jedem Gateway ist eine Reihe von Metriken zugeordnet. Einige Gateway-spezifische Metriken haben denselben Namen wie bestimmte Metriken. file-system-specific Diese Metriken stellen dieselben Arten von Messungen dar, beziehen sich jedoch eher auf das Gateway als auf das Dateisystem.

Geben Sie immer an, ob Sie mit einem Gateway oder einem Dateisystem 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 abrufen können.

Metrik	Description
`AvailabilityNotifications`	Diese Metrik gibt die Anzahl der verfügbar keitsbezogenen Integritätsbenachrichtigung en an, die im Berichtszeitraum vom Gateway generiert wurden. Einheiten: Anzahl

Metrik	Description
`CacheDirectorySize`	Diese Metrik verfolgt die Größe der Ordner im Gateway-Cache. Die Ordnergröße wird durch die Anzahl der Dateien und Unterordner in der ersten Ebene bestimmt. Dabei werden Unterordner nicht rekursiv gezählt. Verwenden Sie diese Metrik zusammen mit der `Average` Statistik, um die durchschn ittliche Größe eines Ordners im Gateway-Cache zu messen. Verwenden Sie diese Metrik zusammen mit der `Max` Statistik, um die maximale Größe eines Ordners im Gateway-C ache zu messen. 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

Metrik	Description
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
CachePercentDirty	Der Gesamtprozentsatz des Gateway-C ache, auf den keine Persistenz angewendet wurde. AWS Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheiten: Prozent
CachePercentUsed	Der Gesamtprozentsatz des verwendeten Gateway-Cache-Speichers. 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

Metrik	Description
`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
`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

Metrik	Description
FileShares	Diese Metrik gibt die Anzahl der Dateifreigaben auf dem Gateway an. Einheiten: Anzahl
FileSystem-ERROR	Diese Metrik gibt die Anzahl der Dateisyst emzuordnungen auf diesen Gateways an, die sich im Fehlerstatus befinden. Wenn diese Metrik meldet, dass sich Dateisyst emzuordnungen im Status ERROR befinden, 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
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

Metrik	Description
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
MemUsedBytes	Diese Metrik gibt die Menge des verwendeten Speichers auf dem Gateway an. Einheiten: Byte
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

Metrik	Description
SmbV2Sessions	Diese Metrik gibt die Anzahl der SMBv2 Sitzungen an, die auf dem Gateway aktiv sind. Diese Metrik wird einmal für jedes dem Gateway zugeordnete Dateisystem ausgegeben. Verwenden Sie die SUM-Statistik, um die Gesamtzahl der aktiven SMBv2 Sitzungen in allen Dateisystemen zu berechnen. Einheiten: Anzahl
SmbV3Sessions	Diese Metrik gibt die Anzahl der SMBv3 Sitzungen an, die auf dem Gateway aktiv sind. Diese Metrik wird einmal für jedes dem Gateway zugeordnete Dateisystem ausgegeben. Verwenden Sie die SUM-Statistik, um die Gesamtzahl der aktiven SMBv3 Sitzungen in allen Dateisystemen zu berechnen. 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

Informationen zu Dateisystem-Metriken

Im Folgenden finden Sie Informationen zu den Storage Gateway Gateway-Metriken, die Dateisysteme abdecken. Jedem Dateisystem ist eine Reihe von Metriken zugeordnet. Einige dateisystemspezifische Metriken haben denselben Namen wie bestimmte Gateway-spezifische

Metriken. Diese Metriken stellen dieselben Arten von Messungen dar, beziehen sich jedoch stattdessen auf das Dateisystem.

Geben Sie immer an, ob Sie entweder mit einer Gateway- oder einer Dateisystem-Metrik arbeiten möchten, bevor Sie mit einer Metrik arbeiten. Insbesondere bei der Arbeit mit Dateisystem-Metriken müssen Sie den Wert angeben`File system ID`, der das Dateisystem identifiziert, für das 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

Die Audit-Logs von Amazon FSx FSx File Gateway (File Gateway) bieten Ihnen Details zum Benutzerzugriff auf Dateien und Ordner innerhalb einer Dateisystemverknüpfung. Sie können Auditprotokolle verwenden, um Benutzeraktivitäten zu überwachen und Maßnahmen zu ergreifen, wenn unangemessene Aktivitätsmuster identifiziert werden. Die Protokolle sind ähnlich wie Windows Server-Sicherheitsprotokollereignisse formatiert, um die Kompatibilität mit vorhandenen Protokollverarbeitungstools für Windows-Sicherheitsereignisse zu gewährleisten.

Operationen

In der folgenden Tabelle werden die Vorgänge zur Prüfung des File Gateway 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.

Vorgangsname	Definition
Delete	Eine Datei oder einen Ordner löschen.
Schreibattribute	Aktualisieren Sie Datei- oder Ordner-Metadaten (ACLs, Besitzer, Gruppe, Berechtigungen).

Attribute

In der folgenden Tabelle werden die FSx Dateizugriffsattribute für das File Gateway-Auditprotokoll beschrieben.

Attribut	Definition
`securityDescriptor`	Zeigt die für ein Objekt festgelegte besitzerv erwaltete Zugriffskontrollliste (DACL) im SDDL-Format an.
`sourceAddress`	Die IP-Adresse des Dateifreigabe-Clie ntcomputers.
`SubjectDomainName`	Die Active Directory-Domäne (AD), zu der das Konto des Clients gehört.
`SubjectUserName`	Der Active Directory-Benutzername des Clients.
`source`	Die ID des Storage Gateway`FileSyste mAssociation` , das geprüft wird.
`mtime`	Der Zeitpunkt, zu dem der Inhalt des Objekts geändert wurde; wird vom Client festgelegt.
`version`	Die Version des Auditprotokollformats.
`ObjectType`	Definiert, ob es sich bei dem Objekt um eine Datei oder einen Ordner handelt.

Attribut	Definition
`locationDnsName`	Der DNS-Name des FSx File Gateway-S ystems.
`objectName`	Der vollständige Pfad zum Objekt.
`ctime`	Der Zeitpunkt, zu dem der Inhalt oder die Metadaten des Objekts geändert wurden; wird vom Client festgelegt.
`shareName`	Der Name der Freigabe, auf die zugegriffen wird.
`operation`	Der Name des Objektzugriffsvorgangs.
`newObjectName`	Der vollständige Pfad zum neuen Objekt, nachdem es umbenannt wurde.
`gateway`	Die Storage Gateway-ID.
`status`	Der Status der aktuellen Operation. Nur Erfolge werden protokolliert (Fehler werden protokolliert, mit Ausnahme von Fehlern, die auf verweigerte Berechtigungen zurückzuf ühren sind).
`fileSizeInBytes`	Die Größe der Datei in Bytes, die vom Client zum Zeitpunkt der Dateierstellung festgelegt wird.

Pro Vorgang protokollierte Attribute

In der folgenden Tabelle werden die FSx File Gateway-Audit-Log-Attribute 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)	Attribute schreiben (chown)	Schreiber Sie Attribute (chmod)	Attribute schreiben (chgrp)
securiescrip							X			
sourceress	X	X	X	X	X	X	X	X	X	X
SubjecmainNa	X	X	X	X	X	X	X	X	X	X
SubjecerName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
versic	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
locatinsName	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
ctime			X	X						
shareN	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)	Attribute schreiben (chown)	Schreiben Sie Attribute (chmod)	Attribute schreiben (chgrp)
operat	X	X	X	X	X	X	X	X	X	X
newObjName					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSinBytes				X						

Wartung Ihres Gateways

Wartung Ihres Amazon FSx 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 Amazon FSx File Gateway Amazon 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 Ihr vorhandenes durch eine neue Instance— Erfahren Sie, wie Sie Ihr 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 werden die Häufigkeit 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

AWS aktualisiert 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 .

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 Ihrem AWS 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 für das Gateway-Wartungsfenster.

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 https://console.aws.amazon.com/storagegateway/zu Hause.
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 https://console.aws.amazon.com/storagegateway/zu Hause.
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 https://console.aws.amazon.com/storagegateway/zu Hause.
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

- Zugreifen auf die lokale Gateway-Konsole- Erfahren Sie, wie Sie sich bei der lokalen Konsole für ein lokales Gateway anmelden, das auf einer Linux-Kernel-basierten virtuellen Maschine (KVM) oder einer Microsoft Hyper-V VMware ESXi 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.

Zugreifen 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 mithilfe von Linux Kernel-based Virtual Machine (KVM) und Microsoft Hyper-V Manager. VMware ESXi

Themen

- Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
- Zugreifen auf die lokale Gateway-Konsole mit VMware ESXi
- Zugreifen auf die lokale Gateway-Konsole mit Microsoft 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 VMs die derzeit in KVM verfügbaren Optionen aufzulisten.

```
# virsh list
```

Der Befehl gibt eine Liste VMs mit jeweils ID -, Namen - und Statusinformationen zurück. Notieren Sie sich die virtuelle Maschine, für die Sie die lokale Gateway-Konsole starten möchten. `Id`

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 File Gateway-Konsole anmelden.

Nachdem Sie sich angemeldet haben, wird das Menü „AWS Geräteaktivierung — 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 Gateway-Konsole mit VMware ESXi

Um auf die lokale Konsole Ihres Gateways zuzugreifen mit VMware ESXi

1. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM aus.
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 File Gateway-Konsole anmelden.

   Nachdem Sie sich angemeldet haben, wird das Menü „AWS Geräteaktivierung — 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 Gateway-Konsole mit Microsoft Hyper-V

Zugreifen auf die lokale Gateway-Konsole (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 File Gateway-Konsole anmelden.

   Nachdem Sie sich angemeldet haben, wird das Menü „AWS Geräteaktivierung — 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 Hyper-V- und Linux-Kernel-basierten virtuellen Maschinen (KVM) Hypervisoren üblich. VMware

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 AWS Geräteaktivierung — 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 https://console.aws.amazon.com/storagegateway/zu Hause.

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

2. Geben Sie im Hauptmenü AWS -Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um HTTP-Proxy aktivieren auszuwählen.
3. Geben Sie im Menü AWS Appliance-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 zur Anmeldung an der VMware ESXi lokalen Konsole finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.

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

2. Geben Sie im Hauptmenü „AWS Geräteaktivierung — 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 Hypervisors 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 zur Anmeldung an der VMware ESXi lokalen Konsole finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. 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 auszuwählen AWS-Region , den Sie testen möchten. Unterstützte Endpunkte AWS-Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte 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 zur Anmeldung an der VMware ESXi Konsole finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. 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 zur Anmeldung an der VMware ESXi lokalen Konsole finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Geben Sie im Hauptmenü AWS Geräteaktivierung — 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. Für ein Gateway, das auf bereitgestellt wird VMware ESXi, reicht es aus, die Hypervisor-Host-Zeit einzustellen und die VM-Zeit mit dem Host zu synchronisieren, um Zeitabweichungen zu vermeiden. Weitere Informationen finden Sie unter Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit. Bei einem Gateway, das auf Microsoft Hyper-V bereitgestellt wird, sollten Sie die Zeit Ihrer VM in regelmäßigen Abständen überprüfe n. Weitere Informationen 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 zur Anmeldung an der VMware ESXi lokalen Konsole finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. 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	Administrationstool für IPv4 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 möchten, dass der AWS Support 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 AWS Appliance-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 AWS Appliance-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 auszuwählen AWS-Region , den Sie testen möchten. Unterstützte Endpunkte AWS-Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage

Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte 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, in der die Ergebnisse der Ressource nprüfung beschrieben werden.

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	Administrationstool für IPv4 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 AWS Appliance-Aktivierung — Konfiguration die entsprechende Zahl ein, um Netzwerkkonfiguration auszuwählen.

3. Geben Sie im Menü AWS Geräteaktivierung — 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 Ihr vorhandenes durch eine neue Instance

Sie können ein vorhandenes 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.

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.

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.

Um Ihr FSx File Gateway-Gateway durch eine neue Instanz mit einer leeren Cache-Festplatte und einer neuen Gateway-ID zu ersetzen:

1. Beenden Sie alle Anwendungen, die auf das bestehende File Gateway schreiben. Stellen Sie sicher, dass die `CachePercentDirty` Metrik auf der Registerkarte Überwachung `0` korrekt ist, bevor Sie Dateisystemzuordnungen auf dem neuen Gateway einrichten.
2. Verwenden Sie AWS Command Line Interface (AWS CLI), um die Konfigurationsinformationen über Ihr vorhandenes und die zugehörigen FSx Dateisysteme zu sammeln und zu speichern. Gehen Sie dazu wie folgt vor:

   a. Speichern Sie die Gateway-Konfigurationsinformationen für das 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 .

```
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 den Domänennamen des Microsoft Active Directory enthält, mit dem das Gateway verbunden ist.

c. Speichern Sie Dateifreigabeinformationen für jedes Dateisystem, das dem zugeordnet ist:

Verwenden Sie den folgenden Befehl für jedes zugehörige Dateisystem.

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

Mit diesem Befehl wird ein JSON-Block ausgegeben, der Metadaten über das Dateisystem enthält, wie z. B. den Standort ARN, das Auditprotokollziel, Cache-Aktualisierungsattribute, konfigurierte IP-Adressen und Tags.

3. Erstellen Sie ein neues File Gateway mit den gleichen Einstellungen und der gleichen Konfiguration wie das alte Gateway. Schlagen Sie gegebenenfalls in den Informationen nach, die Sie in Schritt 2 gespeichert haben.
4. Erstellen Sie neue Dateisystemzuordnungen für das neue Gateway mit denselben Einstellungen und derselben Konfiguration wie die Dateisysteme, die auf dem alten Gateway konfiguriert wurden. Schlagen Sie gegebenenfalls in den Informationen nach, die Sie in Schritt 2 gespeichert haben.
5. Vergewissern Sie sich, dass Ihr neues Gateway ordnungsgemäß funktioniert, und ordnen Sie dann Ihre Clients von den alten Dateisystemen auf die neuen Dateisysteme neu zu, 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 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 https://console.aws.amazon.com/storagegateway/zu Hause.
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.

Leistung und Optimierung

In diesem Abschnitt werden Anleitungen und bewährte Methoden zur Optimierung der File Gateway-Leistung beschrieben.

Themen

Grundlegende Hinweise zur Leistung für File Gateway

In diesem Abschnitt finden Sie Anleitungen zur Bereitstellung von Hardware für Ihre FSx 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.
> 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 Lesevorgängen bei Cache-Treffern um Lesevorgänge aus den Dateidaten, die aus dem Cache bereitgestellt werden. Cache-Fehllesevorgänge sind Lesevorgänge aus den Dateidaten, die von Amazon FSx für Windows File Server bereitgestellt werden.

Die folgende Tabelle zeigt ein Beispiel für eine FSx File Gateway-Konfiguration.

FSx Leistung von File Gateway auf Windows-Clients

Beispielkonfiguration	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-Festplatten: 2 x 2 TiB NVME Mindestnetzwerkleistung: 10 Gbit/s PROZESSOR: 32 vCPU | Arbeitsspeicher: 244 GB	SMBv3 - 1 Faden	162 MiB/sec (1,4 Gbit/s)	403 MiB/sec (3,4 Gbit/s)	288 MiB/sec (2,4 Gbit/s)
	SMBv3 - 8 Fäden	511 MiB/sec (4,3 Gbit/s)	571 MiB/sec (4,8 Gbit/s)	567 MiB/sec (4,8 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.

Optimierung der Gateway-Leistung

Sie können Information im Folgenden darüber bekommen, wie die Leistung Ihrer Gateway optimiert werden kann. Die Anleitungen basiert auf Ihr Hinzufügen von Ressourcen zu Ihrem Gateway und auf dem Hinzufügen von Ressourcen auf Ihrem Anwendungsserver.

Hinzufügen von Ressourcen zu Ihrem Gateway

Sie können die Gateway-Leistung optimieren, indem Sie Ihrem Gateway mit einer der folgenden Methoden Ressourcen hinzufügen.

Verwenden von Hochleistungs-Festplatten

Um die Gateway-Leistung zu optimieren, können Sie Hochleistungsfestplatten wie Solid-State-Laufwerke (SSDs) und einen NVMe Controller hinzufügen. Sie können auch virtuelle Festplatten direkt von einem Storage Area Network (SAN) anstelle des Microsoft Hyper-V NTFS, zu Ihrer VM hinzufügen. Eine verbesserte Festplattenleistung führt im Allgemeinen zu einem besseren Durchsatz und mehr input/output Operationen pro Sekunde (IOPS). Informationen zum Hinzufügen von Festplatten finden Sie unterKonfiguration von zusätzlichem Cache-Speicher.

Um zu den Durchsatz zu messen, verwenden Sie die Metriken `ReadBytes` und `WriteBytes` mit der `Samples` Amazon CloudWatch -Statistik. Beispiel: Mit dem `Samples` Statistik der `ReadBytes` Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie die IOPS. Allgemein gilt, wenn Sie diese Metriken für ein Gateway überprüfen, suchen Sie nach niedrigem Durchsatz und niedrigen IOPS.-Trends um Engpässe im Zusammenhang mit Datenträgern angeben zu können.

> **Note**
>
> CloudWatch Metriken sind nicht für alle Gateways verfügbar. Weitere Informationen, zu Gateway Metriken, finden Sie unter Überwachung Ihres File Gateway.

Hinzufügen von CPU Ressourcen zu Ihrem Gateway-Host

Die Mindestanforderung für einen Gateway-Host-Server sind vier virtuelle Prozessoren. Um die Gateway-Leistung zu optimieren, vergewissern Sie sich, dass die vier virtuellen Prozessoren, die der Gateway-VM zugeordnet sind, von vier Kernen gestützt werden. Stellen Sie außerdem sicher, dass Sie den Host-Server nicht überbucht CPUs haben.

Wenn Sie Ihrem Gateway-Hostserver weitere CPUs hinzufügen, erhöhen Sie die Verarbeitungskapazität des Gateways. Auf diese Weise kann Ihr Gateway parallel Daten aus Ihrer Anwendung in Ihrem lokalen Speicher speichern und diese Daten auf für Windows File Server hochladen. Stellen Sie CPUs außerdem sicher, dass Ihr Gateway genügend CPU-Ressourcen

erhält, wenn der Host mit anderen VMs geteilt wird. Über genügend CPU-Ressourcen zu verfügen hat den allgemeinen Effekt der Verbesserung des Durchsatzes.

Storage Gateway unterstützt die Verwendung von 24 CPUs in Ihrem Gateway-Hostserver. Sie können 24 verwenden CPUs , um die Leistung Ihres Gateways erheblich zu verbessern. Wir empfehlen die folgenden Gateway-Konfiguration für Ihren Gateway-Host-Server:

- CPUs24.
- 16 GiB reservierter RAM für File Gateways
  - 16 GiB reservierter RAM für Gateways mit einer Cache-Größe von bis zu 16 TiB
  - 32 GiB reservierter RAM für Gateways mit einer Cache-Größe von 16 TiB bis 32 TiB
  - 48 GiB reservierter RAM für Gateways mit einer Cache-Größe von 32 TiB bis 64 TiB
- Festplatte 1 zu paravirtual Controller 1 zugeordnet, als Gateway-Cache, wie folgt zu verwenden:
  - SSD mit einem NVMe Controller.
- Netzwerkadapter 1 auf VM Netzwerk 1 konfiguriert:
  - Verwenden Sie VM-Netzwerk 1 und fügen Sie VMXnet3 (10 Gbit/s) hinzu, um es für die Aufnahme zu verwenden.
- Netzwerkadapter 2 auf VM Netzwerk 2 konfiguriert:
  - Verwenden Sie das VM-Netzwerk 2 und fügen Sie ein VMXnet3 (10 Gbit/s) hinzu, mit dem eine Verbindung hergestellt werden soll. AWS

Sichern von virtuellen Gateway-Festplatten mit getrennten physischen Datenträgern

Wenn Sie Gateway-Laufwerke bereitstellen, empfehlen wir dringend, keine lokalen Festplatten für lokalen Speicher bereitzustellen, die dieselbe zugrunde liegende physische Speicherfestplatte verwenden. Beispielsweise VMware ESXi werden die zugrunde liegenden physischen Speicherressourcen als Datenspeicher dargestellt. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-Dateien. Wenn Sie eine virtuelle Festplatte bereitstellen (z. B. als Upload-Puffer), können Sie die virtuelle Festplatte im gleichen Datenspeicher wie die VM oder in einem anderen Datenspeicher speichern.

Wenn Sie über mehr als einen Datenspeicher verfügen, sollten Sie unbedingt einen Datenspeicher für jeden Typ von lokalem Speicher wählen, den sie erstellen. Ein Datenspeicher, der nur durch einen einzigen zugrunde liegenden physischen Datenträger gestützt wird, kann zu einer schlechten Leistung führen. Beispielsweise wenn Sie solch einen Datenträger sowohl zum Stützen des Cache-Speichers als auch des Upload-Puffers in einer Gateway-Konfiguration

verwenden. Dementsprechend kann auch ein Datenspeicher, der durch eine leistungsschwächere RAID-Konfiguration gestützt wird, wie z. B. RAID 1, eine schlechte Leistung zur Folge haben.

Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung

Erhöhen der Bandbreite zwischen Ihrem Anwendungsserver und Ihrem Gateway

Zum Optimieren der Gateway-Leistung, stellen Sie sicher, dass die Netzwerkbandbreite zwischen Ihrer Anwendung und dem Gateway, Ihre Anwendungsansprüche unterstützen kann. Sie können die `WriteBytes` Metriken `ReadBytes` und des Gateways verwenden, um den Gesamtdatendurchsatz zu messen.

Für Ihre Anwendung, vergleichen Sie den gemessenen Durchsatz mit dem gewünschten Durchsatz. Wenn der gemessene Durchsatz weniger als der gewünschte Durchsatz beträgt, dann kann die Erhöhung der Bandbreite zwischen Ihrer Anwendung und dem Gateway die Leistung verbessern können, wenn das Netzwerk der Engpass ist. Ebenso können Sie die Bandbreite zwischen Ihrer VM und Ihren lokalen Festplatten erhöhen, wenn sie nicht direkt angeschlossenen sind.

Hinzufügen von CPU-Ressourcen zu Ihrer Anwendungsumgebung

Wenn Ihre Anwendung zusätzliche CPU-Ressourcen nutzen kann, CPUs kann das Hinzufügen weiterer CPU-Ressourcen dazu beitragen, dass Ihre Anwendung ihre I/O Auslastung skaliert.

Einige Dateioperationen auf dem FSx File Gateway, wie z. B. das Umbenennen von Ordnern auf oberster Ebene oder Änderungen von Berechtigungen, können zu mehreren Dateivorgängen führen, die zu einer hohen I/O Belastung Ihres Dateisystems FSx für Windows File Server führen. Wenn Ihr Dateisystem nicht über genügend Leistungsressourcen für Ihre Arbeitslast verfügt, löscht das Dateisystem möglicherweise Schattenkopien, da es der kontinuierlichen I/O Verfügbarkeit Vorrang vor der Aufbewahrung historischer Schattenkopien einräumt.

Überprüfen Sie in der FSx Amazon-Konsole auf der Seite Überwachung und Leistung, ob Ihr Dateisystem nicht ausreichend bereitgestellt ist. Ist dies der Fall, können Sie zu SSD-Speicher wechseln, die Durchsatzkapazität erhöhen oder die SSD-IOPS erhöhen, um Ihre Arbeitslast zu bewältigen.

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 im AWS Storage 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. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer 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 AWS Services 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 in AWS Storage Gateway

Das AWS Modell der mit gilt für den Datenschutz in AWS Storage Gateway. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der alle Systeme laufen AWS 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. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

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 ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-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-Services verwenden AWS SDKs. 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 mit AWS KMS

Amazon FSx File Gateway unterstützt SMB-Verschlüsselung bis zur neuesten SMB v3.1.1-Spezifikation, einschließlich AES 128 CCM und AES 128 GCM. Kompatible Clients stellen automatisch eine Verbindung mithilfe der Verschlüsselung her. Darüber hinaus verwendet FSx File Gateway SMB-Verschlüsselung bei der Kommunikation mit FSx for Windows File Server in. AWS Sie müssen einen Direct Connect Link zu konfigurieren und entsprechende Richtlinien festlegen AWS, damit SMB-Verkehr und Verwaltungsdatenverkehr weitergeleitet werden können. AWS

Verschlüsseln eines Dateisystems

Weitere Informationen finden Sie unter Datenverschlüsselung FSx in Amazon im Amazon FSx for Windows File Server-Benutzerhandbuch.

Beachten AWS KMS Sie bei der Verwendung zur Verschlüsselung Ihrer Daten Folgendes:

- Ihre Daten werden im Ruhezustand in der Cloud verschlüsselt. Das heißt, die Daten werden in Amazon verschlüsselt FSx.
- 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 für AWS Storage Gateway

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-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 verwenden AWS . IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Fehlerbehebung bei Identität und Zugriff auf AWS Storage Gateway
- Verwenden Sie Tags, um den Zugriff auf Ihr Gateway und Ihre Ressourcen zu kontrollieren

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 Fehlerbehebung bei Identität und Zugriff auf AWS Storage Gateway).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert AWS Storage Gateway mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für Storage Gateway AWS).

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 .

AWS Bietet 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-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-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. AWS bewertet 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.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. 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.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden 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.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. 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.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt 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.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- 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 für eine Anfrage mehrere Arten von Richtlinien 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.

So funktioniert AWS Storage Gateway 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 AWS Storage Gateway verwenden können

IAM-Feature	AWS SGW-Unterstützung
Identitätsbasierte Richtlinien	Ja

IAM-Feature	AWS SGW-Unterstützung
Ressourcenbasierte 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-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS SGW und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für SGW AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. 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.

Beispiele für identitätsbasierte Richtlinien für SGW AWS

Beispiele für identitätsbasierte AWS SGW-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Storage Gateway AWS

Ressourcenbasierte Richtlinien innerhalb von SGW AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. 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.

Politische Aktionen für SGW AWS

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.

Bei Richtlinienaktionen in AWS SGW wird vor der Aktion das folgende Präfix verwendet:

```
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. Beispiele für identitätsbasierte Richtlinien für Storage Gateway AWS

Politische Ressourcen für SGW AWS

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was 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 Eigenschaften 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. Beispiele für identitätsbasierte Richtlinien für Storage Gateway AWS

Bedingungsschlüssel für Richtlinien für SGW AWS

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. Beispiele für identitätsbasierte Richtlinien für Storage Gateway AWS

ACLs AWS in SGW

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit SGW AWS

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-

Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, um Operationen zu ermöglichen, 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 mit SGW AWS

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. AWS empfiehlt, 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 für AWS SGW weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für SGW AWS

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.

Servicebezogene Rollen für SGW AWS

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt 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 Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Storage Gateway AWS

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 ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Storage Gateway in der Service Authorization Reference.

Themen

- Best Practices für Richtlinien
- Verwenden der SGW-Konsole AWS
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identitätsbasierte 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 AWS verwalteten 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 werden AWS-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 erfordert AWS-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.

Verwenden der SGW-Konsole AWS

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 umfasst 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": "*"
        }
    ]
}
```

Fehlerbehebung bei Identität und Zugriff auf AWS 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 in SGW durchzuführen AWS
- Ich bin nicht berechtigt, iam durchzuführen: PassRole

- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS SGW-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in SGW durchzuführen AWS

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 von mir den Zugriff AWS-Konto auf meine AWS SGW-Ressourcen ermöglichen

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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, 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 unter. So funktioniert AWS Storage Gateway 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 anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im 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"
            }
         }
      }
   ]
}
```

Konformitätsprüfung für AWS Storage Gateway

Externe 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, K-ISMS, ENS High, OSPAR und HITRUST CSF.

Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS 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 HIPAA-konforme Anwendungen entwickeln können. AWS
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — 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 können AWS , ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Resilienz im AWS Storage 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 Einheiten 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 AZ-Anschlüssen deutliche Vorteile. Jede AZ verfügt über unabhängige Stromversorgung, Kühlung und physische Sicherheit und ist über redundante ultra-low-latency Netzwerke verbunden. Wenn Ihre Bereitstellung einen Schwerpunkt auf Hochverfügbarkeit erfordert, können Sie Dienste und Ressourcen so konfigurieren, dass mehrere Dienste und Ressourcen verfügbar sind, AZs um eine höhere Fehlertoleranz zu erreichen.

AWS-Regionen erfüllen die höchsten Standards in Bezug auf Infrastruktursicherheit, Compliance und Datenschutz. Der gesamte Verkehr zwischen beiden AZs ist verschlüsselt. Die Netzwerkleistung reicht aus, um eine synchrone Replikation zwischen AZs zu erreichen. AZs vereinfacht die Partitionierung von Diensten und Ressourcen für hohe Verfügbarkeit. Wenn Ihre Bereitstellung übergreifend partitioniert ist AZs, 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 AWS Globale 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 Gateway.

Infrastruktursicherheit in AWS Storage 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 Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. 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.
> AWS überprüft, analysiert und behebt CVEs regelmäßig Abhilfemaßnahmen. 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 verwalten Gateway-Updates mit der AWS Storage Gateway Konsole verwalten.

AWS Bewährte Sicherheitsmethoden

AWS bietet 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 Überwachung AWS Storage Gateway

Storage Gateway ist in einen Dienst integriert AWS 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 CloudTrail Benutzerhandbuch.

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, Dateisystemen, Hochverfügbarkeit, Datenwiederherstellung und Snapshots. 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 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-Adresse 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 entsprechenden 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-Anforderungen.
Die Aktivierung des Gateways schlägt fehl, wenn Sie in der Storage-Gateway-Managementkonsole auf die Schaltfläche 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 automatisch 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-Servers (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 Bandbreite zwischen Ihrem Gateway und AWS verbessern.	Sie können die Bandbreite zwischen Ihrem Gateway und verbessern, 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 über eine Verbindung mit hoher Bandbreite verfügen 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.

Aktivieren Sie den Support Zugriff, um die Fehlerbehebung für Ihr lokal gehostetes Gateway zu erleichtern

Storage Gateway stellt eine lokale Konsole zur Verfügung, mit der Sie verschiedene Wartungsaufgaben ausführen können, einschließlich des Zugriffs auf Ihr Gateway, um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Support 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 Gateway-Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft 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 FSx File Gateway bereit.

Themen

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 stellt eine lokale Konsole zur Verfügung, mit der Sie verschiedene Wartungsaufgaben ausführen können, einschließlich des Zugriffs auf Ihr Gateway, um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Support 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: FileMissing

Der `FileMissing` Fehler ähnelt dem `ObjectMissing` Fehler, und die Schritte zur Behebung des Fehlers sind identisch. Sie können eine `FileMissing` Fehlermeldung erhalten, wenn ein anderer Writer als das angegebene File Gateway die angegebene Datei aus dem Amazon FSx löscht. Alle nachfolgenden Uploads zu Amazon FSx oder Abrufe von Amazon FSx für das Objekt schlagen fehl.

Um einen Fehler zu beheben FileMissing

1. Speichern Sie die neueste Kopie der Datei im lokalen Dateisystem Ihres SMB-Clients (Sie benötigen diese Dateikopie in Schritt 3).
2. Löschen Sie die Datei mit Ihrem SMB-Client vom File Gateway.
3. Kopieren Sie die neueste Version der Datei, die Sie in Schritt 1 Amazon gespeichert haben, FSx mit Ihrem SMB-Client. Tun Sie dies über Ihr File Gateway.

Fehler: FsxFileSystemAuthenticationFailure

Sie können eine `FsxFileSystemAuthenticationFailure` Fehlermeldung erhalten, wenn die beim Anhängen des Dateisystems angegebenen Anmeldeinformationen abgelaufen sind oder wenn die Rechte des Dateisystems entzogen wurden.

Um einen Fehler zu beheben FsxFileSystemAuthenticationFailure

1. Stellen Sie sicher, dass die Anmeldeinformationen, die Sie beim Anhängen des FSx Amazon-Dateisystems angegeben haben, weiterhin gültig sind.
2. Stellen Sie sicher, dass der Benutzer über alle erforderlichen Berechtigungen verfügt, wie unter Ein Amazon FSx for Windows File Server-Dateisystem anhängen beschrieben.

Fehler: FsxFileSystemConnectionFailure

Sie können eine `FsxFileSystemConnectionFailure` Fehlermeldung erhalten, wenn auf den FSx Amazon-Server vom Gateway-Computer aus nicht zugegriffen werden kann.

Um einen Fehler zu beheben FsxFileSystemConnectionFailure

1. Stellen Sie sicher, dass alle Firewall- und VPC-Regeln die Verbindung zwischen dem Gateway-Computer und dem FSx Amazon-Server zulassen.
2. Stellen Sie sicher, dass der FSx Amazon-Server läuft.

Fehler: FsxFileSystemFull

Sie können eine `FsxFileSystemFull` Fehlermeldung erhalten, wenn im FSx Amazon-Dateisystem nicht genügend freier Speicherplatz vorhanden ist.

Um einen FsxFileSystemFull Fehler zu beheben

- Erhöhen Sie den Speicherplatz für das FSx Amazon-Dateisystem.

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 Konfigurieren eines Network Time Protocol (NTP) - Servers für Ihr Gateway.

Fehler: InvalidFileState

Es kann zu einer `InvalidFileState` Fehlermeldung kommen, wenn ein anderer Writer als das angegebene Gateway die angegebene Datei in der angegebenen Dateifreigabe ändert. Infolgedessen stimmt der Status der Datei auf dem Gateway nicht mit dem Status in Amazon überein FSx. Alle nachfolgenden Uploads oder Abrufe der Datei von Amazon FSx könnten fehlschlagen.

Um einen Fehler zu beheben InvalidFileState

1. Speichern Sie die neueste Kopie der Datei im lokalen Dateisystem Ihres SMB-Clients (Sie müssen diese Datei in Schritt 4 kopieren). Wenn die Version der Datei in Amazon die neueste FSx ist, laden Sie diese Version herunter. Sie können dies tun, indem Sie mit einem beliebigen SMB-Client direkt auf die FSx Amazon-Aktie zugreifen.
2. Löschen Sie die Datei FSx direkt in Amazon.
3. Löschen Sie die Datei mit Ihrem SMB-Client vom Gateway.
4. Kopieren Sie mit Ihrem SMB-Client die neueste Version der Datei, die Sie in Schritt 1 gespeichert haben, über Ihr File Gateway nach Amazon FSx.

Fehler: ObjectMissing

Sie können eine `ObjectMissing` Fehlermeldung erhalten, wenn ein anderer Writer als das angegebene File Gateway die angegebene Datei aus Amazon FSx löscht. Alle nachfolgenden Uploads zu Amazon FSx oder Abrufe von Amazon FSx für das Objekt schlagen fehl.

Um einen Fehler zu beheben ObjectMissing

1. Speichern Sie die neueste Kopie der Datei im lokalen Dateisystem Ihres SMB-Clients (Sie benötigen diese Dateikopie in Schritt 3).
2. Löschen Sie die Datei mit Ihrem SMB-Client vom File Gateway.
3. Kopieren Sie die neueste Version der Datei, die Sie in Schritt 1 Amazon gespeichert haben, FSx mit Ihrem SMB-Client. Tun Sie dies über Ihr File Gateway.

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: Probleme mit der Active Directory-Domäne

FSx File Gateway generiert keine spezifischen Protokollmeldungen für Probleme mit der Active Directory-Domäne. Wenn Sie Probleme haben, Ihr Gateway mit Ihrer Active Directory-Domäne zu verbinden, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass das Gateway nicht versucht, einen schreibgeschützten Domänencontroller (RODC) zu verwenden, um der Domäne beizutreten.
- Stellen Sie sicher, dass das Gateway für die Verwendung der richtigen DNS-Server konfiguriert ist.

  Wenn Sie beispielsweise versuchen, eine Amazon EC2 EC2-Gateway-Instance mit einem AWS-verwalteten Active Directory zu verbinden, stellen Sie sicher, dass die für Ihre EC2-VPC festgelegte DHCP-Option die AWS-verwalteten Active Directory-DNS-Server angibt.

  DNS-Server, die Sie über den VPC-DHCP-Optionssatz konfigurieren, werden allen EC2-Instances in der VPC zur Verfügung gestellt. Wenn Sie einen DNS-Server für ein einzelnes Gateway angeben möchten, können Sie dies über die lokale EC2-Konsole dieses Gateways tun.

Für lokale Gateways geben Sie einen DNS-Server mithilfe der lokalen VM-Konsole an.

- Überprüfen Sie die Netzwerkkonnektivität des Gateways, indem Sie die folgenden Befehle an der Eingabeaufforderung in der lokalen Konsole des Gateways ausführen. Ersetzen Sie die hervorgehobenen Variablen durch den tatsächlichen Domänennamen und die IP-Adressen aus Ihrer Bereitstellung.

```
dig -d ExampleDomainName
ncport -d ExampleDomainControllerIPAddress -p 445
ncport -d ExampleDomainControllerIPAddress -p 389
```

- Stellen Sie sicher, dass Ihr Active Directory-Dienstkonto über die erforderlichen Berechtigungen verfügt. Weitere Informationen finden Sie unter Berechtigungsanforderungen für für Active Directory-Dienstkonten.
- Stellen Sie sicher, dass das Gateway der richtigen Organisationseinheit (OU) beitritt.

  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 über eine festgelegte Organisationseinheit für neue Computerobjekte verfügt, müssen Sie diese Organisationseinheit angeben, wenn Sie der Domäne beitreten.

  Wenn Sie beim Versuch, der angegebenen Organisationseinheit beizutreten, auf Fehler mit Zugriff verweigert stoßen, wenden Sie sich an Ihren Active Directory-Domänenadministrator. Möglicherweise muss der Administrator das Computerkonto des Gateways vorab einrichten, bevor es der Domäne beitreten kann. Weitere Informationen finden Sie unter Wie kann ich Probleme beim Verbinden meines Storage Gateway-File-Gateways mit einer Domäne für die Microsoft Active Directory-Authentifizierung beheben? .
- Stellen Sie sicher, dass der Hostname Ihres Gateways in DNS aufgelöst werden kann, indem Sie den folgenden Befehl an der Eingabeaufforderung in der lokalen Konsole des Gateways ausführen. Ersetzen Sie die hervorgehobene Variable durch den tatsächlichen Hostnamen für Ihr Gateway.

```
dig -d ExampleHostName -r A
```

Wenn Sie einen benutzerdefinierten Hostnamen für Ihr Gateway konfiguriert haben, müssen Sie manuell einen DNS-A-Eintrag hinzufügen, der auf seine IP-Adresse verweist.

- Stellen Sie sicher, dass die Netzwerklatenz zwischen dem Gateway und dem Domänencontroller relativ gering ist. Bei der Anfrage zum Beitritt zu einer Domäne kann es zu einem Timeout kommen, wenn das Gateway innerhalb von 20 Sekunden keine Antwort vom Domänencontroller erhält.

  Wenn Sie das Gateway mithilfe des JoinDomainCLI-Befehls mit der Domain verbinden, können Sie das `--timeout-in-seconds` Flag hinzufügen, um das Timeout auf maximal 3.600 Sekunden zu erhöhen.
- Stellen Sie sicher, dass der Active Directory-Benutzer, den Sie für den Beitritt zum Gateway zur Domäne verwenden, über die dafür erforderlichen Rechte verfügt.

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 für Windows File Server 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.

  Diskutieren Sie mit Support dem Inhalt des zugehörigen FSx Amazon-Dateisystems 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.

Sie sehen keine Dateien in Ihrem FSx Amazon-Dateisystem

Wenn Sie feststellen, dass Dateien auf dem Gateway nicht im FSx Amazon-Dateisystem 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.

Sie sehen keine älteren Snapshots in Ihrem FSx Amazon-Dateisystem

Einige Dateioperationen auf dem FSx File Gateway, wie z. B. das Umbenennen von Ordnern auf oberster Ebene oder Änderungen von Berechtigungen, können zu mehreren Dateivorgängen führen, die zu einer hohen I/O Belastung Ihres Dateisystems FSx für Windows File Server führen. Wenn Ihr Dateisystem nicht über genügend Leistungsressourcen für Ihre Arbeitslast verfügt, löscht das Dateisystem möglicherweise Schattenkopien, da es der kontinuierlichen I/O Verfügbarkeit Vorrang vor der Aufbewahrung historischer Schattenkopien einräumt.

Überprüfen Sie in der FSx Amazon-Konsole auf der Seite Überwachung und Leistung, ob Ihr Dateisystem nicht ausreichend bereitgestellt ist. Ist dies der Fall, können Sie zu SSD-Speicher wechseln, die Durchsatzkapazität erhöhen oder die SSD-IOPS erhöhen, um Ihre Arbeitslast zu bewältigen.

Ihr Gateway überträgt langsam Daten an Amazon FSx

Wenn Ihr File Gateway Daten langsam an Amazon FSx for Windows File Server 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 FSx for Windows File Server hochladen kann. Erwägen Sie, die Bandbreite für den Upload von Ihrem File Gateway zu erhöhen, eine oder mehrere Cache-Festplatten hinzuzufügen, Client-Schreibvorgänge zu verlangsamen oder die Durchsatzkapazität für den zugehörigen Amazon FSx for Windows File Server zu erhöhen.
- 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.

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 für Windows File Server 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 für Windows File Server 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.

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

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

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 für Windows File Server ein neues 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 FSx File Gateway bereit.
2. Erstellen Sie ein neues auf dem von Ihnen erstellten EC2-Gateway. Weitere Informationen finden Sie unter Erstellen eines Dateisystems FSx für Windows File Server.

3. Stellen Sie Ihr auf Ihrem Client bereit und ordnen Sie es dem für Windows File Server zu, der die Daten enthält, die Sie wiederherstellen möchten. Weitere Informationen finden Sie unter und verwenden Sie Ihre Dateifreigabe.

Wiederherstellung aus Backups oder Snapshots direkt auf Amazon FSx

In einigen Fällen müssen Sie möglicherweise Daten auf Ihrem FSx Amazon-Dateisystem direkt wiederherstellen, indem Sie ein Backup oder einen Snapshot von einem früheren Zeitpunkt verwenden. In diesen Fällen besteht das Risiko, dass zwischen der Backup-Anwendung und dem FSx File Gateway ein Dual-Writer-Szenario entsteht, was dazu führen kann, dass Dateien hängen bleiben oder nicht übereinstimmen. Gehen Sie wie folgt vor, um Probleme bei der Wiederherstellung Ihres FSx Amazon-Dateisystems aus Backups oder Snapshots zu vermeiden.

> **Note**
>
> Alle derzeit auf Ihrem FSx File Gateway zwischengespeicherten Daten sind nicht gültig, nachdem Sie Ihr FSx Amazon-Dateisystem mithilfe dieses Verfahrens aus einem Backup oder Snapshot wiederhergestellt haben.

Um Probleme bei der Wiederherstellung Ihres FSx Amazon-Dateisystems aus Backups oder Snapshots zu vermeiden

1. Trennen Sie das FSx Amazon-Dateisystem mithilfe der Storage Gateway-Konsole vom FSx File Gateway.
2. Stellen Sie das Backup oder den Snapshot direkt auf Ihrem FSx Amazon-Dateisystem wieder her.
3. Hängen Sie das FSx Amazon-Dateisystem mithilfe der Storage Gateway-Konsole erneut an das FSx File Gateway an.

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.
- 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.

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 FSx File Gateway bereit
- Stellen Sie einen benutzerdefinierten Amazon EC2 EC2-Host für FSx File Gateway bereit
- Metadatenoptionen Amazon EC2 EC2-Instances ändern
- Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Host-Zeit
- Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit
- Netzwerkadapter für Ihr Gateway konfigurieren
- Verwenden von VMware vSphere High Availability mit Storage Gateway

Stellen Sie einen Amazon EC2 EC2-Standardhost für FSx File Gateway bereit

In diesem Thema werden die Schritte zur Bereitstellung eines Amazon-EC2-Hosts unter Verwendung der Standardspezifikationen aufgeführt.

Sie können ein auf einer Amazon 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 FSx 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 Öffentliche IP-Adresse automatisch zuweisen 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
137	UDP	NetBIOS
138	UDP	NetBIOS
139	TCP, UDP	SMB
389	TCP	LDAP
445	TCP	SMB

- 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

Standardeinstellungen	AMI-Root-Volume	Volume 2 Cache				
Beim Beenden löschen	Ja	Ja				
Verschlüsselt	Nein	Nein				
Durchsatz	125	125				

Stellen Sie einen benutzerdefinierten Amazon EC2 EC2-Host für FSx File Gateway bereit

Sie können ein auf einer Amazon 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.
> File Gateway AMIs verwendet die folgende Namenskonvention. Die an den AMI-Namen angehängte Versionsnummer ändert sich mit jeder Versionsversion.
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

Um eine Amazon EC2 EC2-Instance als Host für Ihr Amazon FSx File Gateway bereitzustellen

1. Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter einrichten Amazon FSx 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 .

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 zu den für erforderlichen Ports finden Sie unter Port-Anforderungen. FSx Weitere Informationen finden Sie unter Sicherheitsgruppenregeln im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances.

> **Note**
>
> Amazon FSx 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.
> Darüber hinaus müssen Sie TCP-Port 445 für SMB-Zugriff, UDP-Port 137 für NetBIOS-Zugriff, UDP-Port 138 für NetBIOS-Zugriff und TCP-Port 389 für LDAP-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 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 einrichten Amazon FSx 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_FSX_SMB/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_FSX_SMB/latest
```

Dieser CLI-Befehl gibt etwa die folgende Ausgabe zurück:

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 18,
         "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_FSX_SMB/latest",
         "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
        "Value": "ami-033d1edba5606cffb"
    }
}
```

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 Zugreifen auf die lokale Gateway-Konsole mit Microsoft 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.

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.

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 Sie ein Amazon FSx File Gateway

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
   - Mindestverfügbarkeit: Sekunden **120**
   - Maximum per-VM resets (Maximale Zurücksetzungen pro VM): **5**
   - Maximales Zeitfenster für das Zurücksetzen: 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 aktivieren und Ihr Amazon FSx File Gateway 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 File Gateway-Integritätsprotokollen 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)

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.

So rufen Sie den Aktivierungsschlüssel für einen öffentlichen Endpunkt ab:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

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.

So rufen Sie auf Ihrer lokalen Konsole einen Aktivierungsschlüssel für Ihr Gateway ab

1. Melden Sie sich als Administrator bei Ihrer lokalen Konsole an.
2. Nachdem Sie sich angemeldet haben und das Hauptmenü AWS Appliance-Aktivierung – Konfiguration angezeigt wird, wählen Sie `0`, um Aktivierungsschlüssel abrufen auszuwählen.
3. Wählen Sie die Option Storage Gateway für die Gateway-Produktreihe aus.
4. Wenn Sie dazu aufgefordert werden, geben Sie den AWS-Region Ort ein, an dem Sie Ihr Gateway aktivieren möchten.
5. Geben Sie als Netzwerktyp 1 für „Öffentlich“ oder 2 für „VPC-Endpunkt“ ein.

6. Geben Sie als Endpunkttyp 1 für „Standard“ oder 2 für „Federal Information Processing Standard (FIPS)“ ein.

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 daran zu hindern, Daten zu lesen und zu schreiben
- 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 Gateway-Konsole mit VMware ESXi
- Hyper-V-Host: Zugreifen auf die lokale Gateway-Konsole mit Microsoft 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.

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 allerdings diese Ressourcen-IDs mit der Amazon-EC2-API verwenden, erwartet Amazon-EC2-Ressourcen-IDs in Kleinbuchstaben. Sie müssen Ihre Ressourcen-ID in Kleinbuchstaben ändern, um Sie mit der EC2-API verwenden zu können. Bei einem Storage Gateway beispielsweise könnte die ID für ein Volume `vol-1122AABB` lauten. Wenn Sie diese ID mit der EC2-API verwenden, müssen Sie sie zu `vol-1122aabb` ändern. Andernfalls verhält sich die EC2-API möglicherweise nicht wie erwartet.

> **Important**
>
> IDs für Storage Gateway Gateway-Volumes und Amazon EBS-Snapshots, die aus Gateway-Volumes erstellt wurden, werden in ein längeres Format geändert. Ab Dezember 2016 werden alle neuen Volumes und Snapshots mit einer 17-stelligen Zeichenfolge erstellt. Ab April 2016 können Sie diese länger verwenden, IDs sodass Sie Ihre Systeme mit dem neuen Format testen können. Weitere Informationen finden Sie unter Longer EC2 and EBS Resource. IDs
>
> Beispielsweise sieht ein Volume-ARN mit dem längeren Volume-ID-Format wie folgt aus: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
>
> Eine Snapshot-ID mit dem längeren ID-Format sieht so aus: `snap-78e226633445566ee`. Weitere Informationen finden Sie unter Ankündigung: Heads-up — Longer Storage Gateway Volume und Snapshot IDs erscheinen 2016.

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

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 FSx File Gateway

Für die Bereitstellung der Funktionen von Amazon FSx File Gateway (FSx 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 FSx File Gateway-Software enthalten sind:

- Für Amazon FSx File Gateway Version 2021-07-07: -open-source.tgz sgw-file-fsx-smb

- Für Amazon FSx File Gateway Version 2021-04-06: -20210406-open-source.tgz sgw-file-fsx-smb

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 Tools von Drittanbietern finden Sie unter den folgenden Links:

- Für Amazon FSx File Gateway Version 2021-07-07: Drittanbieter-Lizenz.
- Für Amazon FSx File Gateway Version 2021-04-06: Drittanbieter-Lizenz.

Beschränkungen und Kontingente für Amazon FSx File Gateway

Kontingente für FSx Amazon-Dateisysteme

In der folgenden Tabelle sind Mindest- und Höchstgrenzen und Kontingente für FSx Amazon-Dateisysteme aufgeführt.

Ressource	Limit pro FSx Amazon-Dateisystem
Maximale Anzahl von Tags	50 Schlagworte
Maximale Aufbewahrungsdauer für automatisierte Backups	90 Tage
Maximale Anzahl laufender Backup-Kopie-Anfragen an eine einzelne Zielregion pro Konto.	5 Anfragen
Mindestspeicherkapazität für SSD-Dateisysteme	32 GiB
Mindestspeicherkapazität für HDD-Dateisysteme	2.000 GiB
Maximale Speicherkapazität für SSD- und HDD-Dateisysteme	64 TiB
Minimale Durchsatzkapazität	8 MBps
Maximale Durchsatzkapazität	2.048 MBps

Ressource	Limit pro FSx Amazon-Dateisystem
Maximale Anzahl von FSx Amazon-Dateifreigaben	100 000

Empfohlene Kapazität für die lokalen Datenträger des Gateways

In der folgenden Tabelle werden die Größen für den lokalen Festplattenspeicher für jeden einzelnen Speicherplatz AWS Storage Gateway in Ihrer Bereitstellung empfohlen.

Gateway-Typ	Cache (Minimum)	Cache (Maximum)	
FSx 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 FSx File Gateway Cache hinzufügen, ist es wichtig, neue Festplatten auf Ihrem virtuellen Host (Hypervisor oder Amazon EC2 EC2-Instance) zu erstellen. Ändern Sie nicht die Größe vorhandener Festplatten, wenn die Festplatten zuvor als Cache zugewiesen wurden.

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 FSx 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
Hinweis zur Änderung der Verfügbarkeit für FSx File Gateway	Amazon FSx File Gateway ist für Neukunden nicht mehr verfügbar. Bestandskunden von FSx File Gateway können den Service weiterhin normal nutzen. Informationen zu Funktionen, die FSx File Gateway ähneln, finden Sie in diesem Blogbeitrag.	28. Oktober 2024
Hinweis zur Änderung der Verfügbarkeit von FSx File Gateway	AWS Storage Gateway FSx File Gateway wird ab dem 28.10.24 für Neukunden nicht mehr verfügbar sein. Um den Service nutzen zu können, müssen Sie sich vor diesem Datum anmelden. Bestandsk unden von FSx File Gateway können den Service weiterhin normal nutzen. Informationen zu Funktionen, die FSx File Gateway ähneln, finden Sie in diesem Blogbeitrag.	26. September 2024
Option hinzugefügt, um Wartungsupdates ein- oder auszuschalten	Storage Gateway erhält regelmäßige Wartungsu pdates, die Betriebssystem-	6. Juni 2024

	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 verwalten Gateway-Updates mit der AWS Storage Gateway Konsole verwalten.	
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 zu CloudWatch Alarmen.	2. Oktober 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
Tipps zur Fehlerbehebung beim Active Directory-Beitritt zur Domäne hinzugefügt	Der Abschnitt Problembehandlung: Probleme mit File Gateway enthält jetzt Richtlinien zur Problembehandlung, die bei der Diagnose von Problemen helfen, die auftreten können, wenn Sie versuchen, Ihr Gateway mit einer Active Directory -Domäne zu verbinden. Weitere Informationen finden Sie unter Problembehandlung: Probleme mit der Active Directory-Domäne.	19. Oktober 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
Unterstützung mehrerer Dateisysteme	Amazon FSx File Gateway unterstützt jetzt bis zu fünf angehängte FSx Amazon-Dateisysteme. Weitere Informationen finden Sie unter Anhängen eines Dateisystems von Amazon FSx für Windows.	7. Juli 2021

Unterstützung von Amazon FSx Soft Storage-Kontingenten	Amazon FSx File Gateway unterstützt jetzt Soft-Storage-Kontingente (die Sie warnen, wenn Benutzer ihre Datenlimits überschreiten) beim Schreiben in angehängte FSx Amazon-Dateisysteme, in denen Speicherkontingente konfiguriert sind. Feste Kontingente (die Datenlimits durchsetzen, indem sie den Schreibzugriff verweigern) werden nicht unterstützt. Soft-Quotas funktionieren für alle Benutzer außer dem FSx Amazon-Admin-Benutzer. Weitere Informationen zur Einrichtung von Speicherkontingenten finden Sie unter Speicherkontingente im Amazon FSx for Windows File Server-Benutzerhandbuch.	7. Juli 2021

Neues Handbuch	Zusätzlich zum ursprünglichen File Gateway (jetzt bekannt als Amazon S3 File Gateway) bietet Storage Gateway Amazon FSx File Gateway (FSx File Gateway). FSx File Gateway bietet geringe Latenz und effizienten Zugriff auf Cloud-basierte Dateifreigaben FSx für Windows File Server von Ihrer lokalen Einrichtung aus. Weitere Informationen finden Sie unter Was ist Amazon FSx File Gateway?	27. April 2021
FedRAMP-Compliance	Storage Gateway ist jetzt FedRAMP-konform. Weitere Informationen finden Sie unter Konformitätsprüfung für Storage Gateway.	24. November 2020
File Gateway-Migration	File Gateway bietet jetzt einen dokumentierten Prozess zum Ersetzen eines vorhandenen 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 Leseleistung 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
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 Informationen finden Sie unter AWS Storage Gateway -Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	7. Mai 2020

Unterstützung für die S3 Intelligent-Tiering-Speicherklasse	Storage Gateway unterstützt jetzt die S3 Intelligent-Tiering-Speicherklasse. Die S3 Intelligent-Tiering-Speicherklasse optimiert die Speicherkosten, indem Daten automatisch auf die kostengünstigste Zugriffsebene übertragen werden, ohne dass sich dies auf die Leistungsfähigkeit oder den Betriebsaufwand auswirkt. Weitere Informationen finden Sie unter Speicherklasse zum automatischen Optimieren häufig und selten aufgerufener Objekte im Amazon-Simple-Storage-Service-Benutzerhandbuch.	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-Referenz.	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
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

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
Neu AWS-Region	Tape Gateway ist jetzt in der Region Asien-Pazifik (Singapur) erhältlich. Weitere Informationen hierzu finden Sie unter AWS-Regionen die Storage Gateway unterstützen.	3. April 2018
Neu AWS-Region	Storage Gateway ist jetzt in der Region Europa (Paris) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionen die Storage Gateway unterstützen.	18. Dezember 2017
Support für VMware ESXi Hypervisor Version 6.5	AWS Storage Gateway unterstützt jetzt VMware ESXi Hypervisor Version 6.5. Diese Version wird zusätzlich zu den Versionen 4.1, 5.0, 5.1, 5.5 und 6.0 unterstützt. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	13. September 2017
Unterstützung für den Hypervisor Microsoft Hyper-V in der File Gateway-Konfiguration	Es ist nun möglich, ein File Gateway auf dem Hypervisor Microsoft Hyper-V bereitzustellen. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	22. Juni 2017
Neu AWS-Region	Storage Gateway ist jetzt in der Region Asien-Pazifik (Mumbai) erhältlich. Weitere Informationen hierzu finden Sie unter AWS-Regionen die Storage Gateway unterstützen.	02. Mai 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	08. Februar 2017

Änderungen	Beschreibung	Änderungsdatum
	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 Sie ein Amazon FSx File Gateway Informationen zum Starten eines File Gateway-AMI finden Sie unterStellen Sie einen Amazon EC2 EC2-Standardhost für FSx 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.	
Neu AWS-Region	Storage Gateway ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionen die 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-Regionen die 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 Branchenstandard 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