Benutzerhandbuch für Tape Gateway

AWS Storage Gateway

API-Version 2013-06-30

AWS Storage Gateway: Benutzerhandbuch für Tape Gateway

Table of Contents

Die Amazon S3 File Gateway-Dokumentation wurde nach Was ist Amazon S3 File Gateway? verschoben.

Die Amazon FSx File Gateway-Dokumentation wurde nach Was ist Amazon FSx File Gateway? verschoben.

Die Volume Gateway-Dokumentation wurde nach Was ist Volume Gateway? verschoben.

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 Tape Gateway?

AWS Storage Gateway verbindet eine On-Premises-Software-Appliance mit cloudbasiertem Speicher, um eine nahtlose Integration mit Datensicherheitsfunktionen zwischen Ihrer On-Premises-IT-Umgebung und der AWS Speicherinfrastruktur zu ermöglichen. Mit diesem Service können Sie Daten in der Amazon Web Services Cloud speichern und erhalten so skalierbaren und kosteneffizienten Speicher, der zur Aufrechterhaltung der Datensicherheit dient.

AWS Storage Gateway bietet dateibasierte File Gateways (Amazon S3-Datei und Amazon-FSx-Datei), volumenbasierte (gespeicherte und gespeicherte) und bandbasierte Speicherlösungen.

Themen

Tape Gateway

Tape Gateway – Ein Tape Gateway bietet Cloud-gestützten virtuellen Bandspeicher.

Mit einem Tape Gateway können Sie kostengünstig und dauerhaft Sicherungsdaten in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archivieren. Ein Tape Gateway bietet eine virtuelle Bandinfrastruktur, die sich nahtlos mit Ihren Geschäftsanforderungen skalieren lässt, sodass der betriebliche Aufwand für die Bereitstellung, Skalierung und Verwaltung einer physischen Bandinfrastruktur wegfällt.

Sie können Storage Gateway entweder On-Premises als VM-Appliance bereitstellen, die auf einem VMware ESXi-, KVM- oder Microsoft Hyper-V-Hypervisor, als Hardware-Appliance oder in AWS als Amazon EC2-Instance ausgeführt wird. Sie stellen Ihr Gateway auf einer EC2-Instance bereit, um iSCSI-Speicher-Volumes in AWS bereitzustellen. Sie können Gateways, die auf EC2-Instances gehostet werden, für die Notfallwiederherstellung, die Datenspiegelung und die Bereitstellung von Speicher für Anwendungen verwenden, die in Amazon EC2 gehostet werden.

Eine Übersicht über die Architektur finden Sie unter So funktioniert Tape Gateway (Architektur). Informationen zu den verschiedenen Anwendungsfällen, die AWS Storage Gateway unterstützt, finden Sie unter AWS Storage Gateway.

Dokumentation: Die Dokumentation für Tape Gateway finden Sie unter Erstellen eines Tape Gateways.

Verwenden Sie Storage Gateway zum ersten Mal?

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

- Anweisungen zum Erstellen und Verwenden eines Tape Gateways finden Sie unter Erstellen eines Tape Gateways. Hier erfahren Sie, wie Sie Daten auf virtuellen Tapes sichern und die Tages archivieren.

- Unter Verwalten von Gateways wird beschrieben, wie Verwaltungsaufgaben für Ihr Gateway und die zugehörigen Ressourcen ausgeführt werden.

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

So funktioniert Tape Gateway (Architektur)

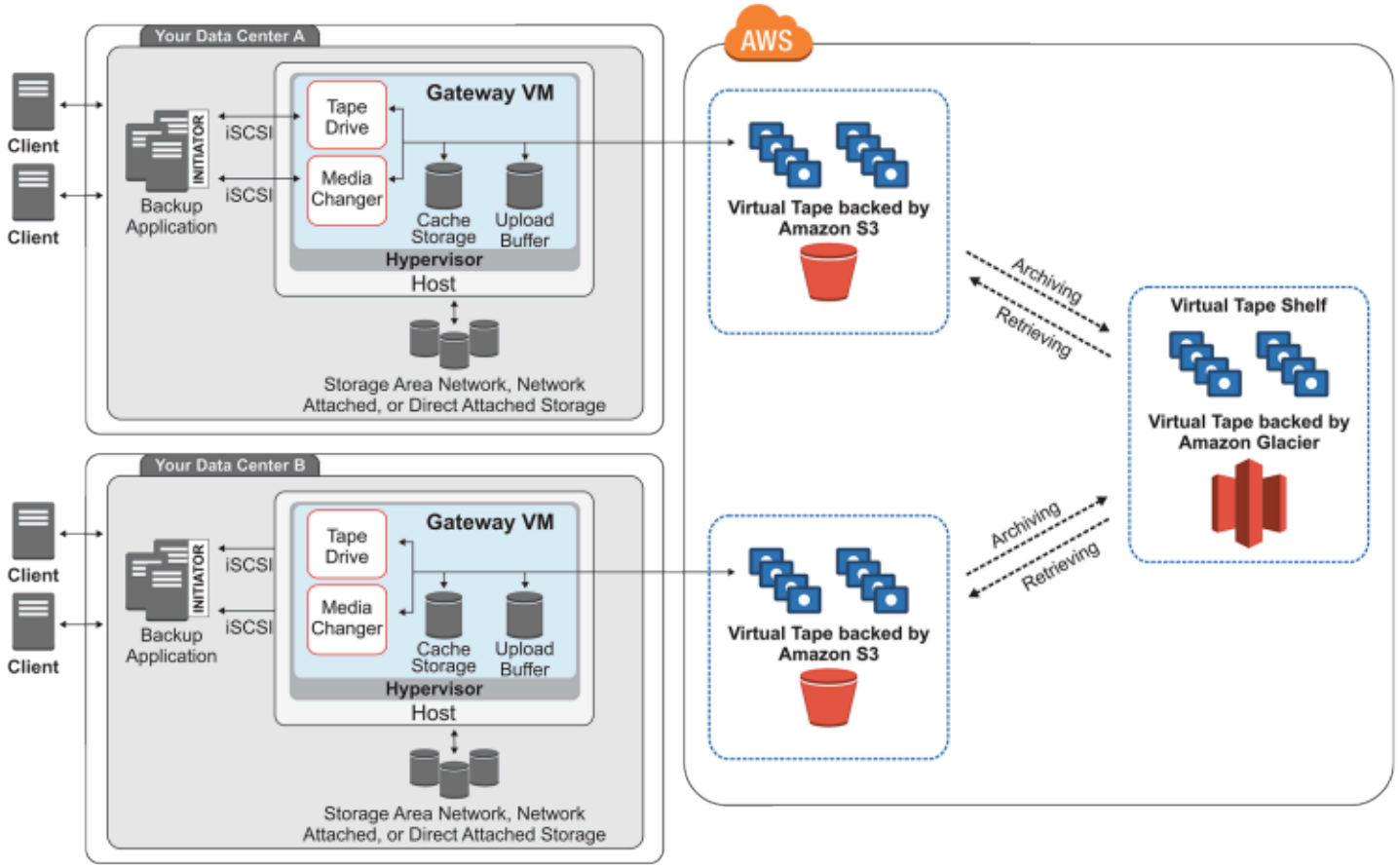
Im Folgenden finden Sie einen Überblick über die Architektur der Lösung für Tape Gateway.

Tape Gateways

Tape Gateway bietet eine zuverlässige, kostengünstige Lösung zum Archivieren von Daten in der Amazon Web Services Cloud. Mit seiner Virtual Tape Library (VTL)-Schnittstelle können Sie mit der vorhandenen Infrastruktur für bandbasierte Sicherungsanwendungen Daten auf virtuellen Bandkassetten speichern, die Sie auf Ihrem Tape Gateway erstellen. Jedes Tape Gateway ist mit

einem Medienwechsler und Bandlaufwerken vorkonfiguriert. Diese werden als iSCSI-Geräte für Ihre Client-Sicherungsanwendungen verfügbar gemacht. Bei Bedarf fügen Sie Bandkassetten zum Archivieren von Daten hinzu.

In dieser Abbildung finden Sie eine Übersicht über die Bereitstellung von Tape Gateway.



Das folgende Diagramm veranschaulicht die Komponenten von Tape Gateway:

- Virtuelles Band – Ein virtuelles Band entspricht einer physischen Bandkassette. Allerdings werden die Daten virtueller Bänder in der Amazon Web Services Cloud gespeichert. Wie bei physischen Bändern, können virtuelle Bänder leer sein oder Daten enthalten. Sie können virtuelle Bänder entweder in der Storage-Gateway-Konsole oder programmgesteuert über die Storage Gateway API erstellen. Jedes Gateway kann jeweils bis zu 1,500 Bänder oder 1 PiB an Banddaten insgesamt enthalten. Die Größe der virtuellen Bänder, die Sie beim Erstellen der Bänder konfigurieren können, liegt zwischen 100 GiB und 15 TiB.
- Virtual Tape Library (VTL) – Eine VTL ist vergleichbar mit einer lokal verfügbaren physischen Bandbibliothek mit automatischen Roboterarmen und Bandlaufwerken, einschließlich der Sammlung virtueller Bänder in der Bibliothek. Jedes Tape Gateway beinhaltet eine VTL.

Die virtuellen Bänder, die Sie erstellen, werden in der Gateway-VTL angezeigt. Bänder in der VTL werden von Amazon S3 gesichert. Wenn Ihre Sicherungssoftware Daten in das Gateway schreibt, speichert das Gateway diese Daten lokal und lädt sie asynchron auf virtuelle Bänder in Ihrer VTL – also Amazon S3 – hoch.

- Bandlaufwerk – Ein VTL-Bandlaufwerk entspricht einem physischen Bandlaufwerk, das E/A- und Suchoperationen auf einem Band ausführen kann. Jede VTL verfügt über eine Gruppe von 10 Bandlaufwerken, die für die Sicherungsanwendung als iSCSI-Geräte verfügbar sind.
- Medienwechsler – Ein VTL-Medienwechsler entspricht einem Roboter, der Bänder in den Speicherslots einer physischen Bandbibliothek und auf Bandlaufwerken verschiebt. Jede VTL verfügt über einen Medienwechsler, der für die Sicherungsanwendung als iSCSI-Gerät verfügbar ist.

- Archivierung – Ein Archiv entspricht einem externen Aufbewahrungsort für Bänder. Sie können Bänder aus der zu archivierenden VTL des Gateways archivieren und bei Bedarf Bänder aus dem Archiv in die Gateway-VTL abrufen.
  - Archivierung von Bändern – Wenn Ihre Sicherungssoftware ein Band auswirft, verschiebt das Gateways dieses Band in das Archiv, wo es langfristig gespeichert wird. Das Archiv befindet sich in der AWS -Region, in der Sie das Gateway aktiviert haben. Bänder im Archiv werden im virtuellen Bandregal (Virtual Tape Shelf, VTS) gespeichert. Das VTS wird von S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive gesichert, einem kostengünstigen Speicherservice für die Datenarchivierung, Sicherung und langfristige Aufbewahrung von Daten.
  - Abrufen von Bändern – Archivierte Bänder können nicht direkt gelesen werden. Wenn Sie ein archiviertes Band lesen möchten, müssen Sie es zuerst von Ihrem Tape Gateway abrufen. Hierzu verwenden Sie die Storage-Gateway-Konsole oder die Storage Gateway API.

  > **Important**
  >
  > Wenn Sie ein Band in „S3 Glacier Flexible Retrieval“ archivieren, können Sie das Band in der Regel innerhalb von 3 bis 5 Stunden abrufen. Wenn Sie das Band in „S3 Glacier Deep Archive“ archivieren, können Sie es in der Regel innerhalb von 12 Stunden abrufen.

Nachdem Sie ein Tape Gateway bereitgestellt und aktiviert haben, mounten Sie die virtuellen Bandlaufwerke und den Medienwechsler als iSCSI-Geräte auf Ihren lokalen Anwendungsservern. Sie erstellen virtuelle Bänder nach Bedarf und verwenden dann die

bestehende Sicherungssoftwareanwendung, um Daten auf die virtuellen Bänder zu schreiben. Der Medienwechsler lädt und entlädt die virtuellen Bänder für Lese- und Schreiboperationen in die virtuellen Bandlaufwerke.

Zuweisen von lokalen Datenträgern für die Gateway-VM

Die Gateway-VM benötigt lokale Datenträger, denen Sie die folgenden Zwecke zuweisen:

- Cache-Speicher – Der Cache-Speicher fungiert wie der dauerhafte Speicher für Daten, die vom Upload-Puffer aus in Amazon S3 hochgeladen werden sollen.

  Wenn Ihre Anwendung Daten von einem virtuellen Band liest, speichert das Gateway die Daten im Cache-Speicher. Das Gateway speichert die Daten, auf die zuletzt zugegriffen wurde, im Cache-Speicher, um einen schnellen Zugriff zu ermöglichen. Wenn Ihre Anwendung Banddaten anfordert, prüft das Gateway zunächst den Cache-Speicher auf die Daten, bevor die Daten von heruntergeladen werden AWS.
- Upload-Puffer – Der Upload-Puffer stellt einen Staging-Bereich für das Gateway bereit, bevor die Daten auf ein virtuelles Band geladen werden. Der Upload-Puffer ist ebenfalls wichtig für die Erstellung von Wiederherstellungspunkten, die Sie verwenden können, um Bänder nach unerwarteten Fehlern wiederherzustellen. Weitere Informationen finden Sie unter Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen..

Wenn die Sicherungsanwendung Daten auf das Gateway schreibt, kopiert das Gateway die Daten sowohl in den Cache-Speicher als auch in den Upload-Puffer. Erst danach wird die Schreiboperation gegenüber der Sicherungsanwendung bestätigt.

Richtlinien zur Bestimmung des Speicherplatzes, den Sie dem Cache-Speicher und dem Upload-Puffer zuweisen sollten, finden Sie unter Bestimmen der Größe des lokalen Festplattenspeichers.

Storage Gateway – Preisgestaltung

Aktuelle Informationen zu Preisen finden Sie unter Preise auf der AWS Storage Gateway Detailseite.

Planen Ihrer Storage-Gateway-Bereitstellung

Durch die Verwendung der Storage Gateway-Software-Appliance können Sie Ihre vorhandene On-Premises-Anwendungsinfrastruktur mit skalierbarem, kosteneffektivem AWS Cloud-Speicher verbinden, der Datensicherheitsfunktionen bereitstellt.

Bei der Bereitstellung einer Storage–Gateway-Lösung müssen Sie zunächst zwei Entscheidungen treffen:

1. Ihr Gateway-Typ – in diesem Handbuch wird der folgende Gateway-Typ behandelt:
   - Tape Gateway – Wenn Sie auf der Suche nach einer kostengünstigen, zuverlässigen, langfristigen, externen Alternative für die Datenarchivierung sind, können Sie ein Tape Gateway bereitstellen. Mit seiner Virtual Tape Library (VTL)-Schnittstelle können Sie mit der vorhandenen Infrastruktur für bandbasierte Sicherungsanwendungen Daten auf virtuellen Bandkassetten speichern, die Sie erstellen. Weitere Informationen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway. Wenn Sie Bänder archivieren, müssen Sie sich keine Gedanken über die Verwaltung der Bänder an Ihrem Standort machen oder ganze Stapel von Bändern extern lagern. Einen Überblick über die Architektur finden Sie unter So funktioniert Tape Gateway (Architektur).
2. Hosting-Option – Sie können Storage Gateway entweder On-Premises als VM-Appliance oder Hardware-Appliance oder in AWS als Amazon EC2 ausführen. Weitere Informationen finden Sie unter Voraussetzungen. Wenn Ihr Rechenzentrum ausfällt und Sie nicht über einen verfügbaren Host verfügen, können Sie ein Gateway auf einer EC2-Instance bereitstellen. Storage Gateway stellt ein Amazon Machine Image (AMI) mit dem Abbild der Gateway-VM bereit.

Da Sie außerdem eine Gateway-Software-Appliance auf einem Host konfigurieren, müssen Sie genügend Speicherplatz für die Gateway-VM bereitstellen.

Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie sicher, dass Sie die folgenden Schritte ausgeführt haben:

1. Wählen Sie für ein lokal bereitgestelltes Gateway den Typ des VM-Hosts aus und richten sie ihn ein. Ihre Optionen sind VMware ESXi Hypervisor, Microsoft Hyper-V und Linux Kernel-basierte virtuelle Maschine (KVM). Wenn Sie das Gateway hinter einer Firewall bereitstellen, sorgen Sie dafür, dass bestimmte Ports für die Gateway-VM geöffnet sind. Weitere Informationen finden Sie unter Voraussetzungen.
2. Installieren Sie Ihre Client-Backup-Software. Weitere Informationen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Erste Schritte

In diesem Abschnitt finden Sie Anweisungen zu den ersten Schritten mit Storage Gateway. Um zu beginnen, registrieren Sie sich zunächst bei AWS. Wenn Sie ein erstmaliger Benutzer sind, sollten Sie den Abschnitt über Regionen und Anforderungen lesen.

Themen

Registrieren für AWS Storage Gateway

Um Storage Gateway verwenden zu können, benötigen Sie ein Amazon-Web-Services-Konto, das Ihnen Zugriff auf alle AWS -Ressourcen, -Foren, -Supportleistungen und -Nutzungsberichte gewährt. Gebühren für die Services werden erst dann berechnet, wenn Sie sie nutzen. Wenn Sie bereits über ein Amazon-Web-Services-Konto verfügen, können Sie diesen Schritt überspringen.

So registrieren Sie sich für ein Amazon-Web-Services-Konto

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

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

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

Informationen zu den Preisen finden Sie unter Preise auf der Storage-Gateway-Detailseite.

AWS Regionen

Storage Gateway speichert Volume-, Snapshot-, Band- und Dateidaten in der AWS Region, in der Ihr Gateway aktiviert ist. Dateidaten werden in der - AWS Region gespeichert, in der sich Ihr Amazon S3-Bucket befindet. Sie wählen eine - AWS Region oben rechts in der Storage Gateway-Managementkonsole aus, bevor Sie mit der Bereitstellung Ihres Gateways beginnen.

- Storage Gateway – Unterstützte AWS Regionen und eine Liste der AWS Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente im Allgemeine AWS-Referenz.
- Storage Gateway-Hardware-Appliance – Informationen zu unterstützten AWS Regionen, die Sie mit der Hardware-Appliance verwenden können, finden Sie unter AWS Storage Gateway Hardware-Appliance-Regionen im Allgemeine AWS-Referenz.

Voraussetzungen

Sofern nicht anders angegeben gelten die folgenden Anforderungen für alle Gateway-Konfigurationen.

Themen

- Hardware- und Speicheranforderungen
- Netzwerk- und Firewall-Anforderungen
- Unterstützte Hypervisoren und Host-Anforderungen
- Unterstützte iSCSI-Initiatoren
- Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway

Hardware- und Speicheranforderungen

In diesem Abschnitt finden Sie Informationen zu den Mindesthardwareanforderungen für Ihr Gateway, den erforderlichen Einstellungen und der erforderlichen Mindestkapazität an Festplattenspeicherplatz, die als erforderlicher Speicher reserviert werden muss.

Hardwareanforderungen für VMs

Bei der Bereitstellung Ihres Gateways müssen Sie sicherstellen, dass die zugrunde liegende Hardware, auf der Sie die Gateway-VM bereitstellen, mindestens die folgenden Ressourcen reservieren kann:

- 4 virtuelle Prozessoren für die VM
- Für ein Tape Gateway sollte Ihre Hardware die folgenden RAM-Mengen reservieren:
  - 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
- 80 GiB Festplattenspeicher zur Installation des VM-Abbilds sowie für die Systemdaten

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

Anforderungen für Amazon-EC2-Instance-Typen

Wenn Sie Ihr Gateway in Amazon Elastic Compute Cloud (Amazon EC2) bereitstellen, müssen Sie als Instance-Größe mindestens xlarge auswählen, damit das Gateway funktioniert. Für die Instance-Familie, die für die Datenverarbeitung optimiert ist, muss die Größe jedoch mindestens 2xlarge sein.

Für Tape Gateway sollte Ihre Amazon EC2-Instance die folgenden RAM-Mengen bereitstellen, abhängig von der Cache-Größe, die Sie für Ihr Gateway verwenden möchten:

- 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

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

Empfohlen für zwischengespeicherte Volumes und Tape-Gateway-Typen

- Allzweck-Instance-Familie: Instance-Typ m4, m5 oder m6.

> **Note**
>
> Die Verwendung des Instance-Typs m4.16xlarge wird nicht empfohlen.

- Instance-Familie „Für Datenverarbeitung optimiert“: Instance-Typ c4, c5 oder c6. Wählen Sie die Instance-Größe 2xlarge oder höher aus, um die erforderlichen RAM-Anforderungen zu erfüllen.
- Speicheroptimierte Instance-Familie: Instance-Typ r3, r5 oder r6.
- Speicheroptimierte Instance-Familie: Instance-Typen i3 oder i4

Speicheranforderungen

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

In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt.

Gateway-Typ	Cache (Minimum)	Cache (Maximum)	Upload-Puffer (Minimum)	Upload-Puffer (Maximum)	Andere erforderliche lokale Festplatten
Tape Gateway	150 GiB	64 TiB	150 GiB	2 TiB	—

> **Note**
>
> Sie können ein oder mehrere lokale Laufwerke für Ihren Cache und Upload-Puffer konfigurieren, bis die maximale Kapazität erreicht ist.
> Wenn Sie einen Cache oder Upload-Puffer zu einem vorhandenen Gateway hinzufügen, müssen neue Festplatten auf Ihrem Host (Hypervisor oder Amazon-EC2-Instance) erstellt werden. Ändern Sie nicht die Größe von vorhandenen Datenträgern, wenn die Datenträger vorher bereits als Cache oder Upload-Puffer zugeordnet wurden.

Informationen zu Gateway-Kontingenten finden Sie unter AWS Storage Gateway -Kontingente.

Netzwerk- und Firewall-Anforderungen

Das Gateway muss unter anderem auf das Internet, lokale Netzwerke, DNS (Domain Name Service)-Server, Firewalls und Router zugreifen können. 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 Storage Gateway auf Amazon EC2 bereitstellen oder andere Bereitstellungstypen (einschließlich On-Premises) mit Netzwerksicherheitsrichtlinien verwenden, die AWS IP-Adressbereiche einschränken. In diesen Fällen kann es bei Ihrem Gateway zu Problemen mit der Serviceverbindung kommen, wenn sich die IP AWS -Bereichswerte ändern. Die Werte des AWS IP-Adressbereichs, die Sie verwenden müssen, befinden sich in der Amazon-Service-Untermenge 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.

> **Note**
>
> 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. In einigen Fällen können Sie Storage Gateway auf Amazon EC2 bereitstellen oder andere Bereitstellungstypen verwenden.

Themen

Port-Anforderungen

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

Allgemeine Ports für alle Gateway-Typen

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

Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
TCP	443 (HTTPS)	Ausgehend	Storage Gateway	AWS	Für die Kommunikation von Storage Gateway zum AWS Service-Endpunkt. Informationen über Service-Endpunkte finden Sie unter Zulassen des AWS Storage Gateway Zugriffs über Firewalls und Router.
TCP	80 (HTTP)	Eingehend	Der Host, von dem aus Sie eine	Storage Gateway	Durch lokale Systeme zum Abrufen

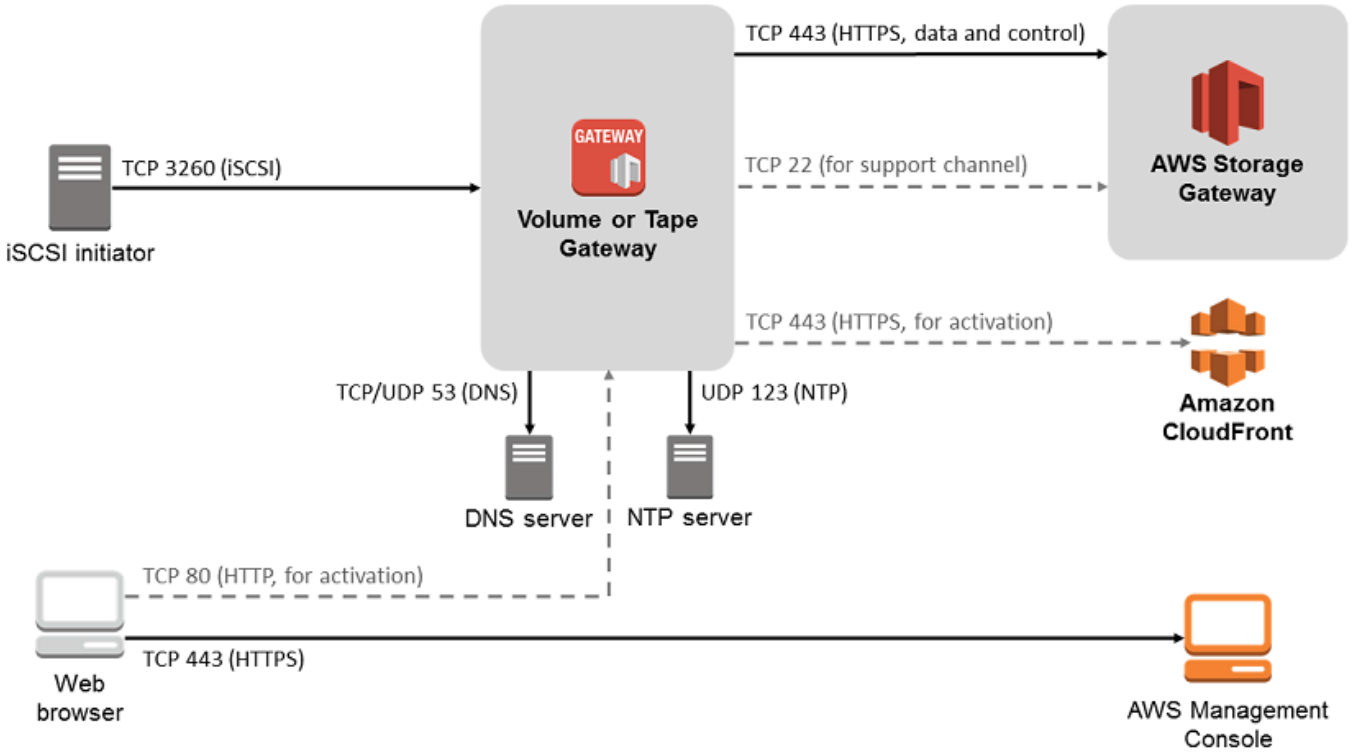
Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
			Verbindung zur - AWS Managementkonsole herstellen.		des Storage-Gateway-Aktivierungsschlüssels. Port 80 wird nur während der Aktivierung einer Storage Gateway-Appliance verwendet. Für Storage Gateway ist es nicht erforderlich, dass Port 80 öffentlich zugänglich ist. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie das Gateway von der Storage-Gateway-Managementkonsole aus

Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
					aktivieren, muss der Host, von dem aus Sie die Verbindung zur Konsole herstellen, Zugriff auf Port 80 des Gateways haben.
TCP/UDP	53 (DNS)	Ausgehend	Storage Gateway	Domain Name Service (DNS)-Server	Für die Kommunikation zwischen dem Storage Gateway und dem DNS-Server.

Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
TCP	22 (Support-Kanal)	Ausgehend	Storage Gateway	AWS Support	Ermöglicht AWS 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 Fehlerbeh ebung ist dies jedoch erforderlich.
UDP	123 (NTP)	Ausgehend	NTP-Client	NTP-Server	Verwendet von lokalen Systemen zur Synchroni sierung der VM-Zeit mit der Host-Zeit.

Ports für Volume Gateway und Tape Gateway

Die folgende Abbildung zeigt die Ports, die für das Tape Gateway offen sein müssen.



Neben den allgemeinen Ports benötigt ein Tape Gateway auch den folgenden Port.

Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
TCP	3260 (iSCSI)	Eingehend	iSCSI-Initiatoren	Storage Gateway	Durch lokale Systeme zum Herstellen einer Verbindung zu vom Gateway verfügbar gemachten iSCSI-Zielen.

Detaillierte Informationen zu den Port-Anforderungen finden Sie unter Port-Anforderungen im Abschnitt Zusätzliche Storage Gateway-Ressourcen.

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

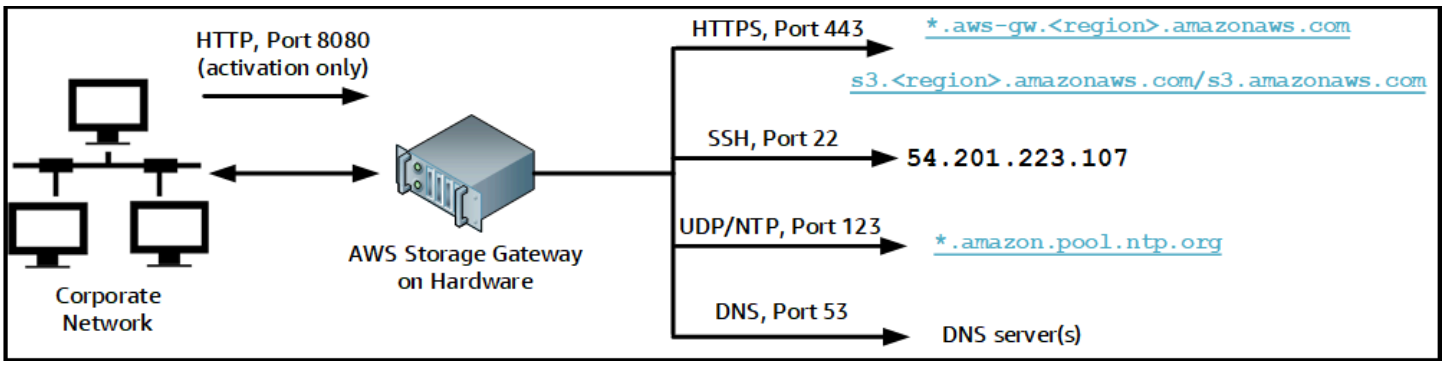
Jedes Storage-Gateway-Hardwaregerät benötigt die folgenden Netzwerkdienste:

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

Am Ende des Dell PowerEdge R640-Servers befinden sich fünf physische Netzwerkports. 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.

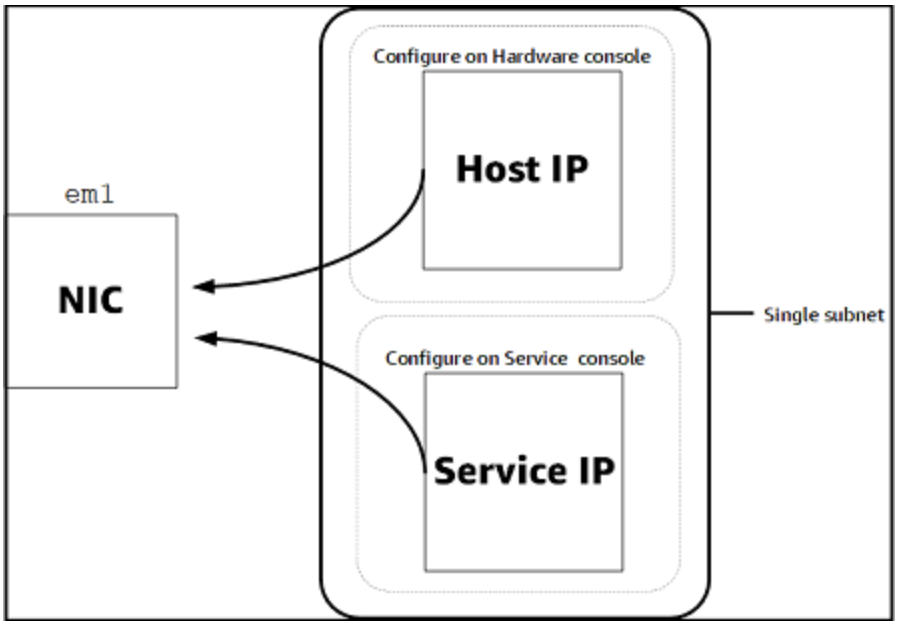
Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
SSH	22	Ausgehend	Hardware-Appliance	`54.201.223.107`	Support-Kanal
DNS	53	Ausgehend	Hardware-Appliance	DNS-Server	Namensauflösung
UDP/NTP	123	Ausgehend	Hardware-Appliance	`*.amazon.pool.ntp.org`	Zeitsynchronisierung
HTTPS	443	Ausgehend	Hardware-Appliance	`*.amazonaws.com`	Datenübertragung
HTTP	8080	Eingehend	AWS	Hardware-Appliance	Aktivierung (nur kurz)

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

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

> **Note**
>
> Eine Abbildung der Rückseite des Servers mit seinen Ports finden Sie unter Rackmontage Ihrer Hardware-Appliance und Anschluss an die Stromversorgung

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 unter Verwenden der Storage-Gateway-Hardware-Appliance.

Zulassen des AWS Storage Gateway Zugriffs über Firewalls und Router

Ihr Gateway benötigt Zugriff auf die folgenden Service-Endpunkte, um mit zu kommunizieren AWS. Falls Sie den Netzwerkdatenverkehr mithilfe einer Firewall oder eines Routers filtern oder einschränken, müssen Sie die Firewall oder 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 für die Verbindung und Datenübertragung zu und von 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 je nach AWS Region Ihres Gateways *Region* im Service-Endpunkt durch die richtige Regionszeichenfolge.

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

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

Die folgenden Service-Endpunkte sind für alle Gateways für Kontrollpfadoperationen (anon-cp, client-cp, proxy-app) und Datenpfadoperationen (dp-1) erforderlich:

```
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
```

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

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

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

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

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

Im Folgenden werden S3-Service-Endpunkte für AWS GovCloud (US) -Regionen aufgeführt.

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

Das folgende Beispiel ist ein FIPS-Service-Endpunkt für einen S3-Bucket in der Region AWS GovCloud (USA-West).

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

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

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

- Storage Gateway – Unterstützte AWS Regionen und eine Liste der AWS Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter -AWS Storage Gateway Endpunkte und -Kontingente im Allgemeine AWS-Referenz.
- Storage-Gateway-Hardware-Appliance – Informationen zu unterstützten AWS Regionen, die Sie mit der Hardware-Appliance verwenden können, finden Sie unter Storage Gateway-Hardware-Appliance-Regionen im Allgemeine AWS-Referenz.

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

Eine Sicherheitsgruppe steuert den Datenverkehr, der zu Ihrer Amazon-EC2-Gateway-Instance fließt. Wenn Sie eine Sicherheitsgruppe konfigurieren, empfehlen wir Folgendes:

- Die Sicherheitsgruppe sollte keine eingehenden Verbindungen aus dem externen Internet zulassen. Sie sollte festlegen, dass ausschließlich Instances innerhalb der Gateway-Sicherheitsgruppe mit dem Gateway kommunizieren dürfen. Müssen Instances von außerhalb der Gateway-Sicherheitsgruppe eine Verbindung mit dem Gateway herstellen, empfehlen wir, solche Verbindungen ausschließlich auf Port 3260 (iSCSI-Verbindungen) und Port 80 (Aktivierung) zuzulassen.
- Wenn Sie Ihr Gateway 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 Port 22 nur dann Zugriff, wenn Sie AWS Support für Fehlerbehebungszwecke verwenden. Weitere Informationen finden Sie unter Sie möchten AWS Support bei der Fehlerbehebung Ihres EC2-Gateways helfen.

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

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

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

Unterstützte Hypervisoren und Host-Anforderungen

Sie können Storage Gateway On-Premises entweder als Virtual Machine (VM)-Appliance oder als physische Hardware-Appliance oder in AWS als Amazon EC2-Instance ausführen.

> **Note**
>
> Wenn ein Hersteller die allgemeine Unterstützung für eine ESXi-Hypervisor-Version beendet, beendet Storage Gateway auch die Unterstützung für diese Version. Ausführliche Informationen zur Unterstützung bestimmter Versionen eines Hypervisors finden Sie in der Dokumentation des Herstellers.

Storage Gateway unterstützt die folgenden Hypervisor-Versionen und Hosts:

- VMware ESXi Hypervisor (Version 7.0 oder 8.0) – Eine kostenlose Version von VMware ist auf der VMware-Website verfügbar. Für diese Einrichtung benötigen Sie außerdem einen VMware vSphere-Client, um eine Verbindung mit dem Host herstellen zu können.
- Hypervisor Microsoft Hyper-V (Version 2012 R2, 2016, 2019 oder 2022): Eine kostenlose Standalone-Version von Hyper-V finden Sie im Microsoft Download Center. Um einen Microsoft Windows-basierten Client-Computer mit dem Host verbinden zu können, benötigen Sie für diese Einrichtung einen Microsoft Hyper-V-Manager.
- Linux Kernel-basierte virtuelle Maschine (KVM): Eine kostenlose Open-Source-Virtualisierungstechnologie. KVM ist in allen Versionen von Linux Version 2.6.20 und neuer enthalten. Storage Gateway wurde für die Distributionen CentOS/RHEL 7.7, Ubuntu 16.04 LTS und Ubuntu 18.04 LTS getestet und wird von diesen Distributionen unterstützt. Jede andere moderne Linux-Verteilung kann funktionieren, aber weder Funktion noch Leistung werden garantiert. Wir empfehlen diese Option, wenn Sie bereits über eine KVM-Umgebung verfügen und bereits mit der Funktionsweise von KVM vertraut sind.
- Amazon-EC2-Instance: Storage Gateway stellt ein Amazon Machine Image (AMI) mit dem Abbild der Gateway-VM bereit. In Amazon EC2 können ausschließlich Gateways vom Typ File Gateway, Gateway für zwischengespeicherte Volumes oder Tape Gateway bereitgestellt werden. Weitere Informationen zur Bereitstellung von Gateways in Amazon EC2 finden Sie unter Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Tape Gateway.
- Storage Gateway-Hardware-Appliance: Storage Gateway bietet eine physische Hardware-Appliance als On-Premises-Bereitstellungsoption für Standorte mit eingeschränkter Infrastruktur für virtuelle Maschinen.

> **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 iSCSI-Initiatoren

Wenn Sie ein Tape Gateway bereitstellen, ist das Gateway mit einem Medienwechsler und 10 Bandlaufwerken vorkonfiguriert. Diese Bandlaufwerke und der Medienwechsler werden als iSCSI-Geräte für Ihre Client-Sicherungsanwendungen verfügbar gemacht.

Zum Herstellen einer Verbindung mit diesen iSCSI-Geräten unterstützt Storage Gateway die folgenden iSCSI-Initiatoren:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- VNware ESX-Initiator (als Alternative zu den Initiatoren in den Gastbetriebssystemen Ihrer VMs)

> **Important**
>
> Storage Gateway bietet keine Unterstützung für Microsoft Multipfad-E/A (MPIO) über Windows-Clients.

Storage Gateway unterstützt jetzt Verbindungen zwischen mehreren Hosts und ein und demselben Volume, wenn die Hosts den Zugriff über Windows Server Failover Clustering (WSFC) koordinieren. Ohne WSFC ist es jedoch nicht möglich, mehrere Hosts mit dem gleichen Volume zu verbinden (z. B. Freigabe eines nicht geclusterten NTFS/ext4-Dateisystems).

Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway

Sie verwenden eine Sicherungsanwendung, um Bänder mit einem Tape Gateway zu lesen, auf die Bänder zu schreiben und sie zu verwalten. Die folgenden Sicherungsanwendungen von Drittanbietern werden für das Arbeiten mit Tape Gateways unterstützt.

Welchen Medienwechslertyp Sie wählen, hängt von der Sicherungsanwendung ab, die Sie verwenden möchten. In der folgenden Tabelle sind Sicherungsanwendungen von Drittanbietern aufgeführt, die getestet wurden und für kompatibel mit Tape Gateways befunden wurden. Diese Tabelle enthält den für jede Sicherungsanwendung empfohlenen Medienwechslertyp.

Sicherungsanwendung	Medienwechslertyp
Arcserve Backup	`AWS-Gateway-VTL`
Bacula Enterprise V10.x	`AWS-Gateway-VTL` oder `STK-L700`
Commvault V11	`STK-L700`
Dell EMC NetWorker 19.5	`AWS-Gateway-VTL`
IBM Spectrum Protect v8.1.10	`IBM-03584L32-0402`
Micro Focus (HPE) Data Protector 9 oder 11.x	`AWS-Gateway-VTL`
Microsoft System Center 2012 R2 oder 2016 Data Protection Manager	`STK-L700`
NovaStor DataCenter/Netzwerk 6.4 oder 7.1	`STK-L700`
Bol NetVault Backup 12.4 oder 13.x	`STK-L700`

Sicherungsanwendung	Medienwechslertyp
Veeam Backup & Replication 11A	`AWS-Gateway-VTL`
Veritas Backup Exec 2014 oder 15 oder 16 oder 20 oder 22.x	`AWS-Gateway-VTL`
Veritas Backup Exec 2012 **Note** Veritas unterstützt Backup Exec 2012 nicht mehr.	`STK-L700`
Ver Bols NetBackup Version 7.x oder 8.x	`AWS-Gateway-VTL`

Important

Wir empfehlen Ihnen dringend, den Medienwechsler zu wählen, der für Ihre Sicherungsanwendung aufgeführt ist. Andere Medienwechsler funktionieren möglicherweise nicht richtig. Sie können einen anderen Medienwechslertyp auswählen nachdem das Gateway aktiviert worden ist. Weitere Informationen finden Sie unter Auswählen eines Medienwechslers nach der Gateway-Aktivierung.

Zugriff auf AWS Storage Gateway

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

Um Browser-Zugriff auf die Storage-Gateway-Konsole zu ermöglichen, stellen Sie sicher, dass Ihr Browser Zugriff auf den Storage-Gateway-API-Endpunkt hat. Weitere Informationen finden Sie unter Storage-Gateway-Endpunkte und -Kontingente in der Allgemeinen AWS -Referenz.

Darüber hinaus können Sie die AWS Storage Gateway -API verwenden, um Ihre Gateways programmgesteuert zu konfigurieren und zu verwalten. Weitere Informationen zur API finden Sie unter API-Referenz für Storage Gateway.

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

Verwenden der Storage-Gateway-Hardware-Appliance

Die Storage-Gateway-Hardware-Appliance ist eine physische Hardware-Appliance mit vorinstallierter Storage-Gateway-Software auf einer validierten Serverkonfiguration. Sie können Ihre Hardware-Appliances auf der Seite Hardware-Appliance-Übersicht der Konsole von AWS Storage Gateway verwalten.

Bei der Hardware-Appliance handelt es sich um einen hochleistungsfähigen 1U-Server, den Sie in Ihrem Rechenzentrum oder On-Premises hinter Ihrer Unternehmens-Firewall bereitstellen können. Wenn Sie Ihre Hardware-Appliance kaufen und aktivieren, wird Ihre Hardware-Appliance während des Aktivierungsvorgangs mit Ihrem Amazon-Web-Services-Konto verknüpft. Nach der Aktivierung wird Ihre Hardware-Appliance in der Konsole auf der Seite Hardware-Appliance-Übersicht als Gateway angezeigt. Sie können Ihre Hardware-Appliance als File Gateway, Tape Gateway oder Volume Gateway konfigurieren. Das Verfahren, mit dem Sie die diese Gateway-Typen auf einer Hardware-Appliance bereitstellen und aktivieren, ist dasselbe wie auf einer virtuellen Plattform.

In den folgenden Abschnitten finden Sie Anweisungen zum Bestellen, Einrichten, Konfigurieren, Aktivieren, Starten und Verwenden einer Storage-Gateway-Hardware-Appliance.

Themen

Informationen zur Bestellung

Die AWS Storage Gateway Hardware-Appliance ist ausschließlich über Wiederverkäufer erhältlich. Bitte wenden Sie sich an Ihren bevorzugten Vertriebspartner, um Kaufinformationen zu erhalten und ein Angebot anzufordern.

Unterstützte Regionen AWS

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

Einrichten Ihrer Hardware-Appliance

Nachdem Sie Ihre Storage Gateway-Hardware-Appliance erhalten haben, verwenden Sie die Hardware-Appliance-Konsole, um das Netzwerk so zu konfigurieren, dass eine immer aktive Verbindung zu Ihrer Appliance hergestellt AWS und aktiviert wird. Durch die Aktivierung wird Ihre Appliance mit dem Amazon Web Services-Konto verknüpft, das während des Aktivierungsvorgangs verwendet wird. Nach der Aktivierung der Appliance können Sie in der Storage-Gateway-Konsole ein File, Volume oder Tape Gateway starten.

> **Note**
>
> Es liegt in Ihrer Verantwortung sicherzustellen, dass die Firmware der Hardware-Appliance ist up-to-date.

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 Rackmontage Ihrer Hardware-Appliance und Anschluss an die Stromversorgung.
2. Legen Sie die IPv4-Adressen für die Hardware-Appliance (den Host) und das Storage Gateway (den Service) fest. Weitere Informationen finden Sie unter Konfigurieren von Netzwerkparametern.

3. Aktivieren Sie die Hardware-Appliance auf der Übersichtsseite der Hardware-Appliance der Konsole in der AWS Region Ihrer Wahl. Weitere Informationen finden Sie unter Aktivieren Ihrer Hardware-Appliance.
4. Installieren Sie das Storage Gateway auf Ihrer Hardware-Appliance. Weitere Informationen finden Sie unter Konfigurieren Ihres Gateways.

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

Erweiterung des nutzbaren Cache-Speichers

Sie können den nutzbaren Speicher auf der Hardware-Appliance von 5 TB auf 12 TB erhöhen. Dies bietet einen größeren Cache für den Zugriff mit niedriger Latenz auf Daten in AWS. Wenn Sie das 5-TB-Modell bestellt haben, können Sie den nutzbaren Speicher auf 12 TB erhöhen, indem Sie fünf 1,92-TB-SSDs (Solid-State-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. Eine Anleitung hierfür erhalten Sie vom Amazon Web Services Support Support.
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 10G-Base-T-Kupfernetzwerkkarte oder einer 10G-DA/SFP+-Netzwerkkarte geliefert werden.

- 10G-Base-T-NIC-Konfiguration:
  - Verwenden Sie CAT6-Kabel für 10G oder CAT5 (e) für 1G
- 10G DA/SFP+ NIC-Konfiguration:
  - Verwenden Sie Twinax-Kupfer-Direktanschlusskabel bei einer Entfernung von bis zu 5 Metern
  - Dell/Intel-kompatible optische SFP+-Module (SR oder LR)
  - SFP/SFP+-Kupfer-Transceiver für 1G-Base-T oder 10G-Base-T

Rackmontage Ihrer Hardware-Appliance und Anschluss an die Stromversorgung

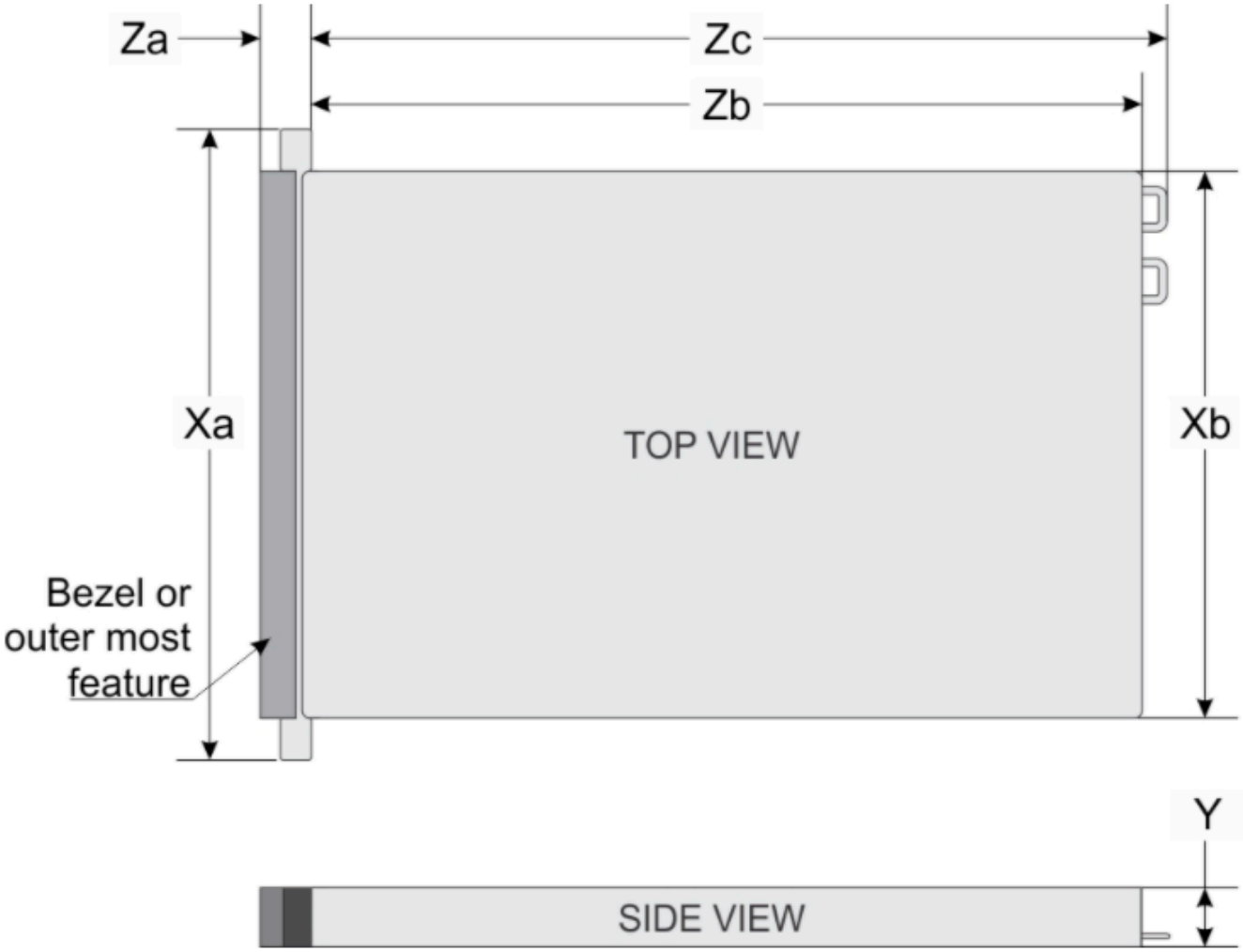
Folgen Sie nach dem Erhalt Ihrer Storage Gateway-Hardware-Appliance den im Lieferumfang enthaltenen Anleitungen für das Mounten des Servers im Rack. Bei Ihrer Appliance handelt es sich um einen 1U-Server, der in ein 19-Zoll-Rack nach dem International Electrotechnical Commission (IEC)-Branchenstandard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

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).

Abmessungen der Hardware-Appliance

Abmessungen der Hardware-Appliance einschließlich Halterungen und Blende.



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

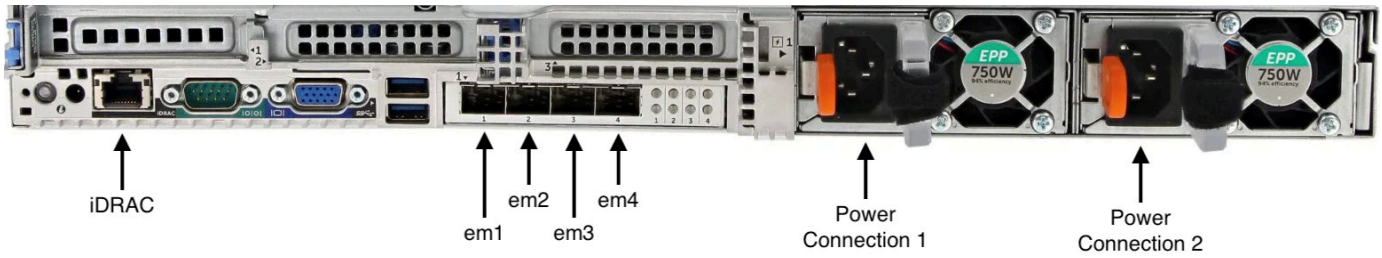
Abmessungen der Hardware-Appliance einschließlich Halterungen und Blende.

So schließen Sie die Hardware-Appliance an die Stromversorgung an

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

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

   Im folgenden Bild werden die verschiedenen Anschlüsse der Hardware-Appliance gezeigt.
   Rückseite der Hardware-Appliance mit Etiketten für Netzwerk- und Stromanschlüsse.

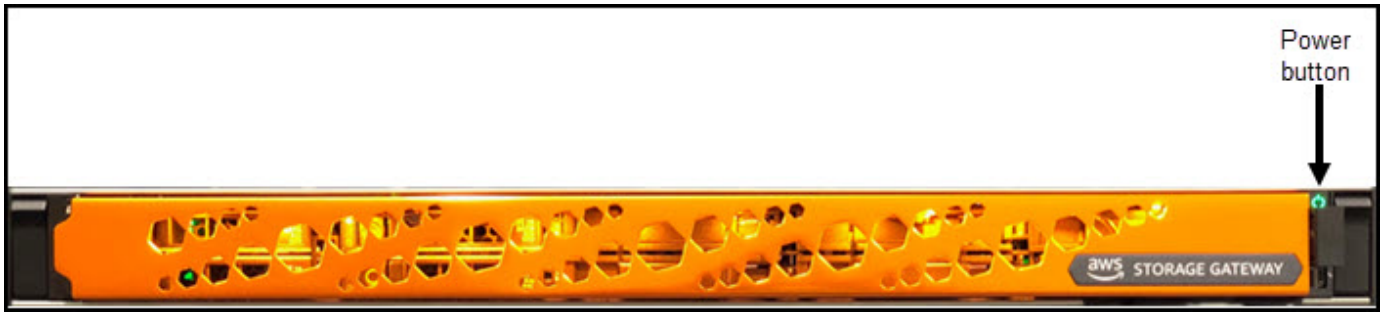
   

   Rückseite der Hardware-Appliance mit Etiketten für Netzwerk- und Stromanschlüsse.

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

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

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



Vorderseite der Hardware-Appliance mit Netzschalter-Etikett.

Nach dem Starten des Servers wird die Hardwarekonsole auf dem Monitor angezeigt. Die Hardwarekonsole bietet eine für spezifische Benutzeroberfläche AWS , mit der Sie anfängliche Netzwerkparameter konfigurieren können. Sie konfigurieren diese Parameter, um die Appliance mit AWS zu verbinden und einen Supportkanal zu öffnen, um eine Problembehebung durch den Amazon Web Services Support zu ermöglichen.

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

So legen Sie zum ersten Mal ein Passwort ein

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

Dialogfeld zur Einstellung des Passworts in der Hardware-Appliance-Konsole.

Dialogfeld zur Einstellung des Passworts in der Hardware-Appliance-Konsole.

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

Hauptmenü der Hardware-Appliance-Konsole mit Verbindungen und Menüoptionen.

Hauptmenü der Hardware-Appliance-Konsole mit Verbindungen und Menüoptionen.

Nächster Schritt

Konfigurieren von Netzwerkparametern

Konfigurieren von Netzwerkparametern

Nach dem Starten des Servers können Sie das erste Passwort in der Hardwarekonsole eingeben wie in Rackmontage Ihrer Hardware-Appliance und Anschluss an die Stromversorgung beschrieben.

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

So richten Sie eine Netzwerkadresse ein

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

Bildschirm „Netzwerk konfigurieren“ der Hardware-Appliance-Konsole.

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

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

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

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

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

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

> **Note**
>
> Wenn Sie eine andere Schnittstelle konfigurieren, muss diese dieselbe immer aktive Verbindung zu den in den Anforderungen aufgeführten AWS Endpunkten herstellen.

Bildschirm der Hardware-Appliance-Konsole zum Konfigurieren einer statischen IP für Netzwerkkarte.

Bildschirm der Hardware-Appliance-Konsole zum Konfigurieren einer statischen IP für Netzwerkkarte.

3. Geben Sie in Subnet (Subnetz) eine gültige Subnetzmaske ein und drücken Sie dann `Down arrow`.
4. Geben Sie in Gateway (Gateway) die IPv4-Adresse Ihres Netzwerk-Gateways ein und drücken Sie dann `Down arrow`.
5. Geben Sie in DNS1 die IPv4-Adresse für Ihren Domain Name Service (DNS)-Server ein und drücken Sie dann `Down arrow`.

6. (Optional) Geben Sie in DNS2 eine zweite IPv4-Adresse ein und drücken Sie dann `Down arrow`. Die Zuweisung eines zweiten DNS-Servers sorgt für zusätzliche Redundanz für den Fall, dass der erste DNS-Server nicht mehr verfügbar ist.
7. Wählen Sie Save (Speichern) aus und drücken Sie dann `Enter`, um Ihre Einstellung für eine statische IPv4-Adresse für die Appliance zu speichern.

So melden Sie sich von der Hardwarekonsole ab

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

Nächster Schritt

Aktivieren Ihrer Hardware-Appliance

Aktivieren Ihrer Hardware-Appliance

Nachdem Sie Ihre IP-Adresse konfiguriert haben, geben Sie diese IP-Adresse auf der Seite Hardware der AWS Storage Gateway Konsole ein, um Ihre Hardware-Appliance zu aktivieren. Während des Aktivierungsvorgangs wird überprüft, ob Ihre Hardware-Appliance die nötigen Sicherheitsanmeldeinformationen besitzt. Anschließend wird die Appliance in Ihrem AWS -Konto registriert.

Sie können Ihre Hardware-Appliance in jeder der unterstützten aktivieren AWS-Regionen. Eine Liste der AWS-Regionen unterstützten finden Sie unter Regionen der Storage Gateway-Hardware-Appliance im Allgemeine AWS-Referenz.

So aktivieren Sie Ihre Storage-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 eines Gateways

Erstellen eines Gateways

Sie können ein S3 File Gateway, FSx File Gateway, Tape Gateway oder Volume Gateway auf der Hardware-Appliance erstellen.

So erstellen Sie einen Gateway auf Ihrer Hardware-Appliance

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Storage Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie Hardware (Hardware) aus.
3. Wählen Sie die aktivierte Hardware-Appliance aus, auf der Sie Ihr Gateway erstellen möchten, und wählen Sie dann Gateway erstellen.
4. Folgen Sie den unter Erstellen Ihres Gateways beschriebenen Anweisungen, um den gewählten Gateway-Typ einzurichten, zu verbinden 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. Es kann 5–10 Minuten dauern, bis ein Gateway in der Konsole als online angezeigt wird.

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

Nächster Schritt

Konfigurieren einer IP-Adresse für das Gateway

Konfigurieren einer IP-Adresse für das Gateway

Bevor Sie Ihre Hardware-Appliance aktiviert haben, haben Sie ihrer physischen Netzwerkschnittstelle eine IP-Adresse zugewiesen. Nachdem Sie die Appliance aktiviert und Ihr Storage Gateway darauf gestartet haben, müssen Sie der virtuellen Storage Gateway-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 auf der lokalen Konsole des betreffenden Gateways. Ihre Anwendungen (wie Ihr NFS- oder SMB-Client, Ihr iSCSI-Initiator usw.) stellen Verbindungen mit dieser IP-Adresse her. Sie können über die Konsole der Hardware-Appliance auf die lokale Konsole des Gateways zugreifen.

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

1. Wählen Sie auf der Hardwarekonsole Open Service Console (Service-Konsole öffnen) aus, um einen Anmeldebildschirm für die lokale Konsole des Gateways zu öffnen.

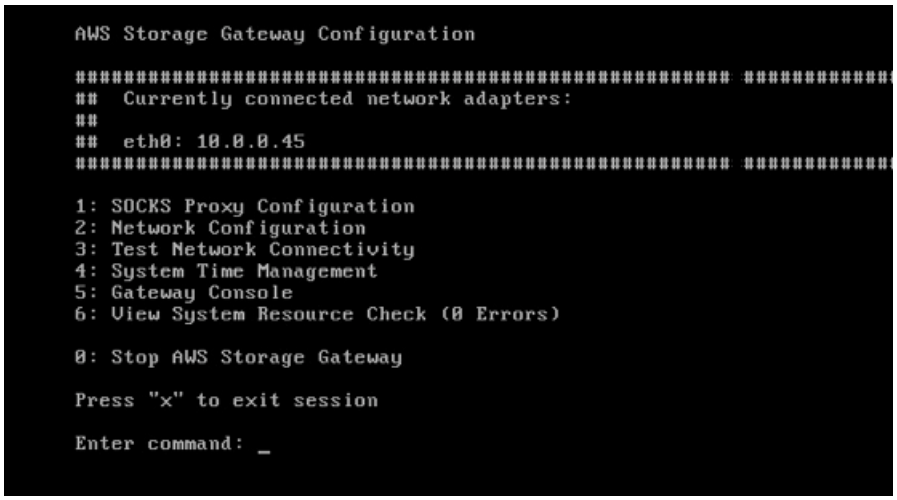
2. Geben Sie das localhost-Passwort in Login (Anmeldung) ein und drücken Sie anschließend `Enter`.

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

3. Ändern Sie das Standardpasswort. Wählen Sie Actions (Aktionen) und dann Set Local Password (Lokales Passwort festlegen) aus. Geben Sie dann die neuen Anmeldeinformationen in das Dialogfeld Set Local Password (Lokales Passwort festlegen) ein.

4. (Optional) Konfigurieren Sie die Proxyeinstellungen. Detaillierte Anweisungen finden Sie unter the section called “Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole”.

5. Navigieren Sie zur Seite „Network Settings (Netzwerkeinstellungen)“ der lokalen Konsole des Gateways wie im Folgenden gezeigt.
   Konfigurationsseite für die lokale Gateway-Konsole mit Optionen, einschließlich der Netzwerkkonfiguration.

   Konfigurationsseite für die lokale Gateway-Konsole mit Optionen, einschließlich der Netzwerkkonfiguration.

6. Geben Sie 2 ein, um zur Seite Network Configuration (Netzwerkkonfiguration) zu wechseln wie im Folgenden gezeigt.
   Seite „Netzwerkkonfiguration“ für die lokale Gateway-Konsole mit DHCP- und statischen IP-Optionen.

Seite „Netzwerkkonfiguration“ für die lokale Gateway-Konsole mit DHCP- und statischen IP-Optionen.

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

So verlassen Sie die lokale Konsole des Gateways

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

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

Nächster Schritt

Konfigurieren Ihres Gateways

Konfigurieren Ihres Gateways

Mach der Aktivierung und Konfigurierung Ihrer Hardware-Appliance wird Ihre Appliance in der Konsole angezeigt. Nun können Sie den gewünschten Gateway-Typ konfigurieren. Setzen Sie die Installation auf der Seite Gateway konfigurieren für Ihren Gateway-Typ fort. Anweisungen finden Sie unter Konfigurieren Ihres Tape Gateways.

Entfernen eines Gateways von einer Hardware-Appliance

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

So entfernen Sie einen Gateway von einer Hardware-Appliance

1. Wählen Sie auf der Seite Hardware der Storage-Gateway-Konsole die Hardware-Appliance aus, die Sie löschen möchten.
2. Wählen Sie für Actions (Aktionen) die Option Remove Gateway (Gateway entfernen). Das Bestätigungsdialogfeld wird angezeigt.
3. Vergewissern Sie sich, dass Sie die Gateway-Software von der angegebenen Hardware-Appliance entfernen möchten, geben Sie dann das Wort entfernen in das Bestätigungsfeld ein und wählen Sie Entfernen aus.

> **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 des Gateways über die AWS Storage Gateway -Konsole und Bereinigen zugehöriger Ressourcen.

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

Löschen Ihrer Hardware-Appliance

Wenn Sie eine Storage 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 in ein anderes AWS Konto oder zu verschieben AWS-Region, müssen Sie sie zunächst mit dem folgenden Verfahren löschen, dann den Support-Kanal des Gateways öffnen und sich an wenden, AWS Support um einen Soft Reset durchzuführen. Weitere

Informationen finden Sie unter Aktivieren des AWS Support Zugriffs, um Probleme mit Ihrem lokal 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 Entfernen eines Gateways von einer Hardware-Appliance.
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 eines Gateways

Die Übersichtsthemen auf dieser Seite geben eine Übersicht darüber, wie der Erstellungsprozess von Storage Gateway funktioniert. step-by-step Verfahren zum Erstellen eines bestimmten Gateway-Typs mithilfe der Storage Gateway-Konsole finden Sie unter Erstellen eines Tape Gateways .

Überblick – Gateway-Aktivierung

Bei der Gateway-Aktivierung müssen Sie Ihr Gateway einrichten, es mit verbinden AWS, dann Ihre Einstellungen überprüfen und aktivieren.

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 bereitstellen, die Sie von Ihrem bevorzugten Konnektor oder als Amazon EC2-Instance in Ihrer AWS Cloud-Umgebung bestellen. 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 AWS Services 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 Amazon CloudWatch Logs und CloudWatch Alarmen zu überwachen, und fügen bei Bedarf Tags hinzu, um das Gateway leichter identifizieren zu können. 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 nachdem, welchen Gateway-Typ Sie erstellt haben, verwenden Sie die Storage-Gateway-Konsole, um Volumes, Bänder oder Amazon S3- oder Amazon FSx-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 eines Tape Gateways

In diesem Abschnitt finden Sie Anweisungen zum Erstellen und Nutzen eines Tape Gateways in AWS Storage Gateway.

Themen

- Erstellen eines Gateways
- Erstellen eines benutzerdefinierten Bandpools
- Erstellen von Bändern
- Verwenden von Tape Gateway

Erstellen eines Gateways

In diesem Abschnitt finden Sie Anweisungen zum Herunterladen, Bereitstellen und Aktivieren eines Standard-Tape Gateways.

Themen

Einrichten eines Tape Gateways

So richten Sie ein neues Tape Gateway ein

1. Öffnen Sie die AWS Management Console unter https://console.aws.amazon.com/storagegateway/home/ und wählen Sie die aus, AWS-Region in der 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. Sie können nach diesem Namen suchen, um Ihr Gateway auf Listenseiten in der 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 die Option Tape 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, und folgen Sie dann den plattformspezifischen Anweisungen auf der Storage-Gateway-Konsolenseite, um Ihre Host-Plattform einzurichten. Sie können aus den folgenden Optionen auswählen:
        - VMware ESXi – Laden Sie die virtuelle Gateway-Maschine mit VMware ESXi herunter, stellen Sie sie bereit und konfigurieren Sie sie.

- Microsoft Hyper-V – Laden Sie die virtuelle Gateway-Maschine mit Microsoft Hyper-V herunter, stellen Sie sie bereit und konfigurieren Sie sie.
- Linux KVM – Laden Sie die virtuelle Gateway-Maschine mit Linux KVM herunter, stellen Sie sie bereit und konfigurieren Sie sie.
- Amazon EC2 – Konfigurieren und starten Sie eine Amazon-EC2-Instance zum Hosten Ihres Gateways. Diese Option ist für Stored Volume-Gateways nicht verfügbar.
- Hardware-Appliance – Bestellen Sie eine dedizierte physische Hardware-Appliance von AWS , um Ihr 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. Wählen Sie im Abschnitt Sicherungsanwendungseinstellungen für Backup-Anwendung die Anwendung aus, mit der Sie Ihre Banddaten auf den virtuellen Bändern sichern möchten, die Ihrem Tape Gateway zugeordnet sind.
7. Wählen Sie Weiter aus, um fortzufahren.

Nachdem Ihr Gateway eingerichtet ist, müssen Sie auswählen, wie es eine Verbindung herstellen und mit kommunizieren soll AWS. Anweisungen finden Sie unter Verbinden Ihres Tape Gateways mit AWS.

Verbinden Sie Ihr Tape Gateway mit AWS

So verbinden Sie ein neues Tape Gateway mit AWS

1. Detaillierte Anweisungen finden Sie unter Erstellen von Bändern. Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Verbinden mit AWS in der Storage-Gateway-Konsole zu öffnen.
2. Wählen Sie im Abschnitt Endpunktoptionen für Service-Endpunkt den Endpunkttyp aus, den Ihr Gateway für die Kommunikation mit verwendet AWS. Sie können aus den folgenden Optionen auswählen:

   - Öffentlich zugänglich – Ihr Gateway kommuniziert mit 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 soll.

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

- VPC-gehostet – Ihr Gateway kommuniziert mit AWS über eine private Verbindung mit Ihrer 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 dem Dropdown-Menü auswählen oder indem Sie den DNS-Namen oder die IP-Adresse des VPC-Endpunkts 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 auswählen:

   - 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. Wählen Sie diese Option, wenn die IP-Adresse Ihres Gateways nicht verfügbar ist.

4. Wählen Sie Weiter aus, um fortzufahren.

Nachdem Sie nun ausgewählt haben, wie Ihr Gateway eine Verbindung zu herstellen soll AWS, müssen Sie das Gateway aktivieren. Anweisungen finden Sie unter Überprüfen von Einstellungen und Aktivieren Ihres Tape Gateways.

Überprüfen von Einstellungen und Aktivieren Ihres Tape Gateways

So aktivieren Sie ein neues Tape Gateway

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

   - Einrichten eines Tape Gateways
   - Verbinden Sie Ihr Tape Gateway mit AWS

   Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Überprüfen und Aktivieren in der 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.

   > **Note**
   >
   > Sie können die Gateway-Optionen oder Verbindungseinstellungen nicht ändern, nachdem Ihr Gateway aktiviert wurde.
4. Wählen Sie Gateway aktivieren, um fortzufahren.

Nachdem Sie Ihr Gateway aktiviert haben, müssen Sie die Erstkonfiguration durchführen, um lokale Speicherfestplatten zuzuweisen und die Protokollierung zu konfigurieren. Anweisungen finden Sie unter Konfigurieren Ihres Tape Gateways mit .

Konfigurieren von Tape Gateway

So führen Sie die Erstkonfiguration auf einem neuen Tape Gateway durch

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

   - Einrichten eines Tape Gateways
   - Verbinden Sie Ihr Tape Gateway mit AWS
   - Überprüfen von Einstellungen und Aktivieren Ihres Tape Gateways

Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Gateway konfigurieren in der Storage-Gateway-Konsole zu öffnen.

2. Verwenden Sie im Abschnitt Speicher konfigurieren die Dropdownmenüs, um mindestens eine Festplatte mit mindestens 165 GiB Kapazität für CACHE STORAGE und mindestens eine Festplatte mit mindestens 150 GiB Kapazität für UPLOAD BUFFER 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 Sie Amazon CloudWatch Logs einrichten, um den Zustand Ihres Gateways zu überwachen. Sie können aus den folgenden Optionen auswählen:

   - 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 dem entsprechenden Dropdown-Menü aus.
   - Protokollierung deaktivieren – Verwenden Sie Amazon CloudWatch Logs nicht, um Ihr Gateway zu überwachen.
4. Wählen Sie im Abschnitt CloudWatch Alarme aus, wie Sie Amazon- CloudWatch Alarme einrichten, um Sie zu benachrichtigen, wenn Gateway-Metriken von den definierten Grenzwerten abweichen. Sie können aus den folgenden Optionen auswählen:

   - Empfohlene Alarme von Storage Gateway erstellen – Erstellen Sie alle empfohlenen CloudWatch Alarme automatisch, wenn das Gateway erstellt wird. Weitere Informationen zu empfohlenen Alarmen finden Sie unter Grundlegendes zu CloudWatch Alarmen.

     > **Note**
     >
     > Diese Funktion erfordert CloudWatch Richtlinienberechtigungen, die nicht automatisch als Teil der vorkonfigurierten Storage 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 deaktiveren
     > - `cloudwatch:EnableAlarmActions` – Alarmaktionen aktiveren

- `cloudwatch:DeleteAlarms` - Alarme löschen

- Erstellen eines benutzerdefinierten Alarms – Konfigurieren Sie einen neuen CloudWatch Alarm, um Sie über die Metriken Ihres Gateways zu informieren. Wählen Sie Alarm erstellen, um Metriken zu definieren und Alarmaktionen in der Amazon- CloudWatch Konsole anzugeben. Anweisungen finden Sie unter Verwenden von Amazon- CloudWatch Alarmen im Amazon- CloudWatch Benutzerhandbuch.
- Kein Alarm – Erhalten Sie keine CloudWatch Benachrichtigungen über die Metriken Ihres Gateways.

5. (Optional) Wählen Sie im Abschnitt Tags die Option Neues Tag hinzufügen und geben Sie dann ein Schlüssel-Wert-Paar ein, bei dem Groß- und Kleinschreibung beachtet wird, damit Sie auf Listenseiten in der Storage-Gateway-Konsole nach Ihrem Gateway suchen und filtern können. Wiederholen Sie diesen Schritt, um bei Bedarf weitere Tags hinzuzufügen.
6. Wählen Sie Konfigurieren, um die Erstellung Ihres Gateways abzuschließen.

   Um den Status Ihres neuen Gateways zu überprüfen, suchen Sie danach auf der Seite Gateway-Übersicht des Storage Gateways.

Nachdem Sie Ihr Gateway erstellt haben, müssen Sie virtuelle Bänder erstellen, damit es verwendet werden kann. Detaillierte Anweisungen finden Sie unter Erstellen von Bändern.

Erstellen eines benutzerdefinierten Bandpools

In diesem Abschnitt wird beschrieben, wie ein neuer benutzerdefinierter Bandpool in AWS Storage Gateway erstellt wird.

Themen

Auswahl eines Bandpool-Typs

AWS Storage Gateway verwendet Bandpools, um die Speicherklasse zu bestimmen, in der Bänder archiviert werden sollen, wenn sie ausgeworfen werden. Storage Gateway bietet zwei Standard-Bandpools:

- Glacier Pool – Archiviert das Band in der Speicherklasse S3 Glacier Flexible Retrieval. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in S3 Glacier Flexible Retrieval archiviert. S3 Glacier Flexible Retrieval wird für aktivere Archive verwendet, sodass Sie die Bänder in der Regel innerhalb von 3 bis 5 Stunden abrufen können. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für Amazon Simple Storage Service.
- Deep Archive Pool – Archiviert das Band in der S3 Glacier Deep Archive Archive-Speicherklasse. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in S3 Glacier Deep Archive archiviert. S3 Glacier Deep Archive wird für die langfristige Datenaufbewahrung und zur Erhaltung digitaler Daten verwendet, wo ein Zugriff nur ein- oder zweimal im Jahr erfolgt. Sie können in S3 Glacier Deep Archive archivierte Bänder in der Regel innerhalb von 12 Stunden abrufen. Ausführliche Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Amazon Simple Storage Service-Benutzerhandbuch.

Sie können die in S3 Glacier Flexible Retrieval archivierten Bänder zu einem späteren Zeitpunkt zu S3 Glacier Deep Archive verschieben. Weitere Informationen finden Sie unter Verschieben eines Bands von der Speicherklasse „S3 Glacier Flexible Retrieval“ zur Speicherklasse „S3 Glacier Deep Archive“.

Storage Gateway unterstützt auch die Erstellung benutzerdefinierter Bandpools, mit denen Sie die Bandaufbewahrungssperre aktivieren können, um zu verhindern, dass archivierte Bänder für einen festgelegten Zeitraum, bis zu 100 Jahre, gelöscht oder in einen anderen Pool verschoben werden. Dazu gehören Sperren von Zugriffsrechten, die festlegen, wer Bänder löschen oder Aufbewahrungseinstellungen ändern kann.

Verwenden der Bandaufbewahrungssperre

Mit der Bandaufbewahrungssperre können Sie archivierte Bänder sperren. Die Bandaufbewahrungssperre ist eine Option für Bänder in einem benutzerdefinierten Bandpool. Bänder, bei denen die Bandaufbewahrungssperre aktiviert ist, können für einen festgelegten Zeitraum, bis zu 100 Jahre, nicht gelöscht oder in einen anderen Pool verschoben werden.

Sie können die Bandaufbewahrungssperre in einem von zwei Modi konfigurieren:

- Governance-Modus – Wenn im Governance-Modus konfiguriert, `storagegateway:BypassGovernanceRetention` können nur AWS Identity and Access Management (IAM)-Benutzer mit den Berechtigungen zum Ausführen von Bänder aus dem Pool

entfernen. Wenn Sie die AWS Storage Gateway -API zum Entfernen des Bands verwenden, müssen Sie auch `BypassGovernanceRetention` auf setzen`true`.

- Compliance-Modus – Wenn der Schutz im Compliance-Modus konfiguriert ist, kann er von keinem Benutzer entfernt werden, auch nicht vom AWS-Konto-Root-Benutzer.

  Wenn ein Objekt im Compliance-Modus gesperrt wurde, können der Aufbewahrungsmodus nicht geändert und der Aufbewahrungszeitraum nicht verkürzt werden. Der Compliance-Modus stellt sicher, dass eine Objektversion während des Aufbewahrungszeitraums weder überschrieben noch gelöscht werden.

> **Important**
>
> Die Konfiguration eines benutzerdefinierten Pools kann nach seiner Erstellung nicht mehr geändert werden.

Sie können die Bandsperre aktivieren, wenn Sie einen benutzerdefinierten Bandpool erstellen. Alle neuen Bänder, die an einen benutzerdefinierten Pool angeschlossen werden, übernehmen den Typ, den Zeitraum und die Speicherklasse der Aufbewahrungssperre für diesen Pool.

Sie können die Bandaufbewahrungssperre auch für Bänder aktivieren, die vor der Veröffentlichung dieses Features archiviert wurden, indem Sie Bänder zwischen dem Standardpool und einem von Ihnen erstellten benutzerdefinierten Pool verschieben. Wenn das Band archiviert ist, ist die Bandaufbewahrungssperre sofort wirksam.

> **Note**
>
> Wenn Sie archivierte Bänder zwischen den Speicherklassen S3 Glacier Flexible Retrieval und S3 Glacier Deep Archive verschieben, wird Ihnen eine Gebühr für das Verschieben eines Bandes berechnet. Für das Verschieben eines Bandes von einem Standard-Pool in einen benutzerdefinierten Pool fallen keine zusätzlichen Gebühren an, sofern die Speicherklasse gleich bleibt.

Erstellen eines benutzerdefinierten Bandpools

Führen Sie die folgenden Schritte aus, um mithilfe der AWS Storage Gateway -Konsole einen benutzerdefinierten Bandpool zu erstellen.

So erstellen Sie einen benutzerdefinierten Bandpool

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Bandbibliothek und danach die Registerkarte Pools.
3. Wählen Sie Pool erstellen aus, um den Bereich Pool erstellen zu öffnen.
4. Geben Sie unter Name einen eindeutigen Namen ein, um Ihren benutzerdefinierten Bandpool zu identifizieren. Der Name muss zwischen 3 und 100 Zeichen lang sein.
5. Wählen Sie als Speicherklasse Glacier oder Glacier Deep Archive.
6. Wählen Sie für den Aufbewahrungssperrtyp die Option Keine, Compliance oder Governance aus.

   > **Note**
   >
   > Wenn Sie Compliance wählen, kann die Bandaufbewahrungssperre von keinem Benutzer entfernt werden, auch nicht vom AWS-Konto-Root-Benutzer.

7. Wenn Sie sich für eine Bandaufbewahrungssperre entscheiden, geben Sie den Aufbewahrungszeitraum in Tagen ein. Die maximale Aufbewahrungsfrist beträgt 100 Jahre.
8. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um Ihrem benutzerdefinierten Bandpool ein Tag hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen benutzerdefinierter Bandpools erleichtert.

   Geben Sie einen Schlüssel und optional einen Wert für das Tag ein. Sie können dem Bandpool bis zu 50 Tags hinzufügen.
9. Wählen Sie Pool erstellen aus, um Ihren neuen benutzerdefinierten Bandpool zu erstellen.

Erstellen von Bändern

In diesem Abschnitt wird beschrieben, wie Sie neue virtuelle Bänder mit AWS Storage Gateway erstellen. Sie können neue virtuelle Bänder entweder über die AWS Storage Gateway Konsole oder die Storage Gateway-API manuell erstellen. Sie können Ihr Tape Gateway auch so konfigurieren, dass sie automatisch erstellt werden. Dadurch können der Bedarf an manueller Bandverwaltung reduziert, Ihre großen Bereitstellungen vereinfacht und der Bedarf an On-Premises-Speicher und Archivspeicher besser skaliert werden.

Tape Gateway unterstützt WORM (Write Once, Read Many) und Bandaufbewahrungssperre bei virtuellen Bändern. Durch WORM-aktivierte virtuelle Bänder wird sichergestellt, dass die Daten auf aktiven Bändern in Ihrer virtuellen Bandbibliothek nicht überschrieben oder gelöscht werden können. Weitere Informationen zum WORM-Schutz für virtuelle Bänder finden Sie im folgenden Abschnitt the section called “WORM-Bandschutz”.

Mit der Bandaufbewahrungssperre können Sie den Aufbewahrungsmodus und den Aufbewahrungszeitraum für archivierte virtuelle Bänder festlegen und so verhindern, dass diese in einem festen Zeitraum von bis zu 100 Jahren gelöscht werden. Dazu gehören Berechtigungen, die festlegen, wer Bänder löschen oder Aufbewahrungseinstellungen ändern kann. Weitere Informationen zur Bandaufbewahrungssperre finden Sie unter the section called “Bandaufbewahrungssperre”.

> **Note**
>
> Sie zahlen nur für die Datenmenge, die Sie auf das Band schreiben, nicht für die Bandkapazität.
> Sie können AWS Key Management Service (AWS KMS) verwenden, um Daten zu verschlüsseln, die auf ein virtuelles Band geschrieben wurden, das in Amazon Simple Storage Service (Amazon S3) gespeichert ist. Derzeit können Sie dies über die AWS Storage Gateway -API oder AWS Command Line Interface () tun AWS CLI. Weitere Informationen finden Sie unter CreateTapes oder create-tapes.

Themen

WORM-Bandschutz (Write Once, Read Many)

Sie können verhindern, dass virtuelle Bänder überschrieben oder gelöscht werden, indem Sie den WORM-Schutz für virtuelle Bänder in AWS Storage Gateway aktivieren. Der WORM-Schutz für virtuelle Bänder wird beim Erstellen von Bändern aktiviert.

Daten, die auf virtuelle WORM-Bänder geschrieben wurden, können nicht überschrieben werden. Es können nur neue Daten an virtuelle WORM-Bänder angehängt werden, doch bestehende Daten

können nicht gelöscht werden. Die Aktivierung des WORM-Schutzes für virtuelle Bänder hilft, diese Bänder während ihrer aktiven Nutzung zu schützen, bevor sie ausgeworfen und archiviert werden.

Die WORM-Konfiguration kann nur bei der Erstellung von Bändern festgelegt werden, und diese Konfiguration kann nach der Erstellung der Bänder nicht mehr geändert werden.

Manuelles Erstellen von Bändern

Sie können neue virtuelle Bänder entweder über die AWS Storage Gateway Konsole oder die Storage Gateway-API manuell erstellen. Die Konsole bietet eine praktische Oberfläche für die Erstellung von Bändern mit der Flexibilität, ein Präfix für einen zufällig generierten Band-Barcode anzugeben. Wenn Sie Ihre Band-Barcodes vollständig anpassen müssen (z. B. damit sie mit der Seriennummer eines entsprechenden physischen Bandes übereinstimmen), müssen Sie die API verwenden. Weitere Informationen zum Erstellen von Bändern mit der Storage Gateway-API finden Sie unter CreateTapeWithBarcode in der Storage Gateway-API-Referenz.

So erstellen Sie virtuelle Bänder über die Storage-Gateway-Konsole

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.
3. Wählen Sie Bänder erstellen aus, um den Bereich Bänder erstellen zu öffnen.
4. Wählen Sie in Gateway (Gateway) einen Gateway aus. Das Band wird für dieses Gateway erstellt.
5. Wählen Sie als Bandtyp die Option Standard aus, um virtuelle Standardbänder zu erstellen. Wählen Sie WORM aus, um virtuelle WORM-Bänder (Write Once, Read Many) zu erstellen.
6. Wählen Sie unter Number of tapes (Anzahl der Bänder) die Anzahl der Bänder aus, die Sie erstellen möchten. Weitere Hinweise zu Bandkontingenten finden Sie unter AWS Storage Gateway -Kontingente.
7. Geben Sie unter Capacity (Kapazität) die Größe des virtuellen Bandes ein, das Sie erstellen möchten. Bänder müssen größer als 100 GiB sein. Hinweise zu Kapazitätskontingenten finden Sie unter AWS Storage Gateway -Kontingente.
8. Geben Sie in Barcode-Präfix das Präfix an, das dem Barcode virtueller Bänder vorangestellt werden soll.

> **Note**
>
> Virtuelle Bänder werden durch einen Barcode eindeutig identifiziert und Sie können diesem ein Präfix hinzufügen. Sie können ein Präfix angeben, um Ihre virtuellen Bänder leichter identifizieren zu können. Das Präfix muss aus Großbuchstaben (A-Z) bestehen und ein bis vier Zeichen lang sein.

9. Wählen Sie für Pool Glacier Pool, Deep Archive Pool oder einen benutzerdefinierten Pool aus, den Sie erstellt haben. Dieser Pool bestimmt die Speicherklasse, in der Ihr Band gespeichert wird, wenn es von Ihrer Sicherungssoftware ausgeworfen wird.

   - Wählen Sie Glacier Pool aus, wenn das Band in der Speicherklasse „S3 Glacier Flexible Retrieval“ gespeichert werden soll. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Flexible Retrieval“ archiviert. Sie verwenden „S3 Glacier Flexible Retrieval“ für aktivere Archive, aus denen Sie ein Band in der Regel innerhalb von 3 bis 5 Stunden abrufen können. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.
   - Wählen Sie Deep Archive Pool aus, wenn Sie das Band in der Speicherklasse „S3 Glacier Deep Archive“ archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Deep Archive“ archiviert. „S3 Glacier Deep Archive“ wird für die langfristige Datenaufbewahrung und zur Erhaltung digitaler Daten verwendet, wo nur ein- oder zweimal im Jahr auf die Daten zugegriffen wird. Sie können ein in „S3 Glacier Deep Archive“ archiviertes Band in der Regel innerhalb von 12 Stunden abrufen. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.
   - Wählen Sie einen benutzerdefinierten Pool aus, sofern verfügbar. Sie konfigurieren benutzerdefinierte Bandpools so, dass sie entweder Deep Archive Pool oder Glacier Pool verwenden. Bänder werden in der konfigurierten Speicherklasse archiviert, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

   Sie können die in „S3 Glacier Flexible Retrieval“ archivierten Bänder zu einem späteren Zeitpunkt zu „S3 Glacier Deep Archive“ verschieben. Weitere Informationen finden Sie unter Verschieben eines Bands von der Speicherklasse „S3 Glacier Flexible Retrieval“ zur Speicherklasse „S3 Glacier Deep Archive“.

> **Note**
>
> Vor dem 27. März 2019 erstellte Bänder werden direkt in „S3 Glacier Flexible Retrieval“ archiviert, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

10. (Optional) Sie fügen Ihrem Band Tags hinzu, indem Sie Neues Tag hinzufügen auswählen und einen Schlüssel und einen Wert eingeben. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen Ihrer Bänder erleichtert.
11. Wählen Sie Create tapes (Bänder erstellen) aus.
12. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.

Der Status der virtuellen Bänder wird zunächst auf CREATING (WIRD ERSTELLT) festgelegt, wenn die virtuellen Bänder erstellt werden. Nach der Erstellung der Bänder wird der Status in VERFÜGBAR geändert. Weitere Informationen finden Sie unter Verwalten von Tape Gateway.

Zulassen der automatischen Banderstellung

Tape Gateway kann automatisch neue virtuelle Bänder erstellen, um die von Ihnen konfigurierte minimale Anzahl verfügbarer Bänder beizubehalten. Anschließend werden diese neuen Bänder für den Import durch die Sicherungsanwendung zur Verfügung gestellt, so dass Ihre Sicherungsaufgaben ohne Unterbrechung ausgeführt werden können. Durch Zulassen der automatischen Banderstellung wird neben der manuellen Erstellung neuer virtueller Bänder auch die benutzerdefinierte Skripterstellung überflüssig.

Das Tape Gateway erzeugt automatisch ein neues Band, wenn weniger Bänder als die für die automatische Banderstellung angegebene Mindestanzahl verfügbarer Bänder vorhanden sind. Ein neues Band wird erzeugt, wenn Folgendes zutrifft:

- Ein Band wird aus einem Import-/Export-Slot importiert.
- Ein Band wird in das Bandlaufwerk importiert.

Das Gateway verwaltet eine Mindestanzahl von Bändern mit dem Barcode-Präfix, das in der Richtlinie für die automatische Banderstellung angegeben ist. Wenn weniger Bänder als die Mindestanzahl von Bändern mit dem Barcode-Präfix vorhanden sind, erstellt das Gateway automatisch so viele neue Bänder, dass die in der Richtlinie für die automatische Banderstellung angegebene Mindestanzahl von Bändern erreicht wird.

Wenn Sie ein Band auswerfen und es in den Import-/Export-Slot gelangt, wird dieses Band nicht auf die Mindestanzahl von Bändern angerechnet, die in Ihrer Richtlinie für die automatische Banderstellung angegeben ist. Nur Bänder im Import-/Export-Slot werden als „verfügbar“ gezählt. Durch das Exportieren eines Bandes wird keine automatische Banderstellung ausgelöst. Nur Importe wirken sich auf die Anzahl der verfügbaren Bänder aus.

Wenn Sie ein Band aus dem Import-/Export-Slot in ein Bandlaufwerk oder einen Speicherschacht verschieben, reduziert sich die Anzahl der Bänder im Import-/Export-Slot mit demselben Barcode-Präfix. Das Gateway erstellt neue Bänder, um die Mindestanzahl verfügbarer Bänder für dieses Barcode-Präfix beizubehalten.

So lassen Sie die automatische Banderstellung zu

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.
3. Wählen Sie das Gateway aus, für das Sie automatisch Bänder erstellen möchten.
4. Wählen Sie im Menü Actions (Aktionen) die Option Configure tape auto-create (Automatische Banderstellung konfigurieren).

   Die Seite Band automatisch erstellen wird angezeigt. Hier können Sie Optionen für die automatische Banderstellung konfigurieren, ändern oder löschen.
5. Um die automatische Banderstellung zuzulassen, wählen Sie Neues Element hinzufügen und konfigurieren dann die Einstellungen für die automatische Banderstellung.
6. Wählen Sie als Bandtyp die Option Standard aus, um virtuelle Standardbänder zu erstellen. Wählen Sie WORM, um virtuelle Bänder write-once-read-many (WORM) zu erstellen.
7. Geben Sie unter Mindestanzahl von Bändern die Mindestanzahl von virtuellen Bändern ein, die auf dem Tape Gateway jederzeit verfügbar sein sollen. Der gültige Bereich für diesen Wert ist mindestens 1 und maximal 10.
8. Geben Sie unter Capacity (Kapazität) die Kapazität der virtuellen Bänder in Byte an. Der gültige Bereich reicht von mindestens 100 Gib bis maximal 15 TiB.

9. Geben Sie in Barcode-Präfix das Präfix an, das dem Barcode virtueller Bänder vorangestellt werden soll.

   > **Note**
   >
   > Virtuelle Bänder werden durch einen Barcode eindeutig identifiziert und Sie können diesem ein Präfix hinzufügen. Das Präfix ist optional, kann jedoch für die Identifizierung Ihrer virtuellen Bänder hilfreich sein. Das Präfix muss aus Großbuchstaben (A-Z) bestehen und ein bis vier Zeichen lang sein.

10. Wählen Sie für Pool Glacier Pool, Deep Archive Pool oder einen benutzerdefinierten Pool aus, den Sie erstellt haben. Dieser Pool bestimmt die Speicherklasse, in der Ihr Band gespeichert wird, wenn es von Ihrer Sicherungssoftware ausgeworfen wird.

    - Wählen Sie Glacier Pool aus, wenn das Band in der Speicherklasse „S3 Glacier Flexible Retrieval“ gespeichert werden soll. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Flexible Retrieval“ archiviert. Sie verwenden „S3 Glacier Flexible Retrieval“ für aktivere Archive, aus denen Sie ein Band in der Regel innerhalb von 3 bis 5 Stunden abrufen können. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.
    - Wählen Sie Deep Archive Pool aus, wenn Sie das Band in der Speicherklasse „S3 Glacier Deep Archive“ archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Deep Archive“ archiviert. „S3 Glacier Deep Archive“ wird für die langfristige Datenaufbewahrung und zur Erhaltung digitaler Daten verwendet, wo nur ein- oder zweimal im Jahr auf die Daten zugegriffen wird. Sie können ein in „S3 Glacier Deep Archive“ archiviertes Band in der Regel innerhalb von 12 Stunden abrufen. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.
    - Wählen Sie einen benutzerdefinierten Pool aus, sofern verfügbar. Sie konfigurieren benutzerdefinierte Bandpools so, dass sie entweder Deep Archive Pool oder Glacier Pool verwenden. Bänder werden in der konfigurierten Speicherklasse archiviert, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

    Sie können die in „S3 Glacier Flexible Retrieval“ archivierten Bänder zu einem späteren Zeitpunkt zu „S3 Glacier Deep Archive“ verschieben. Weitere Informationen finden Sie unter Verschieben eines Bands von der Speicherklasse „S3 Glacier Flexible Retrieval“ zur Speicherklasse „S3 Glacier Deep Archive“.

> **Note**
>
> Vor dem 27. März 2019 erstellte Bänder werden direkt in „S3 Glacier Flexible Retrieval“ archiviert, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

11. Wenn Sie mit der Konfiguration der Einstellungen fertig sind, wählen Sie Änderungen speichern aus.
12. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.

    Der Status der verfügbaren virtuellen Bänder wird zunächst auf CREATING (WIRD ERSTELLT) gesetzt, wenn die virtuellen Bänder erstellt werden. Nach der Erstellung der Bänder wird der Status in VERFÜGBAR geändert. Weitere Informationen finden Sie unter Verwalten von Tape Gateway.

    Weitere Informationen zum Ändern von Richtlinien für die automatische Banderstellung oder zum Löschen der automatischen Banderstellung von einem Tape Gateway finden Sie unter Verwalten der automatischen Banderstellung.

Nächster Schritt

Verwenden von Tape Gateway

Verwenden von Tape Gateway

Im Folgenden finden Sie Anweisungen zur Verwendung von Tape Gateway.

Themen

- Verbinden von VTL-Geräten
- Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung
- Wie geht es weiter?

Verbinden von VTL-Geräten

Im Folgenden finden Sie Anweisungen zum Herstellen einer Verbindung zwischen Virtual Tape Library (VTL)-Geräten und dem Microsoft Windows- oder Red Hat Enterprise Linux (RHEL)-Client.

Themen

Herstellen einer Verbindung mit einem Microsoft Windows-Client

Das folgende Verfahren zeigt eine Zusammenfassung der Schritte, die Sie zum Verbinden mit einem Windows-Client ausführen.

So verbinden Sie VTL-Geräte mit einem Windows-Client

1. Starten `iscsicpl.exe`.

   > **Note**
   >
   > Sie benötigen Administratorrechte auf dem Client-Computer, um den iSCSI-Initiator ausführen zu können.

2. Starten Sie den Microsoft iSCSI-Initiator-Dienst.
3. Wählen Sie im Dialogfeld iSCSI Initiator-Eigenschaften die Registerkarte Ermittlung aus und klicken Sie dann auf Portal ermitteln.
4. Geben Sie unter IP-Adresse oder DNS-Name die IP-Adresse des Tape Gateway ein.
5. Wählen Sie die Registerkarte Targets (Ziele) und dann Refresh (Aktualisieren) aus. Anschließend werden im Feld Discovered targets (Ermittelte Ziele) alle 10 Bandlaufwerke und der Medienwechsler angezeigt. Der Status der Ziele ist Inactive (Inaktiv).
6. Wählen Sie das erste Gerät aus und verbinden Sie es. Die einzelnen Geräte müssen nacheinander verbunden werden.
7. Verbinden Sie alle Ziele.

Auf einem Windows-Client muss als Treiberanbieter des Bandlaufwerks Microsoft festgelegt sein. Gehen Sie wie folgt vor, um zu überprüfen, welcher Treiberanbieter festgelegt ist. Aktualisieren Sie ggf. den Treiber und den Anbieter:

So überprüfen und aktualisieren Sie Treiber und Anbieter

1. Starten Sie auf Ihrem Windows-Client den Geräte-Manager.
2. Erweitern Sie Tape drives (Bandlaufwerke), öffnen Sie mit das Kontextmenü (Rechtsklick) eines der Bandlaufwerke und wählen Sie Properties (Eigenschaften) aus.
3. Überprüfen Sie auf der Registerkarte Driver (Treiber) des Dialogfelds Device Properties (Geräteeigenschaften), ob Microsoft der Driver Provider (Treiberanbieter) ist.
4. Wenn Microsoft nicht der Driver Provider (Treiberanbieter) ist, legen Sie den Wert wie folgt fest:
   a. Wählen Sie Update Driver (Treiber aktualisieren) aus.
   b. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Browse my computer for driver software (Auf dem Computer nach Treibersoftware suchen) aus.
   c. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Let me pick from a list of device drivers on my computer (Aus einer Liste von Gerätetreibern auf dem Computer auswählen) aus.
   d. Wählen Sie LTO Tape drive (LTO-Bandlaufwerk) und dann Next (Weiter) aus.
5. Wählen Sie Close (Schließen) aus, um das Fenster Update Driver Software (Treibersoftware aktualisieren) zu schließen, und überprüfen Sie, ob nun Microsoft als Wert für Driver Provider (Treiberanbieter) festgelegt ist.
6. Wiederholen Sie die Schritte zum Aktualisieren von Treiber und Anbieter für alle Bandlaufwerke.

Herstellen einer Verbindung mit einem Linux-Client

Das folgende Verfahren zeigt eine Zusammenfassung der Schritte, die Sie zum Verbinden mit einem RHEL-Client ausführen.

So stellen Sie eine Verbindung zwischen einem Linux-Client und VTL-Geräten her

1. Installieren Sie das RPM-Paket `iscsi-initiator-utils`.

   Verwenden Sie den folgenden Befehl zum Installieren des Pakets.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. Stellen Sie sicher, dass der iSCSI-Daemon ausgeführt wird.

Verwenden Sie unter RHEL 5 oder 6 den folgenden Befehl.

```
sudo /etc/init.d/iscsi status
```

Verwenden Sie unter RHEL 7 den folgenden Befehl.

```
sudo service iscsid status
```

3. Entdecken Sie die Volume- oder VTL-Geräteziele, die für ein Gateway definiert sind. Verwenden Sie den folgenden Entdeckungsbefehl.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

Die Ausgabe des Erkennungsbefehls gleicht der folgenden Beispielausgabe.

Für Volume Gateways: `[GATEWAY_IP]:3260, 1 iqn.1997-05.com.amazon:myvolume`

Für Tape Gateways: `iqn.1997-05.com.amazon:[GATEWAY_IP]-tapedrive-01`

4. Stellen Sie eine Verbindung mit einem Ziel her.

Stellen Sie sicher, dass Sie im Verbindungsbefehl die korrekte *[GATEWAY_IP]* und den korrekten IQN angeben.

Verwenden Sie den folgenden -Befehl.

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Überprüfen Sie, ob das Volume an die Client-Maschine (den Initiator) angefügt ist. Führen Sie dazu den folgenden Befehl aus.

```
ls -l /dev/disk/by-path
```

Die Ausgabe des Befehls sollte der folgenden Beispielausgabe gleichen.

`lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda`

Für Volume Gateways wird dringend empfohlen, nach der Einrichtung des Initiators Ihre iSCSI-Einstellungen wie unter Anpassen Ihrer Linux iSCSI-Einstellungen beschrieben anzupassen.

Überprüfen Sie, ob das VTL-Geräte an die Client-Maschine (den Initiator) angefügt ist. Führen Sie dazu den folgenden Befehl aus.

```
ls -l /dev/tape/by-path
```

Die Ausgabe des Befehls sollte der folgenden Beispielausgabe gleichen.

```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
```

```
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-lun-0
 -> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-
lun-0-nst -> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-lun-0
 -> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-
lun-0-nst -> ../../nst1
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-lun-0
 -> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-
lun-0-nst -> ../../nst2
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-lun-0
 -> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-
lun-0-nst -> ../../nst5
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-lun-0
 -> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-
lun-0-nst -> ../../nst3
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-lun-0
 -> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-
lun-0-nst -> ../../nst4
```

Nächster Schritt

Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung

Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung

Sie testen Ihre Tape-Gateway-Einrichtung, indem Sie die folgenden Aufgaben mithilfe Ihrer Sicherungsanwendung ausführen:

1. Konfigurieren Sie die Sicherungsanwendung für das Erkennen Ihrer Speichergeräte.

   > **Note**
   >
   > Um die E/A-Leistung zu verbessern, empfehlen wir Ihnen, die Blockgröße der Bandlaufwerke in Ihrer Sicherungsanwendung auf 1 MB einzustellen. Weitere Informationen finden Sie unter Verwenden Sie eine größere Blockgröße für Bandlaufwerke.

2. Sichern Sie Daten auf einem Band.
3. Archivieren Sie das Band.
4. Rufen Sie das Band aus dem Archiv ab.
5. Wiederherstellen von Daten von einem Band

Um Ihre Konfiguration zu testen, verwenden Sie eine kompatible Sicherungsanwendung, wie im Folgenden beschrieben.

> **Note**
>
> Sofern nicht anders angegeben, wurden alle Backup-Anwendungen auf Microsoft Windows qualifiziert.

Themen

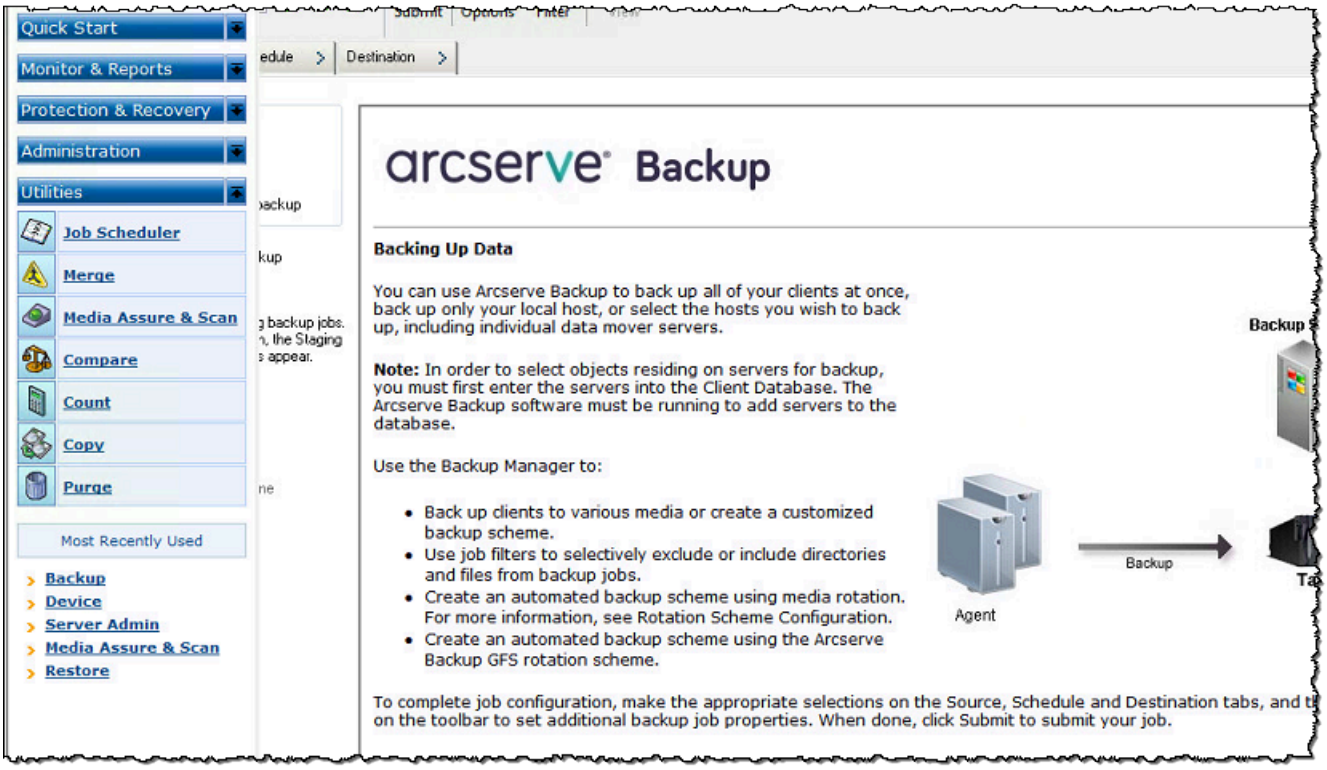
- Testen Ihrer Konfiguration mithilfe von Microsoft System Center Data Protection Manager
- Testen Ihrer Einrichtung mithilfe NovaStor von DataCenter/Network
- Testen Ihrer Einrichtung mithilfe von Bol NetVault Backup
- Testen der Einrichtung mithilfe von Veeam Backup & Replication
- Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec
- Testen Ihrer Einrichtung mithilfe von Ver Bols NetBackup

Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Testen der Einrichtung mithilfe von Arcserve Backup r17.0

Sie können Ihre Daten auf virtuellen Bändern sichern, diese Bänder archivieren und Ihre Virtual Tape Library (VTL)-Geräte verwalten, indem Sie Arcserve Backup r17.0 verwenden. In diesem Thema finden Sie eine grundlegende Anleitung für die Konfiguration von Arcserve Backup mit einem Tape Gateway und die Ausführung von Sicherungs- und Wiederherstellungsoperationen. Detaillierte Informationen zur Verwendung von Arcserve Backup r17.0 finden Sie in der Arcserve Backup r17-Dokumentation im Arcserve Administration Guide.

Der folgende Screenshot zeigt die Menüs von Arcserve.



Themen

Konfigurieren von Arcserve für das Arbeiten mit VTL-Geräten

Nachdem Sie Ihr Virtual Tape Library (VTL)-Geräte mit dem Client verbunden haben, können Sie nach den Geräten suchen.

So suchen Sie nach VTL-Geräten

1. Wählen Sie im Arcserve Backup Manager das Menü Utilities (Hilfsprogramme) aus.
2. Wählen Sie Media Assure und Scan (Medienprüfung und Scan) aus.

Laden von Bändern in einen Medienpool

Wenn die Arcserve-Software eine Verbindung zum Gateway herstellt und die Bänder verfügbar werden, lädt Arcserve diese Bänder automatisch. Wenn das Gateway nicht in der Arcserve-Software gefunden wird, starten Sie die Band-Engine erneut in Arcserve.

So starten Sie die Band-Engine

1. Wählen Sie Quick Start (Schnellstart), Administration (Verwaltung) und dann Device (Gerät) aus.
2. Öffnen Sie im Navigationsmenü das Kontextmenü (rechte Maustaste) für Ihr Gateway und wählen Sie einen Import-/Export-Slot aus.
3. Wählen Sie Quick Import (Schnellimport) aus und weisen Sie das Band einem leeren Steckplatz zu.
4. Öffnen Sie das Kontextmenü (Rechtsklick) für Ihr Gateway und wählen Sie Inventory/Offline Slots (Inventarisierung/Offline-Slots) aus.
5. Wählen Sie Quick Inventory (Schnellinventarisierung) aus, um Medieninformationen aus der Datenbank abzurufen.

Wenn Sie neue Bänder hinzufügen, müssen Sie das Gateway nach dem neuen Band durchsuchen, damit es in Arcserve angezeigt wird. Wenn das neue Band nicht angezeigt wird, müssen Sie die Bänder importieren.

So importieren Sie Bänder

1. Wählen Sie das Menü Quick Start (Schnellstart), dann Back up (Sichern) und schließlich Destination tape (Zielband) aus.
2. Wählen Sie Ihr Gateway aus, öffnen Sie das Kontextmenü (Rechtsklick) für ein einzelnes Band und wählen Sie dann Import-/Export-Slot aus.
3. Öffnen Sie das Kontextmenü (Rechtsklick) für jedes neue Band und wählen Sie Inventory (Inventarisierung) aus.
4. Öffnen Sie das Kontextmenü (Rechtsklick) für jedes neue Band und wählen Sie Format (Formatieren) aus.

Nun wird der Barcode des Bandes in der Storage-Gateway-Konsole angezeigt und das Band ist einsatzbereit.

Sichern von Daten auf einem Band

Wenn die Bänder in Arcserve geladen wurden, können Sie Daten sichern. Der Sicherungsvorgang funktioniert genauso wie die Sicherung von physischen Bänder.

So sichern Sie Daten auf einem Band

1. Öffnen Sie im Menü Schnellstart die Sitzung zum Wiederherstellen einer Sicherung.
2. Wählen Sie die Registerkarte Source (Quelle) und dann das Datei- oder Datenbanksystem aus, das Sie sichern möchten.
3. Wählen Sie die Registerkarte Planen und die Wiederholungsmethode aus, die Sie verwenden möchten.
4. Wählen Sie die Registerkarte Schedule (Planen) und das Band aus, das Sie verwenden möchten. Wenn die Daten, die Sie sichern, größer sind als der Speicherplatz auf dem Band, werden Sie von Arcserve aufgefordert, ein neues Band zu mounten.
5. Wählen Sie Submit (Absenden) aus, um Ihre Daten zu sichern.

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe möglicherweise fehl. Um die fehlgeschlagenen Backup-Aufgabe abzuschließen, müssen Sie sie erneut übermitteln.

Archivieren eines Bandes

Wenn Sie ein Band archivieren, verschiebt Ihr Tape Gateway das Band aus der Bandbibliothek in den Offline-Speicher. Bevor Sie ein Band auswerfen und archivieren, können Sie dessen Inhalt prüfen.

So archivieren Sie ein Band

1. Öffnen Sie im Menü Schnellstart die Sitzung zum Wiederherstellen einer Sicherung.
2. Wählen Sie die Registerkarte Source (Quelle) und dann das Datei- oder Datenbanksystem aus, das Sie sichern möchten.
3. Wählen Sie die Registerkarte Planen und die Wiederholungsmethode aus, die Sie verwenden möchten.
4. Wählen Sie Ihr Gateway aus, öffnen Sie das Kontextmenü (Rechtsklick) für ein einzelnes Band und wählen Sie dann Import-/Export-Slot aus.
5. Weisen Sie einen E-Mail-Steckplatz zu, um das Band zu laden. Der Status in der Storage-Gateway-Konsole wird in Archiv geändert. Der Archivierungsprozess kann einige Zeit in Anspruch nehmen.

Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach dem Archivieren wird das Band nicht mehr in der VTL aufgeführt, aber in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert.

Wiederherstellen von Daten von einem Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie ArcServer, um die Daten wiederherzustellen. Der Vorgang ist identisch mit dem Vorgang zur Wiederherstellung von Daten von physischen Bändern. Anleitungen hierfür finden Sie in der Arcserve Backup r17-Dokumentation.

Befolgen Sie zum Wiederherstellen von Daten von einem Band das folgende Verfahren.

So stellen Sie Daten von einem Band wieder her

1. Öffnen Sie im Menü Quick Start (Schnellstart) die Sitzung zum Wiederherstellen einer Wiederherstellung.
2. Wählen Sie die Registerkarte Source (Quelle) und dann das Datei- oder Datenbanksystem aus, das Sie wiederherstellen möchten.
3. Wählen Sie die Registerkarte Destination (Ziel) aus und übernehmen Sie die Standardeinstellungen.
4. Wählen Sie die Registerkarte Schedule (Planen), die gewünschte Wiederholungsmethode und dann Submit (Absenden) aus.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen Ihrer Konfiguration mithilfe von Bacula Enterprise

Sie können Bacula Enterprise Version 10 verwenden, um Ihre Daten auf virtuellen Bänder zu sichern, diese Bänder zu archivieren und Ihre Virtual Tape Library(VTL)-Geräte zu verwalten. In diesem Thema finden Sie eine grundlegende Dokumentation für die Konfiguration der Bacula 10-Sicherungsanwendung für ein Tape Gateway und die Ausführung von Sicherungen und Wiederherstellungen. Weitere Informationen zur Verwendung von Bacula Version 10 finden Sie in den Bacula-Systemhandbüchern und der Dokumentation oder direkt bei Bacula Systems.

> **Note**
>
> Bacula wird nur unter Linux unterstützt.

Einrichten von Bacula Enterprise

Sobald Sie Ihre VTL-Geräte mit Ihrem Linux-Client verbunden haben, konfigurieren Sie die Bacula-Software, damit Ihre Geräte erkannt werden. Weitere Informationen dazu, wie Sie VTL-Geräte mit Ihrem Client verbinden, finden Sie unter Verbinden von VTL-Geräten.

Einrichten von Bacula

1. Erwerben Sie eine lizenzierte Kopie der Bacula Enterprise-Sicherungssoftware von Bacula Systems.
2. Installieren Sie die Bacula Enterprise-Software auf Ihrem lokalen oder Cloud-basierten Computer.

   Weitere Informationen zum Abrufen der Installationssoftware finden Sie unter Enterprise Backup for Amazon S3 and Storage Gateway. Weitere Informationen zur Installation finden Sie im Bacula-Whitepaper Using Cloud Services and Object Storage with Bacula Enterprise Edition.

Konfigurieren von Bacula für das Arbeiten mit VTL-Geräten

Konfigurieren Sie nun Bacula für das Arbeiten mit Ihren VTL-Geräten. Im Folgenden finden Sie grundlegende Konfigurationsschritte.

Konfigurieren von Bacula

1. Installieren Sie den Bacula Director- und den Bacula Storage-Daemon. Weitere Anweisungen finden Sie in Kapitel 7 des Bacula-Whitepapers Using Cloud Services and Object Storage with Bacula Enterprise Edition.
2. Stellen Sie eine Verbindung mit dem System her, auf dem Bacula Director ausgeführt wird, und konfigurieren Sie den iSCSI-Initiator. Verwenden Sie dazu das Skript in Schritt 7.4 im Bacula-Whitepaper Using Cloud Services and Object Storage with Bacula Enterprise Edition.
3. Konfigurieren Sie die Speichergeräte. Verwenden Sie das Skript im Bacula-Whitepaper wie zuvor erläutert.
4. Konfigurieren Sie den lokalen Bacula Director, fügen Sie Speicherorte hinzu und definieren Sie Medienpools für Ihre Bänder. Verwenden Sie das Skript im Bacula-Whitepaper wie zuvor erläutert.

Sichern von Daten auf einem Band

1. Erstellen Sie Bänder in der Storage-Gateway-Konsole. Weitere Informationen zum Erstellen von Bändern finden Sie unter Erstellen von Bändern.
2. Übertragen Sie Bänder vom E/A-Slot in den Speicherschacht, indem Sie den folgenden Befehl ausführen.

   ```
   /opt/bacula/scripts/mtx-changer
   ```

   Mit dem folgenden Befehl werden beispielsweise Bänder vom E/A-Slot 1601 in den Speicherschacht 1 übertragen.

   ```
   /opt/bacula/scripts/mtx-changer transfer 1601 1
   ```
3. Starten Sie die Bacula-Konsole, indem Sie den folgenden Befehl ausführen.

   ```
   /opt/bacula/bin/bconsole
   ```

   > **Note**
   >
   > Wenn Sie ein Band erstellen und nach Bacula übertragen, verwenden Sie den Befehl `update slots storage=VTL` der Bacula-Konsole (bconsole), damit Bacula über die neuen Bänder, die Sie erstellt haben, informiert wird.
4. Beschriften Sie das Band mit dem Barcode als Namen des Volumes oder beschriften Sie es mithilfe des folgenden bconsole-Befehls.

   ```
   label storage=VTL pool=pool.VTL barcodes === label the tapes with the barcode as the volume name / label
   ```
5. Mounten Sie das Band mit dem folgenden Befehl.

   ```
   mount storage=VTL slot=1 drive=0
   ```
6. Erstellen Sie einen Sicherungsauftrag, der die von Ihnen erstellten Medienpools verwendet, und schreiben Sie dann Daten auf das virtuelle Band, indem Sie die gleichen Verfahren wie bei physischen Bändern verwenden.
7. Heben Sie das Mounting des Bands von der Bacula-Konsole, indem Sie den folgenden Befehl ausführen.

   ```
   umount storage=VTL slot=1 drive=0
   ```

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe fehl und der Bandstatus in Bacula Enterprise ändert sich in FULL. Wenn Sie wissen, dass das Band nicht voll ausgelastet ist, können Sie den Bandstatus manuell wieder in APPEND ändern und die Backup-Aufgabe mit demselben Band fortsetzen. Sie können die Aufgabe auch auf einem anderen Band fortsetzen, wenn andere Bänder mit dem Status APPEND sind.

Archivieren eines Bandes

Wenn alle Sicherungsaufträge für ein bestimmtes Band abgeschlossen sind und Sie das Band archivieren können, verwenden Sie das mtx-changer-Skript, um das Band vom Speicherschacht in den E/A-Slot zu verschieben. Diese Aktion ist ähnlich wie die Auswurfaktion in anderen Sicherungsanwendungen.

So archivieren Sie ein Band

1. Übertragen Sie die Bänder vom Speicherschacht in den E/A-Slot, indem Sie den Befehl `/opt/bacula/scripts/mtx-changer` ausführen.

   Mit dem folgenden Befehl wird beispielsweise ein Band vom Speicherschacht 1 in den E/A-Slot 1601 übertragen.

   ```
   /opt/bacula/scripts/mtx-changer transfer 1 1601
   ```

2. Vergewissern Sie sich, dass das Band im Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) archiviert wurde und den Status Archiviert aufweist.

Wiederherstellen von Daten von einem archivierten und abgerufenen Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Stellen Sie Ihre Daten mit der Bacula-Software wieder her:

a. Importieren Sie die Bänder in den Speicherschacht, indem Sie den Befehl `/opt/bacula/scripts/mtx-changer` ausführen, um die Bänder vom E/A-Slot zu übertragen.

   Mit dem folgenden Befehl werden beispielsweise Bänder vom E/A-Slot 1601 in den Speicherschacht 1 übertragen.

   ```
   /opt/bacula/scripts/mtx-changer transfer 1601 1
   ```

b. Verwenden Sie die Bacula-Konsole, um die Slots zu aktualisieren, und mounten Sie dann das Band.

c. Führen Sie den Befehl zum Wiederherstellen aus, um Ihre Daten wiederherzustellen. Detaillierte Anweisungen finden Sie in der Bacula-Dokumentation.

Testen Ihrer Konfiguration mithilfe von Commvault

Sie können Commvault Version 11 verwenden, um Ihre Daten auf virtuellen Bänder zu sichern, diese Bänder zu archivieren und Ihre VTL (Virtual Tape Library)-Geräte zu verwalten. In diesem Thema finden Sie eine grundlegende Anleitung zur Konfiguration der Commvault-Sicherungsanwendung für ein Tape Gateway, zur Ausführung eines Sicherungsarchivs und zum Abrufen Ihrer Daten von archivierten Bändern. Detaillierte Informationen zum Arbeiten mit Commvault finden Sie im Commvault Quick Start Guide auf der Commvault-Website.

Themen

- Konfigurieren von Commvault für das Arbeiten mit VTL-Geräten
- Erstellen einer Speicher-Richtlinie und eines Subclient
- Sichern von Daten auf einem Band in Commvault
- Archivieren eines Bandes in Commvault
- Wiederherstellen von Daten von einem Band

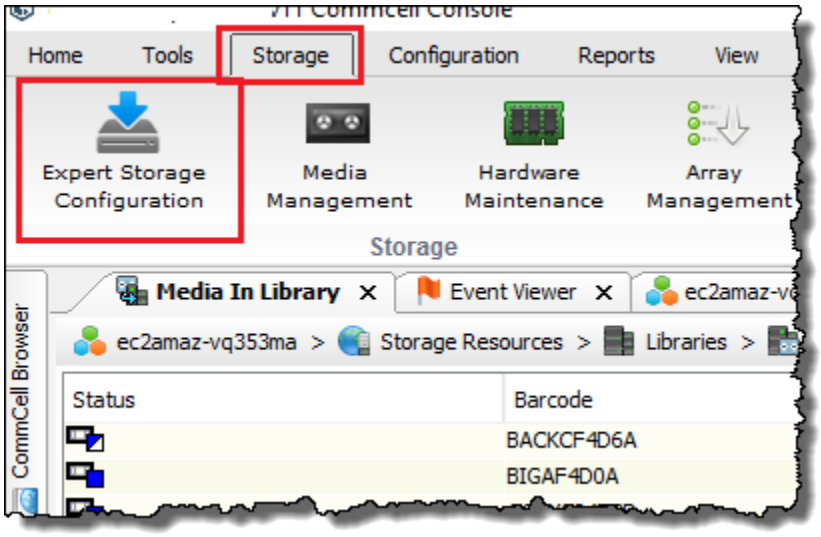
Konfigurieren von Commvault für das Arbeiten mit VTL-Geräten

Nachdem Sie die VTL-Geräte mit dem Windows-Client verbunden haben, konfigurieren Sie Commvault so, dass sie erkannt werden. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Verbinden von VTL-Geräten mit einem Windows-Client.

Standardmäßig erkennt die Commvault-Sicherungsanwendung VTL-Geräte nicht automatisch. Sie müssen die Geräte manuell hinzufügen, um sie für die Commvault-Sicherungsanwendung bereitzustellen, und die Geräte anschließend erkennen lassen.

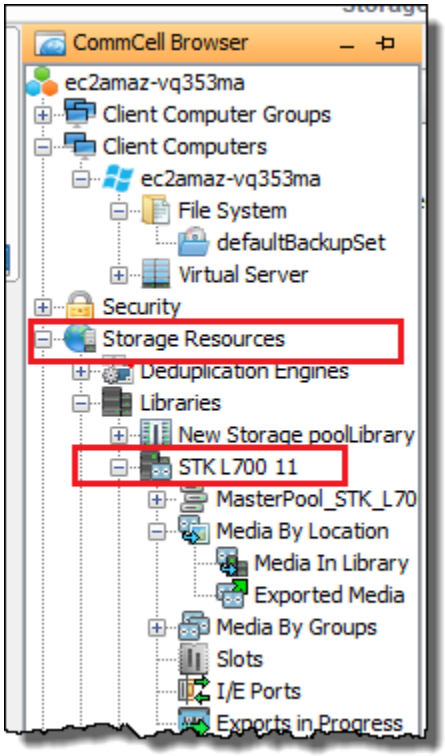
So konfigurieren Sie Commvault

1. Wählen Sie im Hauptmenü der CommCell -Konsole Speicher und dann Eine beliebige Speicherkonfiguration aus, um das Dialogfeld Auswählen MediaAgents zu öffnen.



2. Wählen Sie den verfügbaren Medienagenten, den Sie verwenden möchten, Add (Hinzufügen) und dann OK (OK) aus.
3. Wählen Sie im Dialogfeld Expert Storage Configuration (Fortgeschrittene Speicherkonfiguration) die Option Start (Starten) und dann die Option Detect/Configure Devices (Geräte entdecken/konfigurieren) aus.
4. Lassen Sie die Optionen in Device Type (Gerätetyp) ausgewählt und wählen Sie Exhaustive Detection (Ausführliche Erkennung) und dann OK (OK) aus.
5. Wählen Sie im Bestätigungsfeld Confirm Exhaustive Detection (Ausführliche Erkennung bestätigen) die Option Yes (Ja) aus.
6. Wählen Sie im Dialogfeld Device Selection (Geräteauswahl) Ihre Bibliothek und alle zugehörigen Laufwerke und dann OK (OK) aus. Warten Sie, bis Ihre Geräte erkannt werden, und wählen Sie dann die Option Close (Schließen) aus, um den Protokollbericht zu schließen.
7. Rechtsklicken Sie auf Ihre Bibliothek und wählen Sie die Option Configure (Konfigurieren) und dann Yes (Ja) aus. Schließen Sie das Dialogfeld für die Konfiguration.

8. Wählen Sie im Dialogfeld Does this library have a barcode reader? (Besitzt diese Bibliothek einen Strichcodeleser?) die Option Yes (Ja) und dann als Gerätetyp IBM ULTRIUM V5 (IBM ULTRIUM V5) aus.
9. Wählen Sie im CommCell Browser Speicherressourcen und dann Bibliotheken aus, um Ihre Bandbibliothek anzuzeigen.



10. Um Ihre Bänder in der Bibliothek anzuzeigen, öffnen Sie das Kontextmenü (Rechtsklick) für die Bibliothek und wählen dann Discover Media (Medien entdecken), Media location (Medienspeicherort) und Media Library (Medienbibliothek) aus.
11. Um Ihre Bänder zu mounten, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre Medien und wählen Load (Laden) aus.

Erstellen einer Speicher-Richtlinie und eines Subclient

Jeder Sicherungs- und Wiederherstellungsauftrag ist mit einer Speicher-Richtlinie und einer Subclient-Richtlinie verknüpft.

Eine Speicher-Richtlinie ordnet Ihren Medien den ursprünglichen Speicherort der Daten zu.

So erstellen Sie eine Speicher-Richtlinie

1. Wählen Sie im CommCell Browser Richtlinien aus.

2. Öffnen Sie das Kontextmenü (Rechtsklick) für Storage Policies (Speicherrichtlinien) und wählen Sie dann New Storage Policy (Neue Speicherrichtlinie) aus.
3. Wählen Sie im Assistenten zum Erstellen von Speicherrichtlinien die Option Data Protection and Archiving (Datenschutz und -archivierung) und dann Next (Weiter) aus.
4. Geben Sie in Storage Policy Name (Name der Speicherrichtlinie) einen Namen ein und wählen Sie anschließend die Option Incremental Storage Policy (Richtlinie für inkrementellen Speicher) aus. Wählen Sie eine der Optionen aus, um diese Speicherrichtlinie mit inkrementellen Ladevorgängen zu verknüpfen. Lassen Sie die Optionen andernfalls deaktiviert und wählen Next (Weiter) aus.
5. Wählen Sie im Dialogfeld Do you want to Use Global Deduplication Policy? (Möchten Sie eine Richtlinie für globale Deduplizierung verwenden?) die gewünschte Option für Deduplication (Deduplizierung) und dann Next (Weiter) aus.
6. Wählen Sie in Library for Primary Copy (Bibliothek für primäre Kopie) Ihre VTL-Bibliothek und dann Next (Weiter) aus.
7. Überprüfen Sie, ob Ihre Medienagent-Einstellungen korrekt sind, und wählen Sie dann Next (Weiter) aus.
8. Überprüfen Sie, ob Ihre Scratch-Pool-Einstellungen korrekt sind, und wählen Sie dann Next (Weiter) aus.
9. Konfigurieren Sie in iData Agent Backup data (iData Agent Backup-Daten) Ihre Aufbewahrungsrichtlinien und wählen Sie dann Next (Weiter) aus.
10. Überprüfen Sie die Verschlüsselungseinstellungen und wählen Sie dann Next (Weiter) aus.
11. Um Ihre Speicherrichtlinie anzuzeigen, wählen Sie Storage Policies (Speicherrichtlinien) aus.

Sie erstellen eine Subclient-Richtlinie und verknüpfen diese mit Ihrer Speicherrichtlinie. Eine Subclient-Richtlinie ermöglicht es Ihnen, ähnliche Dateisystem-Clients von einer zentralen Vorlage aus zu konfigurieren, sodass Sie nicht viele ähnliche Dateisysteme manuell einrichten müssen.

So erstellen sie eine Subclient-Richtlinie

1. Wählen Sie im CommCell Browser Client-Computer und dann Ihren Client-Computer aus. Wählen Sie Dateisystem und dann ausdefaultBackupSet.
2. Klicken Sie mit der rechten Maustaste auf defaultBackupSet, wählen Sie Alle Aufgaben und dann Neuer Unterclient aus.
3. Geben Sie im Feld Unterclient-Eigenschaften einen Namen in SubClient Name ein und wählen Sie dann OK aus.

4. Wählen Sie Browse (Durchsuchen) aus, navigieren Sie zu den Dateien, die Sie sichern möchten, wählen Sie Add (Hinzufügen) aus und schließen Sie dann das Dialogfeld.
5. Wählen Sie im Eigenschaftsfeld Subclient (Unterclient) die Registerkarte Storage Device (Speichergerät), unter Storage policy (Speicherrichtlinie) eine Speicherrichtlinie und dann OK (OK) aus.
6. Verknüpfen Sie im nun angezeigten Fenster Backup Schedule (Sicherungszeitplan) den neuen Unterclient mit einem Sicherungszeitplan.
7. Wählen Sie Do Not Schedule (Nicht planen) für eine einmalige Sicherung oder für On-Demand-Sicherungen und dann OK (OK) aus.

   Sie sollten jetzt Ihren Unterclient auf der defaultBackupSet Registerkarte sehen.

Sichern von Daten auf einem Band in Commvault

Zum Erstellen eines Sicherungsauftrags und Schreiben von Daten auf ein virtuelles Band verwenden Sie dieselben Verfahren wie bei physischen Bändern. Weitere Informationen finden Sie in der Commvault-Dokumentation.

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe möglicherweise fehl. In einigen Fällen können Sie eine Option auswählen, um die fehlgeschlagene Aufgabe wieder aufzunehmen. Andernfalls müssen Sie einen neue Aufgabe absenden. Wenn Commvault das Band nach einer fehlgeschlagenen Aufgabe als unbrauchbar markiert, müssen Sie das Band erneut in das Laufwerk einlegen, um weiter darauf schreiben zu können. Wenn mehrere Bänder verfügbar sind, setzt Commvault die fehlgeschlagene Backup-Aufgabe möglicherweise auf einem anderen Band fort.

Archivieren eines Bandes in Commvault

Sie starten den Archivierungsprozess, indem Sie das Band auswerfen. Wenn Sie ein Band archivieren, verschiebt Tape Gateway das Band aus der Bandbibliothek in einen Offline-Speicher. Bevor Sie ein Band auswerfen und archivieren, können Sie zunächst dessen Inhalt prüfen.

So archivieren Sie ein Band

1. Wählen Sie im CommCell Browser Speicherressourcen, Bibliotheken und dann Ihre Bibliothek aus. Wählen Sie Medien nach Speicherort und dann Medien in Bibliothek aus.
2. Öffnen Sie das Kontextmenü (Rechtsklick) des Bands, das Sie archivieren möchten. Wählen Sie All Tasks (Alle Aufgaben), Export (Exportieren) und dann OK (OK) aus.

Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach Abschluss der Archivierung wird das Band nicht mehr in der VTL aufgeführt.

Stellen Sie in der Commvault-Software sicher, dass sich das Band nicht mehr im Speicherschaft befindet.

Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Tapes aus. Überprüfen Sie, ob für das archivierte Band der Status ARCHIVED (ARCHIVIERT) angezeigt wird.

Wiederherstellen von Daten von einem Band

Sie können Daten von einem Band wiederherstellen, das niemals archiviert und abgerufen wurde, oder von einem Band, das archiviert und abgerufen wurde. Bei Bändern, die noch nie archiviert und abgerufen wurden (nicht abgerufene Bänder), haben Sie zwei Möglichkeiten, die Daten wiederherzustellen:

- Wiederherstellen durch Subclient
- Wiederherstellen durch Auftrags-ID

So stellen Sie Daten von einem nicht abgerufenen Band durch einen Subclient wieder her

1. Wählen Sie im CommCell Browser Client-Computer und dann Ihren Client-Computer aus. Wählen Sie Dateisystem und dann ausdefaultBackupSet.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für den Unterclient. Wählen Sie Browse and Restore (Durchsuchen und Wiederherstellen) und dann View Content (Inhalt anzeigen) aus.
3. Wählen Sie die Dateien aus, die Sie wiederherstellen möchten, und dann Recover All Selected (Alle ausgewählten Dateien wiederherstellen).
4. Wählen Sie Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.

So stellen Sie Daten von einem nicht abgerufenen Band durch Auftrags-ID wieder her

1. Wählen Sie im CommCell Browser Client-Computer und dann Ihren Client-Computer aus. Rechtsklicken Sie auf File System (Dateisystem). Wählen Sie View (Anzeigen) und dann Backup History (Sicherungsverlauf) aus.
2. Wählen Sie in der Kategorie Backup Type (Sicherungstyp) den Typ des gewünschten Sicherungsauftrags und dann OK (OK) aus. Es wird Ihnen eine Registerkarte mit dem Verlauf der Sicherungsaufträge angezeigt.
3. Suchen Sie die Job ID (Auftrags-ID), die Sie wiederherstellen möchten, rechtsklicken Sie auf diese und wählen Sie Browse and Restore (Durchsuchen und wiederherstellen) aus.
4. Wählen Sie im Dialogfeld Browse and Restore Options (Optionen für Durchsuchen und Wiederherstellen) die Option View Content (Inhalt anzeigen) aus.
5. Wählen Sie die Dateien aus, die Sie wiederherstellen möchten, und ann Recover All Selected (Alle ausgewählten Dateien wiederherstellen) aus.
6. Wählen Sie Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.

So stellen Sie Daten von einem archivierten und abgerufenen Band wieder her

1. Wählen Sie im CommCell Browser Speicherressourcen, Bibliotheken und dann Ihre Bibliothek aus. Wählen Sie Medien nach Speicherort und dann Medien in Bibliothek aus.
2. Rechtsklicken Sie auf das abgerufene Band. Wählen Sie All Tasks (Alle Aufgaben) und dann Catalog (Katalog) aus.
3. Wählen Sie im Dialogfeld Catalog Media (katelogmedien) die Option Catalog only (Nur Katalog) und dann OK (OK) aus.
4. Wählen Sie CommCell Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.
5. Öffnen Sie nach erfolgreichem Abschluss des Auftrags das Kontextmenü (Rechtsklick) für Ihr Band. Wählen Sie View (Anzeigen) und dann View Catalog Contents (Kataloginhalt anzeigen) aus. Notieren Sie zur späteren Verwendung die Job ID (Auftrags-ID).
6. Wählen Sie die Option Recatalog/Merge (Neu katalogisieren/Zusammenführen) aus. Stellen Sie sicher, dass im Dialogfeld Catalog Media (Katalogmedien) die Option Merge only (Nur zusammenführen) ausgewählt ist.
7. Wählen Sie Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.

8. Nachdem der Auftrag erfolgreich war, wählen Sie CommCell Home , wählen Sie Systemsteuerung und dann Durchsuchen/Suchen/Wiederherstellung aus.
9. Wählen Sie Show aged data during browse and recovery (Veraltete Daten während Durchsuchen und Wiederherstellen anzeigen) und dann OK (OK) aus. Schließen Sie dann Control Panel (Steuerungsbereich).
10. Klicken Sie im CommCell Browser mit der rechten Maustaste auf Client-Computer und wählen Sie dann Ihren Client-Computer aus. Wählen Sie View (Anzeigen) und dann Job History (Auftragsverlauf) aus.
11. Wählen Sie im Dialogfeld Job History Filter (Auftragsverlaufsfilter) die Option Advanced (Erweitert) aus.
12. Wählen Sie Include Aged Data (Veraltete Daten einschließen) und dann OK (OK) aus.
13. Wählen Sie im Dialogfeld Job History (Auftragsverlauf) OK (OK) aus, um die Registerkarte history of jobs (Verlauf von Aufträgen) zu öffnen.
14. Suchen Sie den Auftrag, den Sie wiederherstellen möchten, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie dann Browse and Restore (Durchsuchen und Wiederherstellen) aus.
15. Wählen Sie im Dialogfeld Browse and Restore (Durchsuchen und Wiederherstellen) die Option View Content (Inhalt anzeigen) aus.
16. Wählen Sie die Dateien aus, die Sie wiederherstellen möchten, und ann Recover All Selected (Alle ausgewählten Dateien wiederherstellen) aus.
17. Wählen Sie Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.

Testen Ihrer Einrichtung mit Dell EMC NetWorker

Mit Dell EMC NetWorker 19.5 können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL)-Geräte verwalten. In diesem Thema finden Sie eine grundlegende Dokumentation zur Konfiguration der Dell EMC- NetWorker Software für die Arbeit mit einem Tape Gateway und zur Durchführung einer Sicherung, einschließlich der Konfiguration von Speichergeräten, des Schreibens von Daten auf ein Band, des Archivierens eines Bands und des Wiederherstellens von Daten von einem Band.

Ausführliche Informationen zur Installation und Verwendung der Dell EMC- NetWorker Software finden Sie im -Administratorhandbuch.

Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

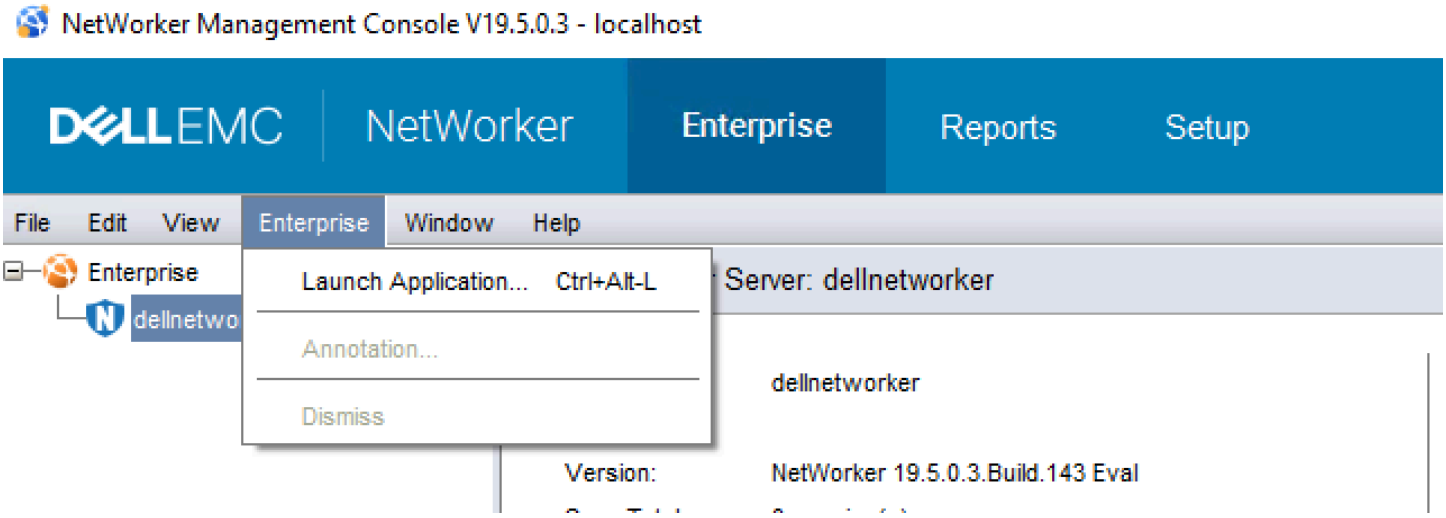
- Konfigurieren der Arbeit mit VTL-Geräten
- Zulassen des Imports von WORM-Banden in Dell EMC NetWorker
- Sichern von Daten auf einem Band in Dell EMC NetWorker
- Archivieren eines Bands in Dell EMC NetWorker
- Wiederherstellen von Daten aus einem archivierten Band in Dell EMC NetWorker

Konfigurieren der Arbeit mit VTL-Geräten

Nachdem Sie die VTL (Virtual Tape Library)-Geräte mit dem Microsoft Windows-Client verbunden haben, müssen Sie die Software so konfigurieren, dass sie Ihre Geräte erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Verbinden von VTL-Geräten.

Die Software erkennt Tape Gateway-Geräte nicht automatisch. Um Ihre VTL-Geräte der NetWorker Software zur Verfügung zu stellen und die Software zur Erkennung zu bringen, konfigurieren Sie die Software manuell. Im Folgenden nehmen wir an, dass Sie die Software ordnungsgemäß installiert haben und mit der Management Console vertraut sind. Weitere Informationen zur -Managementkonsole finden Sie im Abschnitt über die NetWorker -Managementkonsolenschnittstelle im Dell EMC NetWorker Administration Guide.

Der folgende Screenshot zeigt Dell EMC NetWorker 19.5.



So konfigurieren Sie die Dell EMC NetWorker -Software für VTL-Geräte

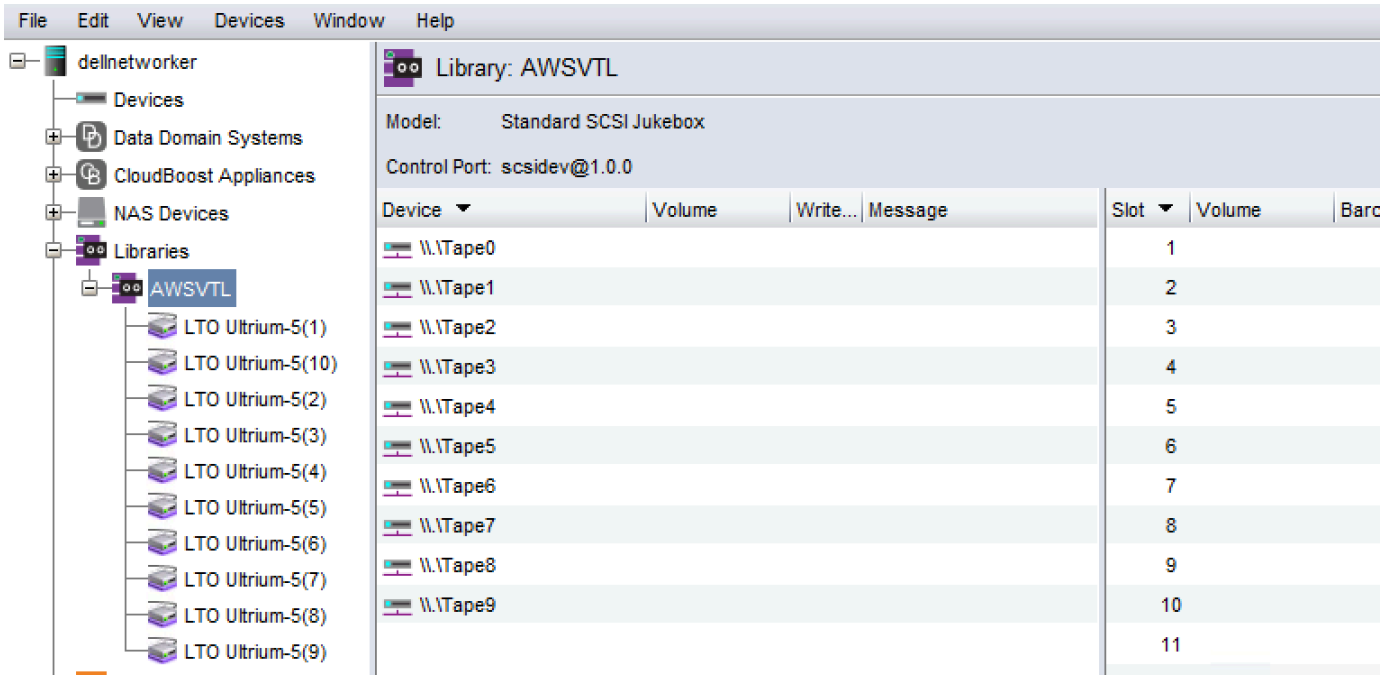
1. Starten Sie die Dell EMC NetWorker Management Console-Anwendung, wählen Sie im Menü Enterprise und dann im linken Bereich localhost aus.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für localhost (Lokaler Host) und wählen Sie dann Launch Application (Anwendung starten) aus.
3. Wählen Sie die Registerkarte Devices (Geräte) aus, öffnen Sie das Kontextmenü (Rechtsklick) für Libraries (Bibliotheken) und wählen Sie dann Scan for Devices (Nach Geräten scannen) aus.
4. Wählen Sie im Assistenten für das Scannen nach Geräten Start Scan (Scan starten) und dann im anschließend angezeigten Dialogfeld OK (OK) aus.
5. Erweitern Sie die Ordnerstruktur Bibliotheken, um alle Ihre Bibliotheken anzuzeigen und aktualisieren Sie die Anzeige mit F5. Dieser Vorgang kann einige Sekunden dauern, um die Geräte in die Bibliothek zu laden.
6. Öffnen Sie ein Befehlsfenster (CMD.exe) mit Administratorrechten und führen Sie das Dienstprogramm „jbconfig“ aus, das mit Dell EMC NetWorker 19.5 installiert ist.

```
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>jbconfig

Jbconfig is running on host dellnetworker (Windows Server 2019 Datacenter 10.0),
  and is using dellnetworker as the NetWorker server.

        1) Configure an Autodetected SCSI Jukebox.
        2) Configure an Autodetected NDMP SCSI Jukebox.
        3) Configure an SJI Jukebox.
        4) Configure an STL Silo.
        5) Exit.

which activity do you want to perform? [1]
14484:jbconfig: Scanning SCSI buses; this may take a while ...
Installing 'Standard SCSI Jukebox' jukebox - scsidev@1.0.0.

What name do you want to assign to this jukebox device? AWSVTL
15814:jbconfig: Attempting to detect serial numbers on the jukebox and drives ...

15815:jbconfig: Will try to use SCSI information returned by jukebox to configure drives.

Turn NetWorker auto-cleaning on (yes / no) [yes]? no

The following drive(s) can be auto-configured in this jukebox:
 1> LTO Ultrium-5 @ 1.1.0 ==> \\.\Tape0
 2> LTO Ultrium-5 @ 1.2.0 ==> \\.\Tape1
 3> LTO Ultrium-5 @ 1.3.0 ==> \\.\Tape2
 4> LTO Ultrium-5 @ 1.4.0 ==> \\.\Tape3
 5> LTO Ultrium-5 @ 1.5.0 ==> \\.\Tape4
 6> LTO Ultrium-5 @ 1.6.0 ==> \\.\Tape5
 7> LTO Ultrium-5 @ 1.7.0 ==> \\.\Tape6
 8> LTO Ultrium-5 @ 1.8.0 ==> \\.\Tape7
 9> LTO Ultrium-5 @ 1.9.0 ==> \\.\Tape8
10> LTO Ultrium-5 @ 1.10.0 ==> \\.\Tape9
These are all the drives that this jukebox has reported.
```

```
To change the drive model(s) or configure them as shared or NDMP drives,
 you need to bypass auto-configure. Bypass auto-configure? (yes / no) [no]


Jukebox has been added successfully

The following configuration options have been set:

> Jukebox description to the control port and model.
> Autochanger control port to the port at which we found it.
> Autocleaning off.
> Barcode reading to on.
> Volume labels that match the barcodes.

You can review and change the characteristics of the autochanger and its
        associated devices using the NetWorker Management Console.

Would you like to configure another jukebox? (yes/no) [no]

C:\Users\Administrator>_
```

7. Wenn „jbconfig“ abgeschlossen ist, kehren Sie zur Networker-GUI zurück und drücken Sie F5, um die Aktualisierung durchzuführen.

8. Wählen Sie Ihre Bibliothek aus, um Ihre Bänder im linken Bereich und die entsprechende Liste der leeren Volume-Slots im rechten Fensterbereich anzuzeigen. In diesem Screenshot ist die Bibliothek „AWSVTL“ ausgewählt.



9. Wählen Sie in der Volume-Liste die Volumes aus, die Sie aktivieren möchten (ausgewählte Volumes werden hervorgehoben), öffnen Sie das Kontextmenü (Rechtsklick) für die

ausgewählten Volumes und wählen Sie dann Ablegen aus. Mit dieser Aktion wird das Band vom E/A-Slot in den Volume-Slot verschoben.

10. Wählen Sie im nun angezeigten Dialogfeld Yes (Ja) und dann im Dialogfeld Load the Cartridges into (Kartuschen laden in) erneut Yes (Ja) aus.
11. Wenn Sie keine weiteren Bänder ablegen möchten, wählen Sie No (Nein) oder Ignore (Ignorieren) aus. Wählen Sie andernfalls Yes (Ja) aus, um weitere Bänder abzulegen.

Zulassen des Imports von WORM-Banden in Dell EMC NetWorker

Sie können jetzt Bänder aus Ihrem Tape Gateway in die Dell EMC NetWorker-Bibliothek importieren.

Die virtuellen Bänder werden geschrieben, sobald viele (WORM) Bänder gelesen wurden, aber Dell EMC NetWorker erwartet Nicht-WORM-Bänder. Damit Dell EMC mit Ihren virtuellen Bändern funktioniert, müssen Sie NetWorker den Import von Bändern in Nicht-WORM-Medienpools aktivieren.

So ermöglichen Sie den Import von WORM-Bändern in Nicht-WORM-Medienpools

1. Wählen Sie in der NetWorker Konsole Medien aus, öffnen Sie das Kontextmenü (rechte Maustaste) für localhost und wählen Sie dann Eigenschaften aus.
2. Wählen Sie im Fenster NetWorker Servereigenschaften die Registerkarte Konfiguration aus.
3. Deaktivieren Sie im Abschnitt Worm tape handling (WORM-Band-Bearbeitung) das Kästchen WORM tapes only in WORM pools (WORM-Bänder nur in WORM-Pools) und wählen Sie dann OK (OK) aus.

Sichern von Daten auf einem Band in Dell EMC NetWorker

Das Sichern von Daten auf einem Band ist ein zweistufiger Prozess.

1. Beschriften Sie die Bänder, auf denen Sie Daten sichern möchten, erstellen Sie den Zielmedienpool und fügen Sie die Bänder zum Pool hinzu.

   Erstellen Sie einen Medienpool und schreiben Sie Daten auf ein virtuelles Band indem Sie dieselben Verfahren wie bei physischen Bändern verwenden. Ausführliche Informationen finden Sie im Abschnitt Backup-Daten im Dell EMC NetWorker Administration Guide .
2. Schreiben Sie Daten auf das Band. Sie sichern Daten mithilfe der Dell EMC- NetWorker Benutzeranwendung anstelle der Dell EMC NetWorker -Managementkonsole. Die Dell EMC NetWorker -Benutzeranwendung wird als Teil der NetWorker Installation installiert.

> **Note**
>
> Sie verwenden die Dell EMC NetWorker -Benutzeranwendung, um Backups durchzuführen, aber Sie zeigen den Status Ihrer Backup- und Wiederherstellungsaufträge in der EMC-Managementkonsole an. Um den Status anzuzeigen, wählen Sie das Menü Devices (Geräte) aus und zeigen den Status im Fenster Log (Protokoll) an.

> **Note**
>
> Wenn Ihr Tape Gateway aus irgendeinem Grund während einer laufenden Backup-Aufgabe neu startet, wird die Backup-Aufgabe unterbrochen und der Bandstatus in Dell EMC Networker ändert sich auf Schreibgeschützt. Sie können das Band archivieren oder weiterhin Daten daraus lesen. Sie können die unterbrochene Backup-Aufgabe auf einem anderen Band fortsetzen.

Archivieren eines Bands in Dell EMC NetWorker

Wenn Sie ein Band archivieren, verschiebt Tape Gateway das Band von der Dell EMC NetWorker -Bandbibliothek in den Offline-Speicher. Sie beginnen die Bandarchivierung durch Auswerfen eines Bands aus dem Bandlaufwerk in den Speicherschacht. Anschließend ziehen Sie das Band mithilfe Ihrer Sicherungsanwendung, d. h. der Dell EMC- NetWorker Software, vom Slot in das Archiv zurück.

So archivieren Sie ein Band mit Dell EMC NetWorker

1. Wählen Sie auf der Registerkarte Geräte im NetWorker Verwaltungsfenster localhost oder Ihren EMC-Server und dann Bibliotheken aus.
2. Wählen Sie die Bibliothek aus, die Sie aus Ihrer virtuellen Bandbibliothek importiert haben.
3. Öffnen Sie in der Liste der Bänder, zu denen Sie Daten geschrieben haben, das Kontextmenü (Rechtsklick) für das Band, das Sie archivieren möchten, und wählen Sie dann Eject/Withdraw (Auswerfen/Zurückziehen) aus.
4. Klicken Sie im nun angezeigten Bestätigungsfenster auf OK (OK).

Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung

gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach Abschluss der Archivierung wird das Band nicht mehr in der VTL aufgeführt.

Stellen Sie in der Dell EMC- NetWorker Software sicher, dass sich das Band nicht mehr im Speicher-Slot befindet.

Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Tapes aus. Überprüfen Sie, ob für das archivierte Band der Status ARCHIVED (ARCHIVIERT) angezeigt wird.

Wiederherstellen von Daten aus einem archivierten Band in Dell EMC NetWorker

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig:

1. Rufen Sie das archivierte Band auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie die Dell EMC NetWorker -Software, um die Daten wiederherzustellen. Dazu erstellen Sie einen Wiederherstellungsordner, wie bei der Wiederherstellung von Daten von physischen Bändern. Anweisungen finden Sie im Abschnitt Verwenden des - NetWorker Benutzerprogramms im Dell EMC NetWorker Administration Guide.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen Ihrer Konfiguration mithilfe von IBM Spectrum Protect

Sie können Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL)-Geräte verwalten, indem Sie IBM Spectrum Protect mit verwenden AWS Storage Gateway. (IBM Spectrum Protect wurde früher als Tivoli Storage Manager bezeichnet.)

Dieses Thema enthält grundlegende Informationen zur Konfiguration der Sicherungssoftware IBM Spectrum Protect Version 8.1.10 für ein Tape Gateway. Es enthält auch grundlegende Informationen zur Durchführung von Sicherungs- und Wiederherstellungsvorgängen mit IBM Spectrum Protect. Weitere Informationen zur Verwaltung der IBM Spectrum Protect-Sicherungssoftware finden Sie in Overview of administration tasks für IBM Spectrum Protect.

Die IBM Spectrum Protect-Sicherungssoftware unterstützt AWS Storage Gateway auf den folgenden Betriebssystemen.

- Microsoft Windows Server

- Red Hat Linux

Informationen zu Geräten, die von IBM Spectrum Protect für Windows unterstützt werden, finden Sie unter IBM Spectrum Protect (formerly Tivoli Storage Manager) Supported Devices for AIX, HP-UX, Solaris, and Windows.

Informationen zu Geräten, die von IBM Spectrum Protect für Linux unterstützt werden, finden Sie unter IBM Spectrum Protect (formerly Tivoli Storage Manager) Supported Devices for Linux.

Themen

Einrichten von IBM Spectrum Protect

Nachdem Sie Ihre VTL-Geräte mit Ihrem Client verbunden haben, konfigurieren Sie die Software IBM Spectrum Protect Version 8.1.10, damit sie sie erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit Ihrem Client verbinden, finden Sie unter Verbinden von VTL-Geräten.

Einrichten von IBM Spectrum Protect

1. Erwerben Sie eine lizenzierte Kopie der Software IBM Spectrum Protect Version 8.1.10 von IBM.
2. Installieren Sie die IBM Spectrum Protect-Software in Ihrer lokalen Umgebung oder auf einer Cloud-basierten EC2-Instance. Weitere Informationen finden Sie in der Dokumention Installing and upgrading für IBM Spectrum Protect.

   Weitere Informationen zur Konfiguration der IBM Spectrum Protect-Software finden Sie unter Configuring AWS Tape Gateway virtual tape libraries for an IBM Spectrum Protect server.

Konfigurieren von IBM Spectrum Protect für das Arbeiten mit VTL-Geräten

Konfigurieren Sie nun IBM Spectrum Protect für das Arbeiten mit Ihren VTL-Geräten. Sie können IBM Spectrum Protect unter Microsoft Windows Server oder Red Hat Linux dazu konfigurieren, mit VTL-Geräten zu arbeiten.

Konfigurieren von IBM Spectrum Protect für Windows

Umfassende Anweisungen zur Konfiguration von IBM Spectrum Protect unter Windows finden Sie unter Tape Device Driver-W12 6266 for Windows 2012 auf der Lenovo-Website. Im Folgenden finden Sie eine grundlegende Dokumentation zu diesem Prozess.

So konfigurieren Sie IBM Spectrum Protect für Microsoft Windows

1. Holen Sie sich das richtige Treiberpaket für Ihren Medienwechsler. Für die Bandgerätetreiber erfordert IBM Spectrum Protect Version W12 6266 für Windows 2012. Anweisungen zum Abrufen der Treiber finden Sie unter Tape Device Driver-W12 6266 for Windows 2012 auf der Lenovo Website.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie "vom Betriebssystem unabhängige" Treiber installieren.

2. Öffnen Sie auf Ihrem Computer die Computerverwaltung, erweitern Sie Medienwechslergeräte und stellen Sie sicher, dass der Medienwechslertyp als IBM 3584 Tape Library aufgeführt ist.
3. Stellen Sie sicher, dass der Barcode für jedes Band in der Virtual Tape Library acht Zeichen oder weniger beträgt. Wenn Sie versuchen, Ihrem Band einen Barcode zuzuordnen, der länger als acht Zeichen ist, erhalten Sie diese Fehlermeldung: `"Tape barcode is too long for media changer"`.
4. Stellen Sie sicher, dass alle Ihre Bandlaufwerke und Medienwechsler in IBM Spectrum Protect angezeigt werden. Führen Sie dazu den folgenden Befehl aus: `\Tivoli\TSM \server>tsmdlst.exe`

Konfigurieren von IBM Spectrum Protect für Linux

Im Folgenden finden Sie eine grundlegende Dokumentation zur Konfiguration von IBM Spectrum für die Arbeit mit VTL-Geräten unter Linux.

So konfigurieren Sie IBM Spectrum Protect für Linux

1. Rufen Sie IBM Fix Central auf der IBM Support-Website auf und wählen SieProdukt auswählen aus.
2. Wählen Sie für Product Group (Produktgruppe) die Option System Storage (Systemspeicher) aus.

3. Wählen Sie für Select from System Storage (Systemspeicher-Auswahl) die Option Tape systems (Bandsysteme) aus.
4. Wählen Sie für Tape systems (Bandsysteme) die Option Tape drivers and software (Bandtreiber und -software) aus.
5. Wählen Sie für Select from Tape drivers and software (Bandtreiber und -software-Auswahl), die Option Tape device drivers (Bandgerätetreiber)aus.
6. Wählen Sie für Platform (Plattform) Ihr Betriebssystem aus und klicken Sie auf Continue (Weiter).
7. Wählen Sie die Gerätetreiber-Version aus, die Sie herunterladen möchten. Folgen Sie dann den Anweisungen auf der Fix Central -Downloadseite, um IBM Spectrum Protect herunterzuladen und zu konfigurieren.
8. Stellen Sie sicher, dass der Barcode für jedes Band in der Virtual Tape Library acht Zeichen oder weniger beträgt. Wenn Sie versuchen, Ihrem Band einen Barcode zuzuordnen, der länger als acht Zeichen ist, erhalten Sie diese Fehlermeldung: `"Tape barcode is too long for media changer"`.

Schreiben von Daten auf ein Band in IBM Spectrum Protect

Beim Schreiben von Daten auf ein virtuelles Band auf einem Tape Gateway verwenden Sie das gleiche Verfahren und die gleichen Sicherungsrichtlinien wie beim Schreiben auf physische Bänder. Erstellen Sie die erforderliche Konfiguration für Sicherungs- und Wiederherstellungsaufträge. Weitere Informationen zur Konfiguration von IBM Spectrum Protect finden Sie in Overview of administration tasks für IBM Spectrum Protect.

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe einen Fehler aufweist, schlägt die Backup-Aufgabe möglicherweise fehl. Wenn der Backup-Auftrag fehlschlägt, ändert sich der Bandstatus in IBM Spectrum Protect in ReadOnly. Wenn Sie wissen, dass das Band nicht vollständig ausgelastet ist, können Sie den Bandstatus manuell wieder in ändern ReadWriteund den Sicherungsauftrag mit demselben Band entweder fortsetzen oder erneut einreichen. IBM Spectrum Protect setzt den fehlgeschlagenen Sicherungsauftrag möglicherweise auf einem anderen Band fort, wenn andere Bänder mit dem ReadWrite Status verfügbar sind.

Wiederherstellen von Daten von einem in IBM Spectrum Protect archivierten Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Stellen Sie die Daten mithilfe der IBM Spectrum Protect-Sicherungssoftware wieder her. Dazu erstellen Sie einen Wiederherstellungspunkt, ganz wie bei der Wiederherstellung von Daten von physischen Bändern. Weitere Informationen zur Konfiguration von IBM Spectrum Protect finden Sie in Overview of administration tasks für IBM Spectrum Protect.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen Ihrer Konfiguration mithilfe von Micro Focus (HPE) Data Protector

Sie können Ihre Daten auf virtuellen Bändern sichern, diese Bänder archivieren und Ihre Virtual Tape Library (VTL)-Geräte verwalten, indem Sie Micro Focus (HPE) Data Protector v9.x verwenden. In diesem Thema finden Sie eine grundlegende Dokumentation zur Konfiguration der Micro Focus (HPE) Data Protector-Software für ein Tape Gateway und zur Ausführung von Sicherungs- und Wiederherstellungsoperationen. Detaillierte Informationen zur Verwendung der Micro Focus (HPE) Data Protector-Software finden Sie in der Hewlett Packard-Dokumentation. Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

- Konfigurieren von Micro Focus (HPE) Data Protector für das Arbeiten mit VTL-Geräten
- Vorbereiten virtueller Bänder für die Verwendung mit HPE Data Protector
- Laden von Bändern in einen Medienpool
- Sichern von Daten auf einem Band
- Archivieren eines Bandes
- Wiederherstellen von Daten von einem Band

Konfigurieren von Micro Focus (HPE) Data Protector für das Arbeiten mit VTL-Geräten

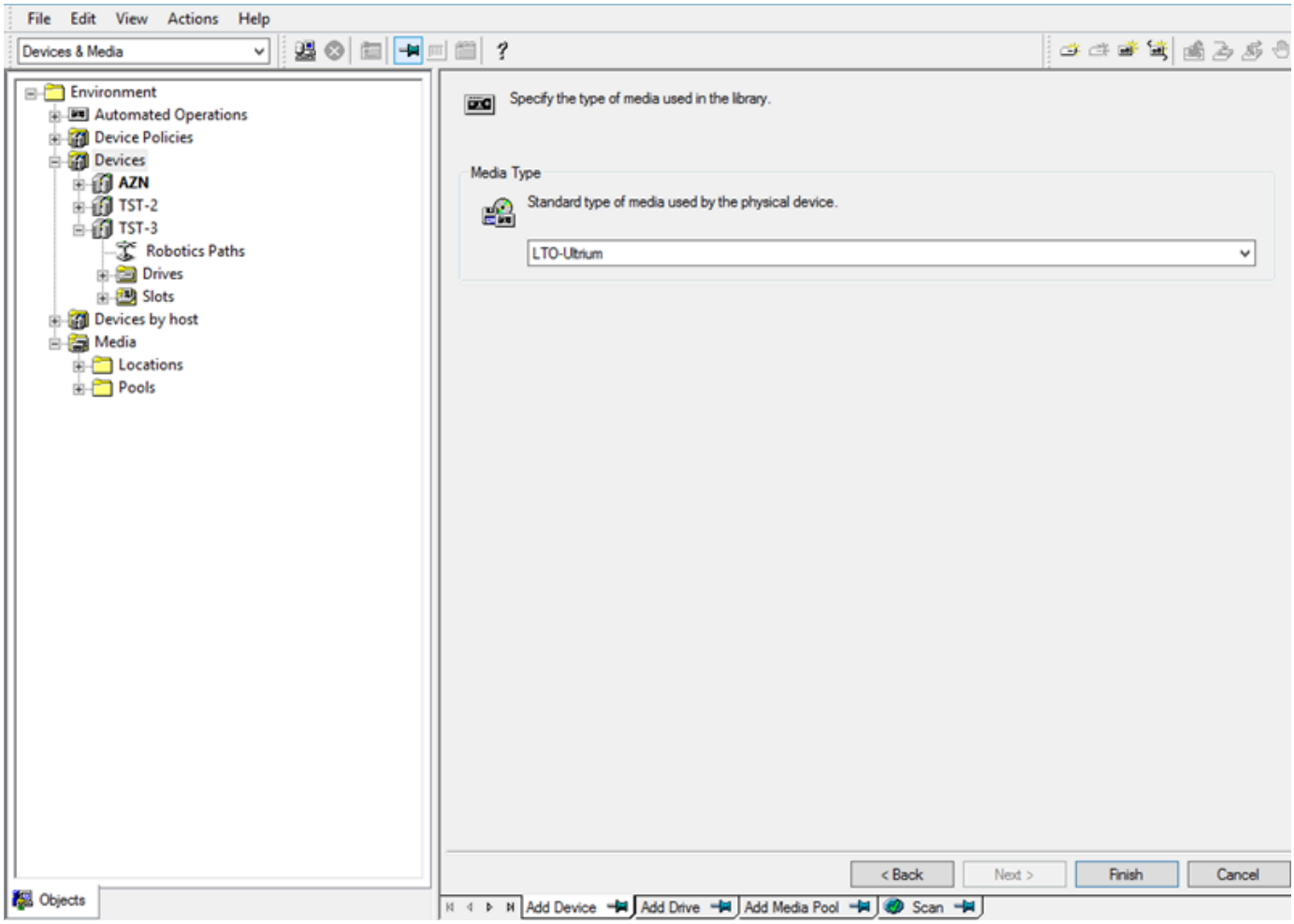
Sobald Sie die VTL (Virtual Tape Library)-Geräte mit dem Client verbunden haben, müssen Sie Micro Focus (HPE) Data Protector so konfigurieren, dass Ihre Geräte erkannt werden. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Client verbinden können, finden Sie unter Verbinden von VTL-Geräten.

Standardmäßig erkennt die Micro Focus (HPE) Data Protector-Software Tape Gateway-Geräte nicht automatisch. Damit die Software diese Geräte erkennt, fügen Sie die VTL-Geräte manuell hinzu und lassen Sie sie anschließend wie folgt erkennen.

So fügen Sie VTL-Geräte hinzu

1. Wählen Sie im Hauptfenster von Micro Focus (HPE) Data Protector das Regal Devices & Media (Geräte und Medien) in der Liste oben links aus.

   Öffnen Sie das Kontextmenü (Rechtsklick) für Devices (Geräte) und wählen Sie Add Device (Gerät hinzufügen)aus.



2. Geben Sie auf der Registerkarte Add Device (Gerät hinzufügen) einen Wert für Device Name (Gerätename) ein. Wählen Sie in Device Type (Gerätetyp) die Option SCSI Library (SCSI-Bibliothek) und dann Next (Weiter) aus.
3. Tun Sie im nächsten Bildschirm Folgendes:

   a. Wählen Sie in SCSI address of the library robotic (SCSI-Adresse der Robotikbibliothek) Ihre spezifische Adresse aus.

   b. Wählen Sie in Select what action Data Protector should take if the drive is busy (Aktion auswählen, die Data Protector ausführen soll, wenn das Laufwerk belegt ist) „Abort (Abbrechen)“ oder die von Ihnen gewünschte Aktion aus.

   c. Wählen Sie, ob Sie diese Optionen aktivieren möchten:

      - Barcode reader support (Strichcode-Leser-Unterstützung)
      - Automatically discover changed SCSI address (Geänderte SCSI-Adressen automatisch entdecken)

- SCSI Reserve/Release (robotic control) (SCSI reservieren/freigeben (Robotiksteuerung)

d. Lassen Sie Use barcode as medium label on initialization (Strichcode als Medienbezeichnung bei Initialisierung verwenden) frei (nicht markiert), es sei denn, Ihr System erfordert die Markierung.

e. Wählen Sie Next (Weiter), um fortzufahren.

4. Geben Sie auf dem nächsten Bildschirm die Slots an, die Sie mit HP Data Protector verwenden möchten. Verwenden Sie einen Bindestrich ("-") zwischen Zahlen, um eine Reihe von Slots anzugeben, z. B. 1-6. Wählen Sie Next Weiter) aus, wenn Sie die Slots angegeben haben, die verwendet werden sollen.
5. Wählen Sie als den vom physischen Gerät verwendeten Standardmedientyp LTO_Ultrium und dann Finish (Beenden) aus, um die Einrichtung abzuschließen.

Ihre Bandbibliothek ist jetzt einsatzbereit. Informationen zum Laden von Bändern in die Bibliothek finden Sie im nächsten Abschnitt.

Vorbereiten virtueller Bänder für die Verwendung mit HPE Data Protector

Bevor Sie Daten auf einem virtuellen Band sichern können, müssen Sie das Band vorbereiten. Dies umfasst folgende Aktionen:

- Laden eines virtuellen Bands in eine Bandbibliothek
- Laden des virtuellen Bands in einen Slot
- Erstellen eines Medienpools
- Laden des virtuellen Bands in den Medienpool

In den folgenden Abschnitten finden Sie Anleitungen für diesen Prozess.

Laden virtueller Bänder in eine Bandbibliothek

Ihre Bandbibliothek sollte nun unter Devices (Geräte) aufgeführt werden. Wenn sie nicht angezeigt wird, drücken Sie F5, um den Bildschirm zu aktualisieren. Wenn Ihre Bibliothek aufgeführt wird, können Sie virtuelle Bänder in die Bibliothek laden.

So laden Sie virtuelle Bänder in Ihre Bandbibliothek

1. Wählen Sie das Pluszeichen neben Ihrer Bandbibliothek, um die Knoten für Robotik-Pfade, Laufwerke und Slots anzuzeigen.

2. Öffnen Sie das Kontextmenü (Rechtsklick) für Drives (Laufwerke), wählen Sie Add Drive (Laufwerk hinzufügen) aus, geben Sie einen Namen für Ihr Band ein und wählen Sie dann Next (Weiter) aus, um fortzufahren.
3. Wählen Sie das Bandlaufwerk, das Sie in SCSI address of data drive (SCSI-Adresse des Datenlaufwerks) hinzufügen möchten. Wählen Sie anschließend Automatically discover changed SCSI address (Geänderte SCSI-Adressen automatisch entdecken) und dann Next (Weiter) aus.
4. Wählen Sie im nächsten Bildschirm Advanced (Erweitert) aus. Das Popup-Fenster Advanced Options (Erweiterte Optionen) wird angezeigt.

   a. Sie sollten auf der Registerkarte Settings (Einstellungen) die folgenden Optionen aktivieren:

      - CRC Check (CRC-Prüfung) (um versehentliche Datenänderungen zu erkennen)
      - Detect dirty drive (Verschmutztes Laufwerk erkennen) (um sicherzustellen, dass das Laufwerk sauber ist, bevor die Sicherung ausgeführt wird)
      - SCSI Reserve/Release (drive) (SCSI reservieren/freigeben (Laufwerk) (um Bandkonflikte zu vermeiden)

      Zu Testzwecken können Sie diese Optionen deaktiviert (nicht markiert) lassen.

   b. Legen Sie auf der Registerkarte Sizes (Größen) die Option Block size (KB) (Blockgröße (KB)) auf Default (256) (Standard (256)) fest.
   c. Wählen Sie OK (OK) aus, um den Bildschirm für erweiterte Optionen zu schließen, und dann Next (Weiter), um fortzufahren.
5. Wählen Sie im nächsten Bildschirm unter Device Policies (Geräterichtlinien) die folgenden Optionen aus:

   - Device may be used for restore (Gerät kann für Wiederherstellung verwendet werden)
   - Device may be used as source device for object copy (Gerät kann als Quell gerät für Objektkopie verwendet werden)
6. Wählen Sie Finish (Beenden) aus, um das Hinzufügen des Bandlaufwerks zur Bandbibliothek abzuschließen.

Laden virtueller Bänder in Slots

Nachdem Sie ein Bandlaufwerk in Ihre Bandbibliothek geladen haben, können Sie virtuelle Bänder in Slots laden.

So Laden Sie ein Band in einen Slot

1. Öffnen Sie im Bandbibliothek-Strukturknoten den Knoten mit der Bezeichnung Slots (Slots). Jeder Slot hat einen Status, der durch ein Symbol dargestellt wird:
   - Ein grünes Band bedeutet, dass bereits ein Band in den Slot geladen wurde.
   - Ein grauer Slot bedeutet, dass der Slot leer ist.
   - Ein cyanfarbenes Fragezeichen bedeutet, dass das Band in diesem Slot nicht formatiert ist.
2. Im Fall eines leeren Slots öffnen Sie das Kontextmenü (Rechtsklick) und wählen Enter (Eingeben) aus. Wenn Bänder vorhanden sind, wählen Sie eins aus, um es in diesen Slot zu laden.

Erstellen eines Medienpools

Ein Medienpool ist eine logische Gruppe, die für die Organisierung Ihrer Bänder verwendet wird. Um eine Bandsicherung einzurichten, erstellen Sie einen Medienpool.

So erstellen Sie einen Medienpool

1. Öffnen Sie im Regal Devices & Media (Geräte und Medien) den Strukturknoten für Media (Medien), öffnen Sie das Kontextmenü (Rechtsklick) für den Knoten Pools (Pools) und wählen Sie dann Add Media Pool (Medienpool hinzufügen) aus.
2. Geben Sie im Feld Pool name (Poolname) einen Namen ein.
3. Wählen Sie in Media Type (Medientyp) die Option LTO_Ultrium und dann Next (Weiter) aus.
4. Akzeptieren Sie im folgenden Bildschirm die Standardwerte und wählen Sie dann Next (Weiter) aus.
5. Wählen Sie Finish (Beenden) aus, um das Erstellen eines Medienpools zu beenden.

Laden von Bändern in einen Medienpool

Bevor Sie Daten auf Ihren Bänder sichern können, müssen Sie die Bänder in den erstellten Medienpool laden.

So laden Sie ein virtuelles Band in einen Medienpool

1. Wählen Sie im Bandbibliothek-Strukturknoten den Knoten Slots (Slots) aus.

2. Wählen Sie ein geladenes Band aus, das ein grünes Symbol mit einem geladenen Band aufweist. Öffnen Sie das Kontextmenü (Rechtsklick), wählen Sie Format (Format) und dann Next (Weiter) aus.
3. Wählen Sie den von Ihnen erstellten Medienpool aus und dann Next (Weiter) aus.
4. Wählen Sie in Medium Description (Medienbeschreibung) die Option Use barcode (Strichcode verwenden) und dann Next (Weiter) aus.
5. Wählen Sie in Options (Optionen) die Option Force Operation (Operation erzwingen) und dann Finish (Beenden) aus.

Der Status des ausgewählten Slots sollte jetzt von "Unassigned" (grau) zu "Tape inserted" (grün) wechseln. Eine Reihe von Nachrichten wird angezeigt, um zu bestätigen, dass Ihre Medien initialisiert werden.

Nun sollte alles konfiguriert sein, sodass Sie Ihre virtuelle Bandbibliothek mit HPE Data Protector nutzen können. Prüfen Sie anhand des folgenden Verfahrens, dass dem so ist.

So prüfen Sie, ob Ihre Bandbibliothek für die Verwendung konfiguriert ist

- Wählen Sie Drives (Laufwerke) aus, öffnen Sie das Kontextmenü (Rechtsklick) für Ihr Laufwerk und wählen Sie dann Scan (Scannen) aus.

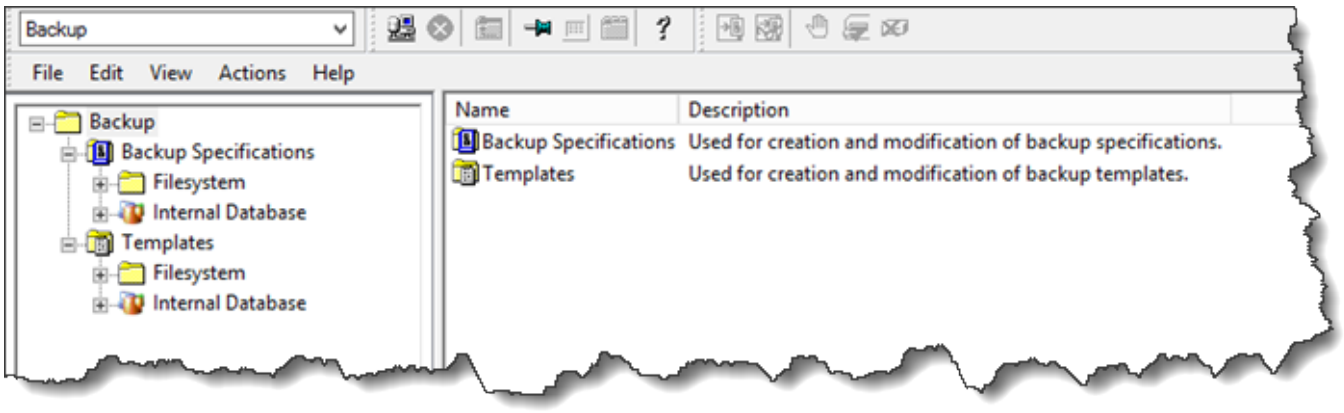
Wenn die Konfiguration korrekt ist, wird durch eine Meldung bestätigt, dass Ihre Medien erfolgreich gescannt wurden.

Sichern von Daten auf einem Band

Wenn die Bänder in einen Medienpool geladen wurden, können Sie Daten auf ihnen sichern.

So sichern Sie Daten auf einem Band

1. Wählen Sie das Regal Backup (Sicherung) oben links im Bildschirm aus.



2. Öffnen Sie das Kontextmenü (Rechtsklick) für File system (Dateisystem) und wählen Sie Add Backup (Sicherung hinzufügen) aus.
3. Wählen Sie im Bildschirm Create New Backup (Neue Sicherung erstellen) unter File system (Dateisystem) die Option Blank File System Backup (Leere Dateisystemsicherung) und dann OK (OK) aus.
4. Wählen Sie im Strukturknoten, der Ihr Hostsystem zeigt, das Dateisystem oder die Dateisysteme aus, die Sie sichern möchten, und dann Next (Weiter) aus, um fortzufahren.
5. Öffnen Sie den Strukturknoten für die Bandbibliothek, die Sie verwenden möchten, öffnen Sie das Kontextmenü (Rechtsklick) für das Bandlaufwerk, das Sie verwenden möchten, und wählen Sie dann Properties (Eigenschaften) aus.
6. Wählen Sie den Medienpool, OK (OK) und dann Next (Weiter) aus.
7. Akzeptieren Sie auf den nächsten drei Bildschirmen die Standardeinstellungen und wählen Sie Next (Weiter) aus.
8. Wählen Sie im Bildschirm Perform finishing steps in your backup/template design (Abschließende Schritte in Ihrem Sicherungs-/Vorlagendesign ausführen) die Option Save as (Speichern unter) aus, um diese Sitzung zu speichern. Geben Sie der Sicherung im Popup-Fenster einen Namen und weisen Sie sie der Gruppe zu, in der Sie Ihre neue Sicherungsspezifikation speichern möchten.
9. Wählen Sie Start Interactive Backup (Interaktive Sicherung starten) aus.

Wenn das Hostsystem ein Datenbanksystem enthält, können Sie es als Zielsicherungssystem auswählen. Die Bildschirme und Auswahlmöglichkeiten ähneln der gerade beschriebenen Dateisystemsicherung.

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe fehl, und das Bandlaufwerk wird in Data Protector als Dirty markiert. Data Protector markiert außerdem die Bandqualität als Schlecht und verhindert so, dass auf das Band geschrieben werden kann. Um weiterhin Daten vom Band lesen zu können, müssen Sie das Laufwerk reinigen und das Band erneut mounten. Um die fehlgeschlagenen Backup-Aufgabe abzuschließen, müssen Sie sie erneut auf ein neues Band übermitteln.

Archivieren eines Bandes

Wenn Sie ein Band archivieren, verschiebt Tape Gateway das Band aus der Bandbibliothek in den Offline-Speicher. Bevor Sie ein Band auswerfen und archivieren, können Sie dessen Inhalt prüfen.

So prüfen Sie den Inhalt eines Bands vor dem Archivieren

1. Wählen Sie Slots (Slots) und dann das Band aus, das Sie prüfen möchten.
2. Wählen Sie Objects (Objekte) aus und überprüfen Sie, welche Inhalte sich auf dem Band befinden.

Wenn Sie ein Band für die Archivierung ausgewählt haben, gehen Sie folgendermaßen vor.

So werfen Sie ein Band aus und archivieren es

1. Öffnen Sie das Kontextmenü (Rechtsklick) für dieses Band. Wählen Sie Eject (Auswerfen) aus.
2. Wählen Sie in der Storage-Konsole Ihr Gateway und dann VTL-Bandkartuschen aus. Überprüfen Sie den Status des virtuellen Bands, das Sie archivieren.

Nachdem das Band ausgeworfen wurde, wird es automatisch im Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) archiviert. Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach dem Archivieren wird das Band nicht mehr in der VTL aufgeführt, aber in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert.

Wiederherstellen von Daten von einem Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

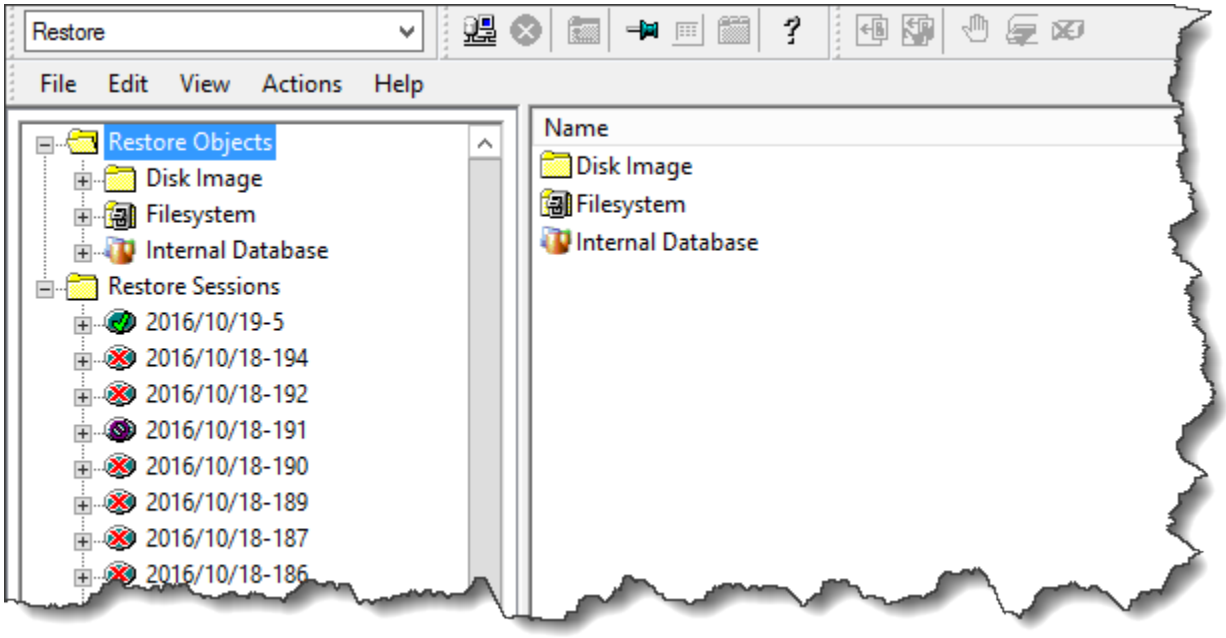
Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie HPE Data Protector, um die Daten wiederherzustellen. Der Vorgang ist identisch mit dem Vorgang zur Wiederherstellung von Daten von physischen Bändern.

Befolgen Sie zum Wiederherstellen von Daten von einem Band das folgende Verfahren.

So stellen Sie Daten von einem Band wieder her

1. Wählen Sie das Regal Restore (Wiederherstellen) oben links im Bildschirm aus.



2. Wählen Sie das Dateisystem oder Datenbanksystem, das Sie wiederherstellen möchten. Achten Sie darauf, dass das Kontrollkästchen für die wiederherzustellende Sicherung ausgewählt ist. Wählen Sie Restore (Wiederherstellen) aus.
3. Wählen Sie im Fenster Start Restore Session (Wiederherstellungssitzung starten) die Option Needed Media (Benötigte Medien) aus. Wählen Sie All media (Alle Medien) aus. Anschließend sollte Ihnen das Band angezeigt werden, das ursprünglich für die Sicherung verwendet wurde. Wählen Sie dieses Band und dann Close (Schließen) aus.

4. Akzeptieren Sie im Fenster Start Restore Session (Wiederherstellungssitzung starten) die Standardeinstellungen aus. Wählen Sie Next (Weiter) und dann Finish Beenden) aus.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen Ihrer Konfiguration mithilfe von Microsoft System Center Data Protection Manager

Sie können Microsoft System Center 2012 R2 oder 2016 Data Protection Manager (DPM) verwenden, um Ihre Daten auf virtuelle Bänder zu sichern, diese Bänder zu archivieren und Ihre VTL (Virtual Tape Library)-Geräte zu verwalten. In diesem Thema finden Sie eine grundlegende Anleitung zur Konfiguration der DPM-Sicherungsanwendung für ein Tape Gateway sowie zur Durchführung einer Sicherung und Wiederherstellung.

Detaillierte Informationen zum Arbeiten mit DPM finden Sie in der DPM-Dokumentation auf der Microsoft System Center-Website. Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

- Konfigurieren von DPM zur Erkennung von VTL-Geräten
- Importieren eines Bands in DPM
- Schreiben von Daten auf ein Band in DPM
- Archivieren eines Bands mithilfe von DPM
- Wiederherstellen von Daten von einem in DPM archivierten Band

Konfigurieren von DPM zur Erkennung von VTL-Geräten

Sobald Sie die VTL (Virtual Tape Library)-Geräte mit dem Windows-Client verbunden haben, müssen Sie die DPM-Software so konfigurieren, dass sie Ihre Geräte erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Verbinden von VTL-Geräten.

Tape Gateway-Geräte werden standardmäßig nicht vom DPM-Server erkannt. Sie müssen die folgenden Schritte durchführen, um den Server so zu konfigurieren, dass er mit Tape Gateway-Geräten zusammenarbeitet:

1. Sie müssen die Gerätetreiber der VTL-Geräte aktualisieren, um die Geräte für den DPM-Server verfügbar zu machen.
2. Sie müssen die VTL-Geräte manuell der DPM-Bandbibliothek zuweisen.

Aktualisieren Sie die Treiber der VTL-Geräte wie folgt:

- Aktualisieren Sie im Geräte-Manager den Treiber des Medienwechslers. Anweisungen finden Sie unter Aktualisieren des Gerätetreibers für den Medienwechsler.

Sie verwenden das DPMDriveMappingTool , um Ihre Bandlaufwerke der DPM-Bandbibliothek zuzuordnen.

Weisen Sie der Bandbibliothek des DPM-Servers wie folgt Bandlaufwerke zu:

1. Erstellen Sie mindestens ein Band auf Ihrem Gateway. Wie Sie das in der Konsole tun können, erfahren Sie unter Erstellen von Bändern.
2. Importieren Sie das Band in die DPM-Bibliothek. Weitere Informationen hierzu finden Sie unter Importieren eines Bands in DPM.
3. Falls der DPMLA-Dienst ausgeführt wird, müssen Sie ein Befehlsterminal öffnen und den folgenden Befehl in die Befehlszeile eingeben, um den Dienst anzuhalten:

   ```
   net stop DPMLA
   ```

4. Navigieren Sie auf dem DPM-Server zur Datei `%ProgramFiles%\System Center 2016 R2\DPM\DPM\Config\DPMLA.xml`.

   > **Note**
   >
   > Wenn diese Datei vorhanden ist, DriveMappingTool überschreibt das DPM sie. Soll die ursprüngliche Datei erhalten bleiben, müssen Sie eine Sicherungskopie erstellen.

5. Öffnen Sie ein Befehlsterminal, wechseln Sie in das Verzeichnis `%ProgramFiles%\System Center 2016 R2\DPM\DPM\Bin` und führen Sie den folgenden Befehl aus:

   ```
   C:\Microsoft System Center 2016 R2\DPM\DPM\bin>DPMDriveMappingTool.exe
   ```

Die Ausgabe dieses Befehls sieht wie folgt aus:

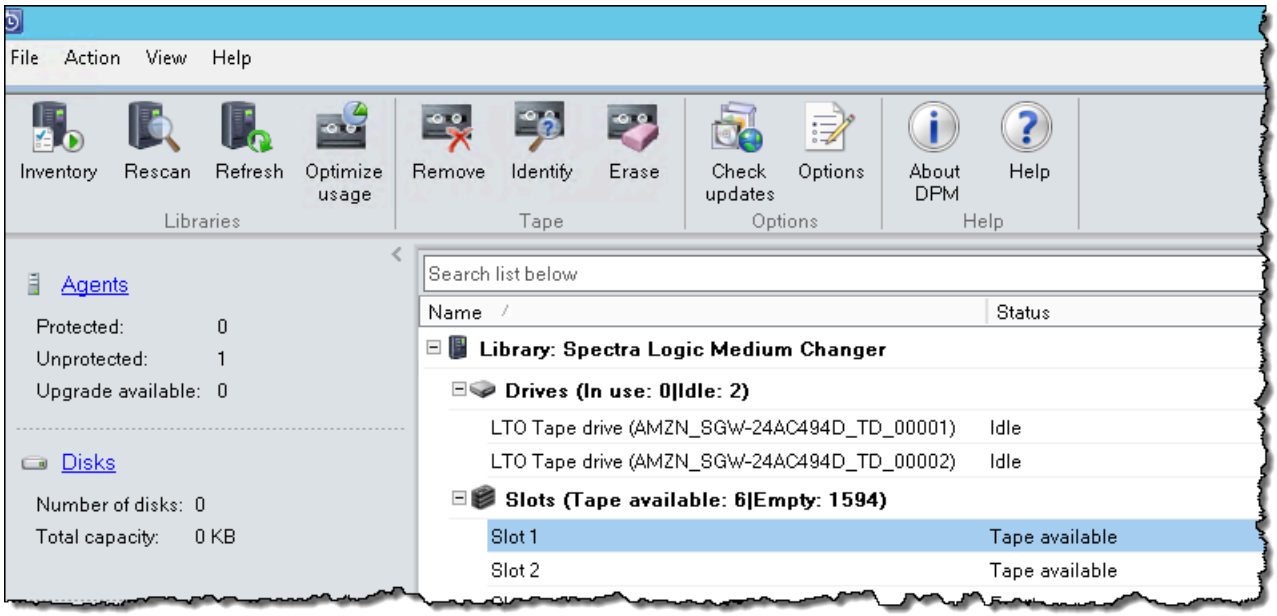
```
Performing Device Inventory ...
Mapping Drives to Library ...
Adding Standalone Drives ...
Writing the Map File ...
Drive Mapping Completed Successfully.
```

Importieren eines Bands in DPM

Nun können Sie Bänder von Ihrem Tape Gateway in die Bibliothek der DPM-Sicherungsanwendung importieren.

So importieren Sie Bänder in die Bibliothek der DPM-Sicherungsanwendung

1. Öffnen Sie auf dem DPM-Server die Verwaltungskonsole. Wählen Sie Recan (Erneut scannen) und dann Refresh (Aktualisieren) aus. Nun werden Ihr Medienwechsler und Ihre Bandlaufwerke angezeigt.



2. Öffnen Sie im Abschnitt Library (Bibliothek) das Kontextmenü (Rechtsklick) für den Medienwechsler. Wählen Sie Add tape (I/E port) (Band hinzufügen (E/A-Port)) aus, um der Liste Slots (Slots) ein Band hinzuzufügen.

> **Note**
>
> Es kann mehrere Minuten dauern, bis die Bänder hinzugefügt werden.

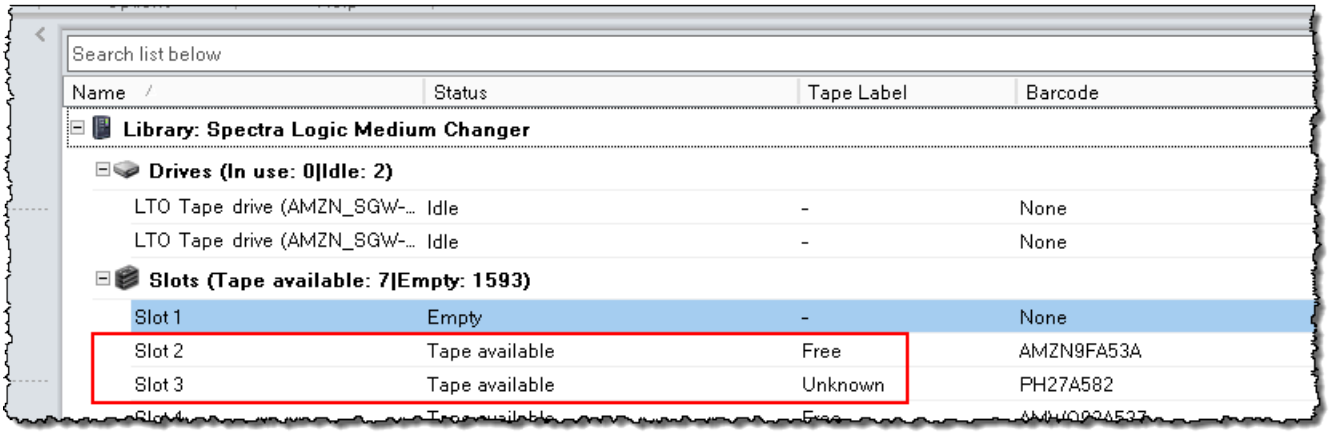
Die Bandbezeichnung wird als Unknown (Unbekannt) angezeigt und das Band kann nicht verwendet werden. Damit Sie das Band verwenden können, müssen Sie es identifizieren.

3. Öffnen Sie das Kontextmenü (Rechtsklick) des Bands, das Sie identifizieren möchten, und wählen Sie dann Identify unknown tape (Unbekanntes Band identifizieren) aus.

> **Note**
>
> Die Identifizierung eines Bandes kann einige Sekunden oder Minuten dauern.
> Wenn auf den Bändern keine Barcodes korrekt angezeigt werden, müssen Sie den Treiber des Medienwechslers in So/StorageTek Bibliothek ändern. Weitere Informationen finden Sie unter Anzeigen von Barcodes für Bänder in Microsoft System Center DPM.

Nach Abschluss der Identifizierung wird die Bandbezeichnung in Free (Frei) geändert. Das bedeutet, dass nun Daten auf das Band geschrieben werden können.

Auf dem Screenshot unten sehen Sie, dass das Band in Einschubfach 2 identifiziert und zur Verwendung freigegeben wurde, das Band in Einschubfach 3 jedoch nicht.



Schreiben von Daten auf ein Band in DPM

Beim Schreiben von Daten auf ein virtuelles Band auf einem Tape Gateway; verwenden Sie dieselben Schutzvorkehrungen und Richtlinien wie beim Schreiben auf physische Bänder. Zunächst erstellen Sie eine Schutzgruppe und fügen die Daten hinzu, die Sie sichern möchten. Dann erstellen Sie einen Wiederherstellungspunkt, um die Daten zu sichern. Detaillierte Informationen zum Arbeiten mit DPM finden Sie in der DPM-Dokumentation auf der Microsoft System Center-Website.

Standardmäßig beträgt die Kapazität eines Bandes 30 GB. Wenn Sie Daten sichern, die größer als die Kapazität eines Bandes sind, tritt ein Geräte-E/A-Fehler auf. Wenn die Position, an der der Fehler aufgetreten ist, größer als die Größe des Bandes ist, behandelt Microsoft DPM den Fehler als Hinweis auf das Bandende. Wenn die Position, an der der Fehler aufgetreten ist, kleiner als die Größe des Bandes ist, schlägt der Sicherungsauftrag fehl. Um dieses Problem zu beheben, ändern Sie den `TapeSize`-Wert im Registry-Eintrag, sodass er der Größe Ihres Bandes entspricht. Informationen zu diesem Verfahren finden Sie unter Fehler-ID: 30101 im Microsoft System Center.

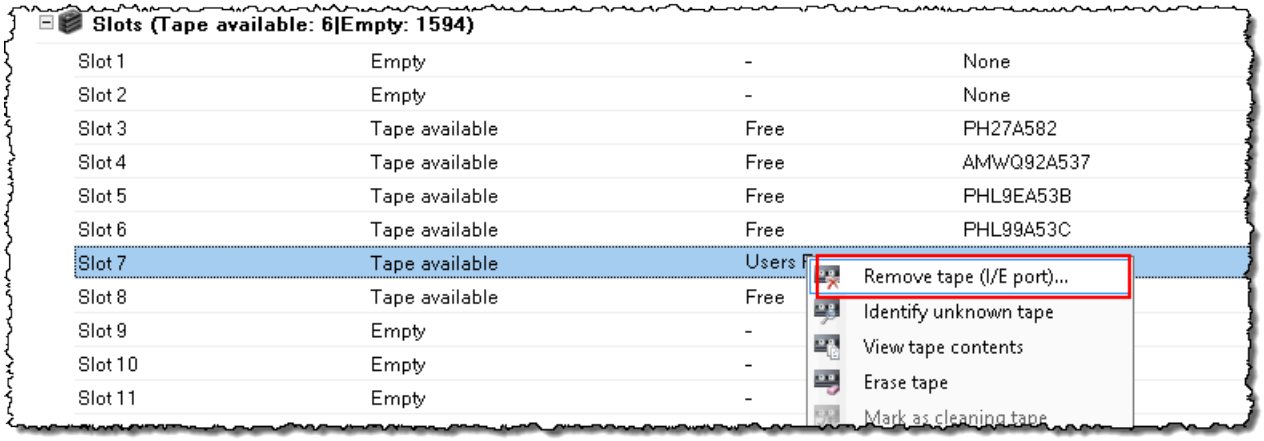
> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe fehl. Um die fehlgeschlagenen Backup-Aufgabe abzuschließen, müssen Sie sie erneut übermitteln.

Archivieren eines Bands mithilfe von DPM

Wenn Sie ein Band archivieren, verschiebt Tape Gateway das Band aus der DPM-Bandbibliothek in einen Offline-Speicher. Der erste Schritt bei der Bandarchivierung besteht darin, das Band mithilfe Ihrer Sicherungsanwendung (DPM) aus dem Slot zu entfernen.

Archivieren Sie ein Band wie folgt in DPM:

1. Öffnen Sie das Kontextmenü (Rechtsklick) des Bands, das Sie archivieren möchten, und wählen Sie dann Remove tape (I/E port) (Band entfernen (E/A-Station)) aus.



2. Wählen Sie im anschließend angezeigten Dialogfeld Yes (Ja) aus. Dadurch wird das Band aus dem Speichereinschubfach des Medienwechslers ausgeworfen und in eines der E/A-Einschubfächer des Gateways verschoben. Sobald ein Band in ein E/A-Einschubfach des Gateways verschoben wird, wird es sofort archiviert.
3. Wählen Sie in der Storage-Konsole Ihr Gateway und dann VTL-Bandkartuschen aus. Überprüfen Sie den Status des virtuellen Bands, das Sie archivieren.

   Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach Abschluss der Archivierung wird das Band nicht mehr in der VTL aufgeführt.

Wiederherstellen von Daten von einem in DPM archivierten Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie die DPM-Sicherungsanwendung, um die Daten wiederherzustellen. Dazu erstellen Sie einen Wiederherstellungspunkt, ganz wie bei der Wiederherstellung von Daten von physischen Bändern. Anleitung hierfür finden Sie unter Wiederherstellen von Clientcomputerdaten auf der DPM-Website.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen Ihrer Einrichtung mithilfe NovaStor von DataCenter/Network

Sie können Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL)-Geräte mithilfe von NovaStor DataCenter/Network Version 6.4 oder 7.1 verwalten. In diesem Thema finden Sie eine grundlegende Dokumentation zur Konfiguration der Backup-Anwendung NovaStor DataCenter/Network Version 7.1 für ein Tape Gateway sowie zur Durchführung von Backup- und Wiederherstellungsvorgängen. Ausführliche Informationen zur Verwendung von NovaStor DataCenter/Network Version 7.1 finden Sie unter Dokumentation NovaStor DataCenter/Network .

Einrichten von NovaStor DataCenter/Network

Nachdem Sie Ihre Virtual Tape Library (VTL)-Geräte mit Ihrem Microsoft Windows-Client verbunden haben, konfigurieren Sie die NovaStor Software so, dass sie Ihre Geräte erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden, finden Sie unter Verbinden von VTL-Geräten.

NovaStor DataCenter/Network erfordert Treiber von den Treiberherstellern. Sie können auch die Windows-Treiber nutzen, müssen dann aber zunächst andere Datensicherungsanwendungen deaktivieren.

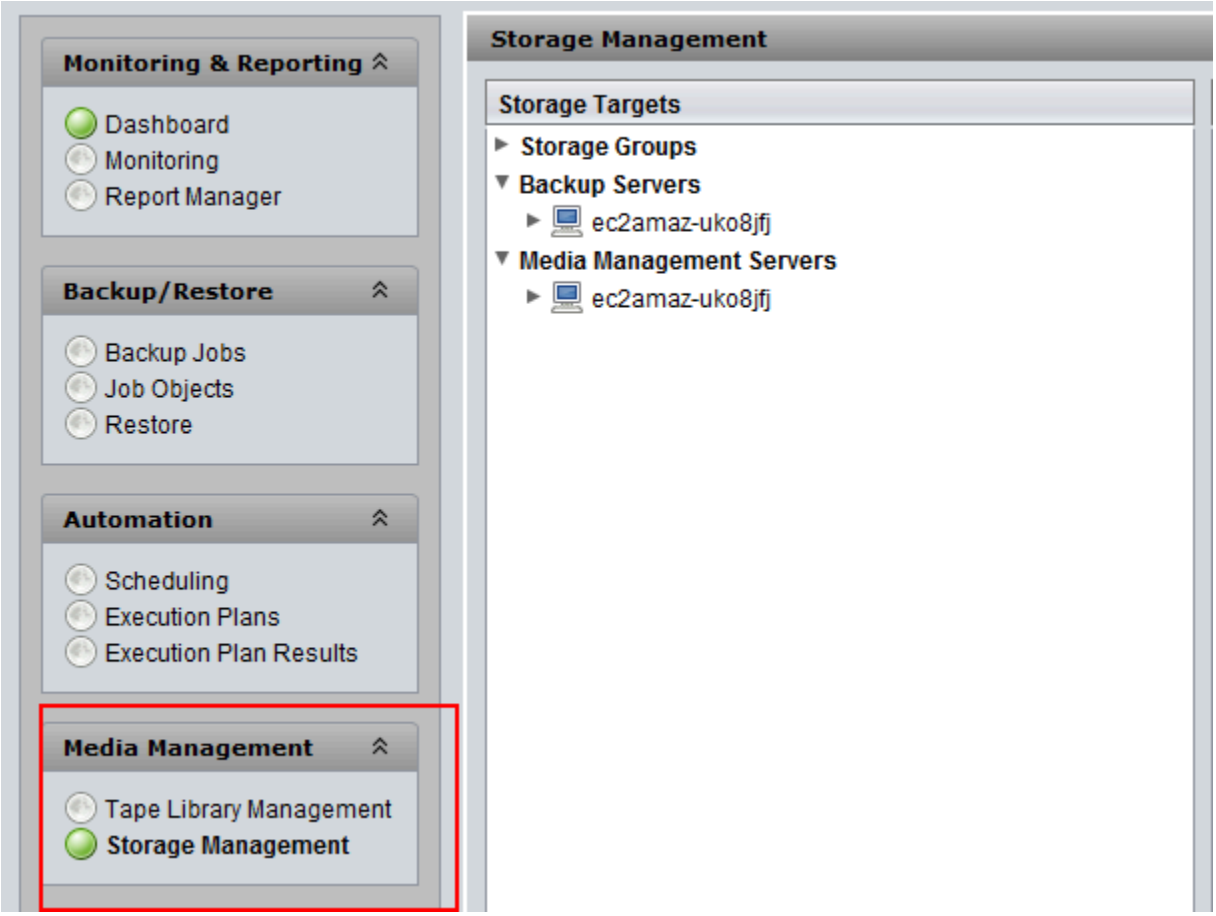
Konfigurieren von NovaStor DataCenter/Network für die Arbeit mit VTL-Geräten

Wenn Sie Ihre VTL-Geräte so konfigurieren, dass sie mit NovaStor DataCenter/Network Version 6.4 oder 7.1 funktionieren, wird möglicherweise eine Fehlermeldung mit dem Hinweis angezeigt`External Program did not exit correctly`. Für dieses Problem ist eine Behelfslösung erforderlich, damit Sie fortfahren können.

Zur Vermeidung des Problems können Sie eine Behelfslösung erstellen, ehe Sie mit der Konfiguration Ihrer VTL-Geräte beginnen. Weitere Informationen zum Erstellen dieser Befehlslösung finden Sie unter Beheben eines "External Program Did Not Exit Correctly"-Fehlers.

So konfigurieren Sie NovaStor DataCenter/Network für die Arbeit mit VTL-Geräten

1. Wählen Sie in der NovaStor DataCenter/Network Admin-Konsole Media Management und dann Storage Management aus.

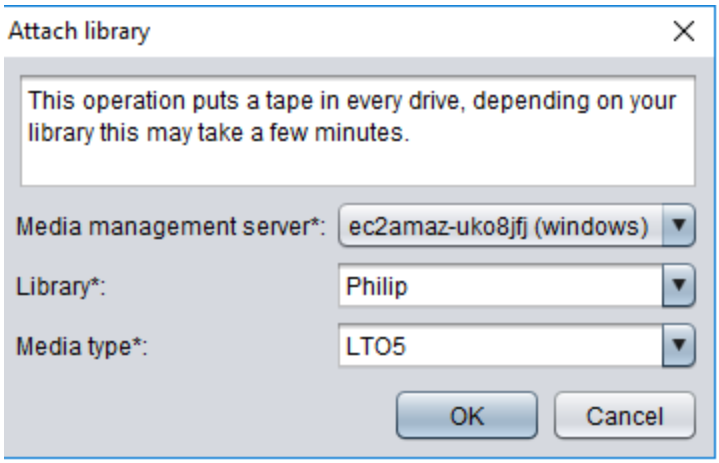


2. Öffnen Sie im Menü Storage Targets (Speicherziele) das Kontextmenü (Rechtsklick) für Media Management Servers (Medienverwaltungsserver). Wählen Sie New (Neu) und OK (OK) aus, um einen storage (Speicher)-Knoten zu erstellen und vorab auszufüllen.

   Wenn eine Fehlermeldung mit dem Text `External Program did not exit correctly` angezeigt wird, lösen Sie das Problem, bevor Sie fortfahren. Für dieses Problem ist eine Behelfslösung erforderlich. Informationen zum Beheben dieses Problems finden Sie unter Beheben eines "External Program Did Not Exit Correctly"-Fehlers.

   > **Important**
   >
   > Dieser Fehler tritt auf, weil der Bereich der Elementzuweisung für AWS Storage Gateway Speicherlaufwerke und Bandlaufwerke die von DataCenter/Network zulässige Anzahl NovaStor überschreitet.

3. Öffnen Sie das Kontextmenü (Rechtsklick) für den erstellten storage (Speicher)-Knoten und wählen Sie New Library (Neue Bibliothek) aus.
4. Wählen Sie den Bibliotheksserver aus der Liste aus. Die Bibliotheksliste wird automatisch gefüllt.
5. Geben Sie der Bibliothek einen Namen und wählen Sie dann OK (OK) aus.
6. Wählen Sie die Bibliothek zur Anzeige aller Eigenschaften der virtuellen Storage Gateway-Bandbibliothek aus.
7. Erweitern Sie im Menü Storage Targets (Speicherziele) die Option Backup Servers (Sicherungsserver), öffnen Sie das Kontextmenü (Rechtsklick) für den Server und wählen Sie Attach Library (Bibliothek anfügen) aus.
8. Wählen Sie im nun angezeigten Dialogfeld Attach Library (Bibliothek anfügen) den Medientyp LTO5 und dann OK (OK) aus.



9. Erweitern Sie Backup Servers (Sicherungsserver), um die virtuelle -Bandbibliothek und die Bibliothekspartition anzuzeigen, die alle aufgespielten Bandlaufwerke anzeigt.

Erstellen eines Bandpools

Ein Bandpool wird dynamisch in der NovaStor DataCenter/Network-Software erstellt und enthält daher keine feste Anzahl von Medien. Ein Bandpool, der ein Band benötigt, holt sich dieses aus dem Scratch-Pool. Ein Scratch-Pool ist ein Behälter für Bänder, die für mindestens einen Bandpool frei verfügbar sind. Ein Bandpool gibt alle Medien an den Scratch-Pool zurück, für die der Aufbewahrungszeitraum abgelaufen ist und die nicht mehr länger benötigt werden.

Ein Bandpool kann in drei Schritten erstellt werden:

1. Sie erstellen einen Scratch-Pool.
2. Sie weisen dem Scratch-Pool Bänder zu.

3. Sie erstellen einen Bandpool.

So erstellen Sie einen Scratch-Pool.

1. Wählen Sie im linken Navigationsmenü die Registerkarte Scratch Pools (Scratch-Pools) aus.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für Scratch Pools (Scratch-Pools) und wählen Sie Create Scratch Pool (Scratch-Pool erstellen) aus.
3. Geben Sie dem Scratch-Pool im Dialogfeld Scratch Pools (Scratch-Polls) einen Namen und wählen Sie dann den Medientyp aus.
4. Wählen Sie Label Volume (Volume bezeichnen) aus und erstellen Sie eine „Niedrigstandmarke“ für den Scratch-Pool. Wenn der Scratch-Pool soweit geleert ist, dass diese Marke erreicht wird, wird eine Warnung angezeigt.
5. Wählen Sie im Warndialogfeld OK (OK) aus, um den Scratch-Pool zu erstellen.

Sie weisen Sie dem Scratch-Pool Bänder zu

1. Wählen Sie im linken Navigationsmenü Tape Library Management (Bandbibliothekverwaltung) aus.
2. Wählen Sie die Registerkarte Library (Bibliothek) aus, um den Bibliotheksbestand anzuzeigen.
3. Wählen Sie die Bänder aus, die Sie dem Scratch-Pool zuweisen möchten. Stellen Sie sicher, dass für die Bänder der korrekte Medientyp festgelegt ist.
4. Öffnen Sie das Kontextmenü (Rechtsklick) für die Bibliothek und wählen Sie Add to Scratch Pool (Zum Scratch-Pool hinzufügen) aus.

Sie verfügen jetzt über einen gefüllten Scratch-Pool, den Sie für Bandpools nutzen können.

So erstellen Sie einen Band-Pool

1. Wählen Sie im linken Navigationsmenü Tape Library Management (Bandbibliothekverwaltung) aus.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für die Registerkarte Media Pools (Medienpools) und wählen Sie Create Media Pool (Medienpool erstellen) aus.
3. Geben Sie dem Medienpool einen Namen und wählen Sie Backup Server (Sicherungsserver) aus.
4. Wählen Sie eine Bibliothekspartition für den Medienpool aus.

5. Wählen Sie den Scratch-Pool aus, aus dem der Pool die Bänder erhalten soll.
6. Wählen Sie in Schedule (Plan) die Option Not Scheduled (Nicht geplant) aus.

Konfigurieren des Medienimports und -exports zum Archivieren von Bändern

NovaStor DataCenter/Network kann Import-/Export-Slots verwenden, wenn sie Teil des Medienwechslers sind.

Für einen Export muss NovaStor DataCenter/Netzwerk wissen, welche Bänder physisch aus der Bibliothek entfernt werden.

Für einen Import erkennt NovaStor DataCenter/Netzwerk Bandmedien, die in der Bandbibliothek exportiert werden, und bietet an, sie alle zu importieren, entweder aus einem Datenslot oder einem Exportslot. Ihr Tape Gateway archiviert Bänder im Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive).

So konfigurieren Sie den Medienimport- und export

1. Navigieren Sie zu Tape Library Management (Bandbibliothekverwaltung). Wählen Sie einen Server als Media Management Server (Medienverwaltungsserver) und dann Library (Bibliothek) aus.
2. Wählen Sie die Registerkarte Off-site Locations (Speicherort außerhalb) aus.
3. Öffnen Sie das Kontextmenü (Rechtsklick) für den weißen Bereich und wählen Sie Add (Hinzufügen) aus, um einen neuen Bereich zu öffnen.
4. Geben Sie im Bereich **`S3 Glacier Flexible Retrieval`** oder **`S3 Glacier Deep Archive`** ein und fügen Sie im Textfeld optional eine Beschreibung hinzu.

Sichern von Daten auf einem Band

Zum Erstellen eines Sicherungsauftrags und zum Schreiben von Daten auf ein virtuelles Band verwenden Sie dieselben Verfahren wie bei physischen Bändern. Ausführliche Informationen zum Sichern von Daten mithilfe der NovaStor Software finden Sie unter Dokumentation NovaStor DataCenter/Netzwerk .

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe fehl, und das Band kann nicht mehr

beschrieben werden. Sie können das Band archivieren oder weiterhin Daten daraus lesen. Um die fehlgeschlagenen Backup-Aufgabe abzuschließen, müssen Sie sie erneut auf ein neues Band übermitteln.

Archivieren eines Bandes

Wenn Sie ein Band archivieren, wirft Tape Gateway das Band aus der Bandbibliothek in den Speicherschacht aus. Anschließend wird das Band mithilfe Ihrer Sicherungsanwendung – d. h. NovaStor DataCenter/Network – aus dem Slot in das Archiv exportiert.

So archivieren Sie ein Band

1. Wählen Sie im linken Navigationsmenü Tape Library Management (Bandbibliothekverwaltung) aus.
2. Wählen Sie die Registerkarte Library (Bibliothek) aus, um den Bibliotheksbestand anzuzeigen.
3. Markieren Sie die Bänder, die Sie archivieren möchten, öffnen Sie das Kontextmenü (Rechtsklick) für die Bänder und wählen Sie den externen Archivstandort.

Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach Abschluss der Archivierung wird das Band nicht mehr in der VTL aufgeführt.

Überprüfen Sie in NovaStor DataCenter/Network, ob sich das Band nicht mehr im Speicher-Slot befindet.

Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Tapes aus. Überprüfen Sie, ob für das archivierte Band der Status ARCHIVED (ARCHIVIERT) angezeigt wird.

Wiederherstellen von Daten von einem archivierten und abgerufenen Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.

2. Verwenden Sie die NovaStor DataCenter/Network-Software, um die Daten wiederherzustellen. Dazu aktualisieren Sie den E-Mail-Slot und verschieben genau wie beim Wiederherstellen von Daten von physischen Bändern jedes abzurufende Band in einen leeren Slot. Informationen zum Wiederherstellen von Daten finden Sie unter Dokumentation NovaStor DataCenter/Netzwerk .

Gleichzeitiges Schreiben von mehreren Sicherungsaufträgen auf ein Bandlaufwerk

In der NovaStor Software können Sie mehrere Aufträge gleichzeitig mit der Multiplexing-Funktion auf ein Bandlaufwerk schreiben. Diese Funktion ist verfügbar, wenn ein Multiplexer für einen Medienpool verfügbar ist. Weitere Informationen zur Verwendung von Multiplexing finden Sie in der Dokumentation NovaStor DataCenter/dem Netzwerk .

Beheben eines "External Program Did Not Exit Correctly"-Fehlers

Wenn Sie Ihre VTL-Geräte so konfigurieren, dass sie mit NovaStor DataCenter/Network Version 6.4 oder 7.1 funktionieren, wird möglicherweise eine Fehlermeldung mit dem Hinweis angezeigt`External Program did not exit correctly`. Dieser Fehler tritt auf, weil der Bereich für die Elementzuweisung von Storage Gateway für Speicherlaufwerke und Bandlaufwerke die von DataCenter/Network zulässige Anzahl NovaStor überschreitet.

Storage Gateway gibt 3200 Speicher- und Import/Export-Slots zurück, was über dem von NovaStor DataCenter/Network erlaubten Limit von 2400 liegt. Um dieses Problem zu beheben, fügen Sie eine Konfigurationsdatei hinzu, die die NovaStor Software aktiviert, um die Anzahl der Speicher- und Import/Export-Slots zu begrenzen, und den Elementzuweisungsbereich vorkonfiguriert.

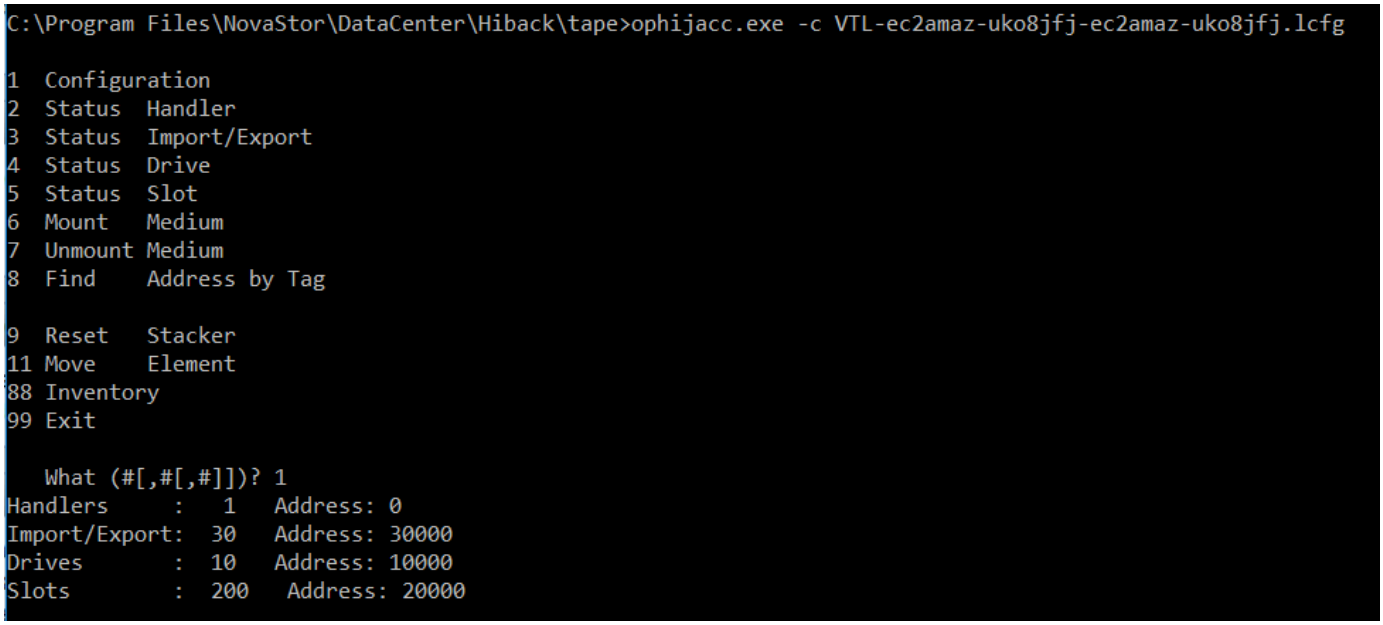
So wenden Sie die Behelfslösung für einen "External program did not exit correctly"-Fehler an

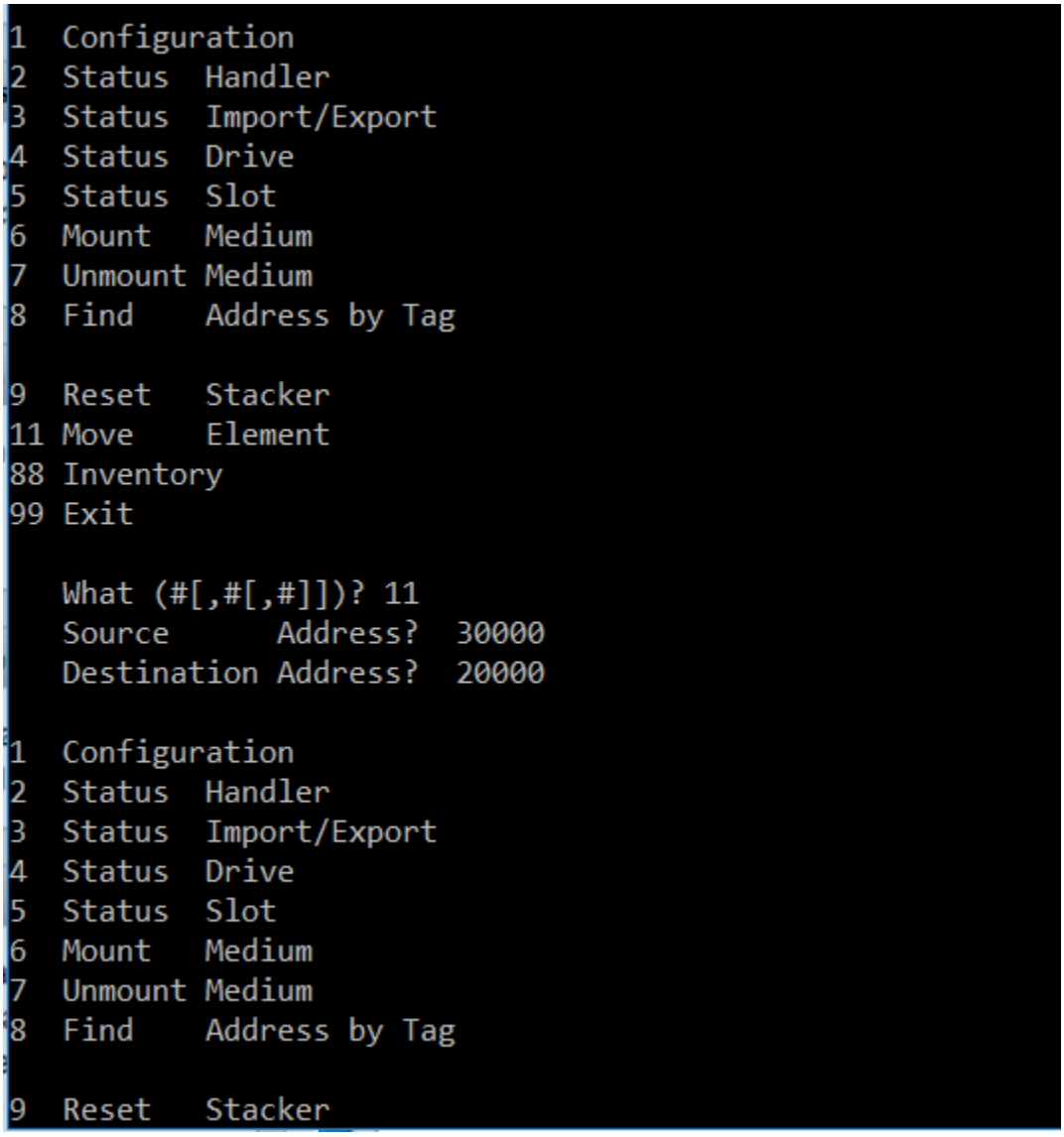
1. Navigieren Sie zum Ordner Band auf Ihrem Computer, auf dem Sie die NovaStor Software installiert haben.
2. Erstellen Sie im Bandordner eine Textdatei und geben Sie ihr den Namen `hijacc.ini`.
3. Kopieren Sie den folgenden Inhalt in eine `hijacc.ini`-Datei und speichern Sie diese.

```
port:12001
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
```

```
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. Fügen Sie die Bibliothek zum Medienverwaltungsserver hinzu.
5. Verschieben Sie mit dem folgenden Befehl ein Band aus dem Import/Export-Slot in die Bibliothek, wie im unten stehenden Screenshot gezeigt. Ersetzen Sie im Befehl VTL durch den Namen Ihrer Bibliothek.





6. Fügen Sie die Bibliothek zum Sicherungsserver hinzu.
7. Importieren Sie in der NovaStor Software alle Bänder aus Import-/Export-Slots in die Bibliothek.

Testen Ihrer Einrichtung mithilfe von Bol NetVault Backup

Sie können Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL)-Geräte verwalten, indem Sie die folgenden Versionen von Quest (früher Dell) NetVault Backup verwenden:

- Bol NetVault Backup 12.4
- Bol NetVault Backup 13.x

In diesem Thema finden Sie eine grundlegende Dokumentation zur Konfiguration der Bol NetVault Backup-Anwendung für ein Tape Gateway und zur Durchführung eines Sicherungs- und Wiederherstellungsvorgangs.

Ausführliche Informationen zur Verwendung der Bol NetVault Backup-Anwendung finden Sie im Quest NetVault Backup – Administration Guide. Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

Konfigurieren von Bol NetVault Backup für die Verwendung mit VTL-Geräten

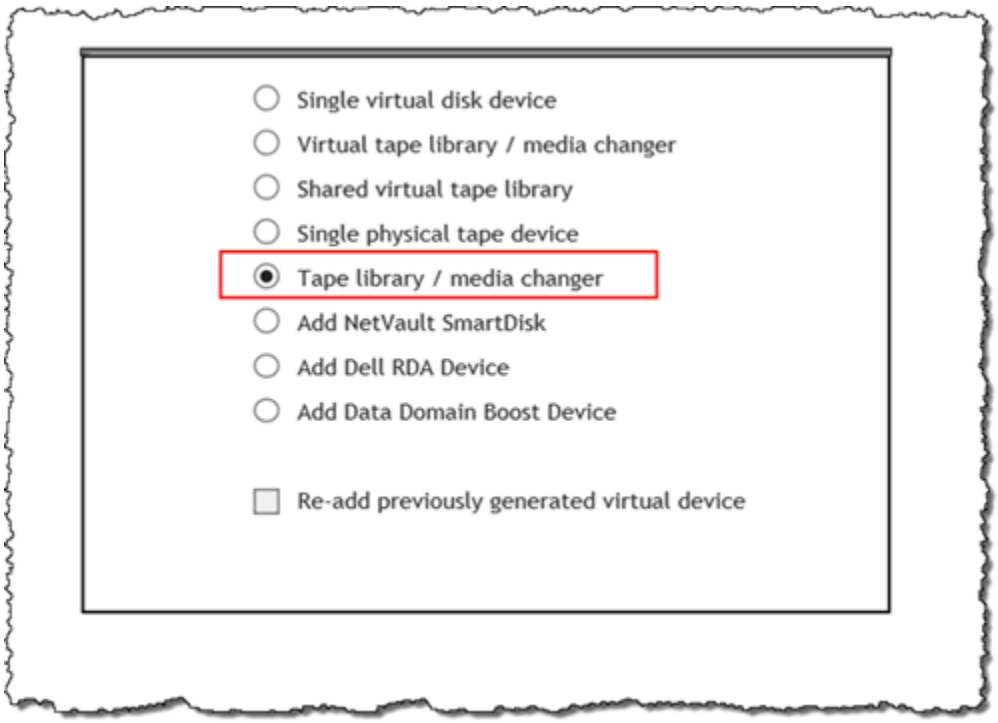
Nachdem Sie die Virtual Tape Library (VTL)-Geräte mit dem Windows-Client verbunden haben, konfigurieren Sie Bol NetVault Backup so, dass Ihre Geräte erkannt werden. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Verbinden von VTL-Geräten.

Die Bol NetVault Backup-Anwendung erkennt Tape Gateway-Geräte nicht automatisch. Sie müssen die Geräte manuell hinzufügen, um sie der Bol NetVault Backup-Anwendung zur Verfügung zu stellen, und dann die VTL-Geräte ermitteln.

Hinzufügen von VTL-Geräten

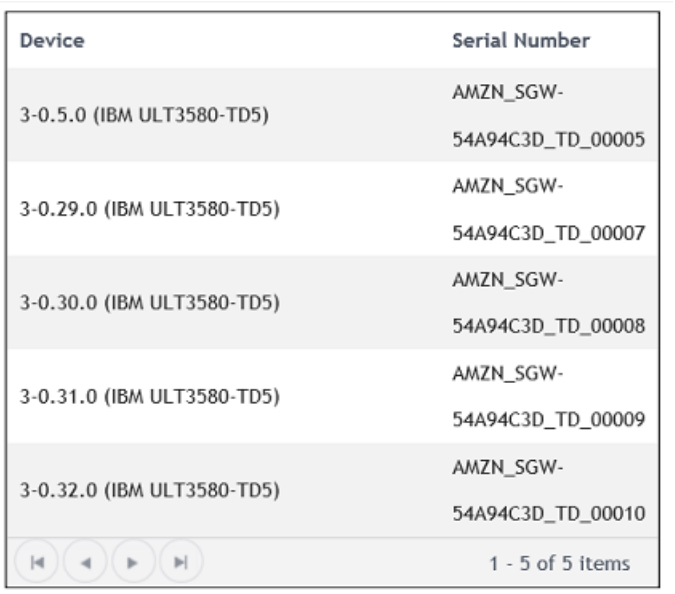
So fügen Sie VTL-Geräte hinzu

1. Wählen Sie in Bol NetVault Backup auf der Registerkarte Konfiguration die Option Geräte verwalten aus.
2. Wählen Sie auf der Seite „Manage Devices (Geräte verwalten)“ Add Devices (Geräte hinzufügen) aus.
3. Wählen Sie im Assistenten zum Hinzufügen von Speicher Tape library/media changer (Bandbibliothek/Medienwechsler) und dann Next (Weiter) aus.



4. Wählen Sie auf der nächsten Seite den Clientcomputer aus, der physisch mit der Bibliothek verbunden ist. Wählen Sie dann Next (Weiter) aus, um nach Geräten zu suchen.
5. Wenn Geräte gefunden werden, werden sie angezeigt. In diesem Fall wird der Medienwechsler im Gerätefeld angezeigt.
6. Wählen Sie den Medienwechsler und dann Next (Weiter) aus. Detaillierte Informationen über das Gerät werden im Assistenten angezeigt.
7. Wählen Sie auf der Seite „Add Tapes to Bays (Bänder zu Schächten hinzufügen)“ Scan For Devices (Nach Geräten suchen), Ihren Clientcomputer und dann Next (Weiter) aus.

   Alle Laufwerke werden auf der Seite angezeigt. Bol NetVault Backup zeigt die 10 Laufwerksbereiche an, denen Sie Ihre Laufwerke hinzufügen können. Die Schächte werden nacheinander angezeigt.



Device	Serial Number
3-0.5.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00005
3-0.29.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00007
3-0.30.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00008
3-0.31.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00009
3-0.32.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00010

1 - 5 of 5 items

8. Wählen Sie das Laufwerk aus, das Sie dem angezeigten Schacht hinzufügen möchten, und dann Next (Weiter) aus.

> **Important**
>
> Wenn Sie ein Laufwerk einem Schacht hinzufügen, müssen die Laufwerks- und Schachtnummern übereinstimmen. Wenn beispielsweise Schacht 1 angezeigt wird, müssen Sie Laufwerk 1 hinzufügen. Wenn ein Laufwerk nicht angeschlossen ist, lassen Sie den entsprechenden Schacht leer.

9. Wenn Ihre Client-Maschine angezeigt wird, wählen Sie diese und dann Next (Weiter) aus. Der Client-Computer kann mehrfach angezeigt werden.
10. Wenn die Laufwerke angezeigt werden, wiederholen Sie die Schritte 7 bis 9, um alle Laufwerke den Schächten hinzuzufügen.
11. Wählen Sie auf der Registerkarte Configuration (Konfiguration) die Option Manage devices (Geräte verwalten) aus. Erweitern Sie auf der Seite Manage Devices (Geräte verwalten) den Medienwechsler, um die hinzugefügten Geräte anzuzeigen.

Sichern von Daten auf einem Band im Quest NetVault Backup

Zum Erstellen eines Sicherungsauftrags und Schreiben von Daten auf ein virtuelles Band verwenden Sie dieselben Verfahren wie bei physischen Bändern. Ausführliche Informationen zum Sichern von Daten finden Sie im Quest NetVault Backup – Administration Guide.

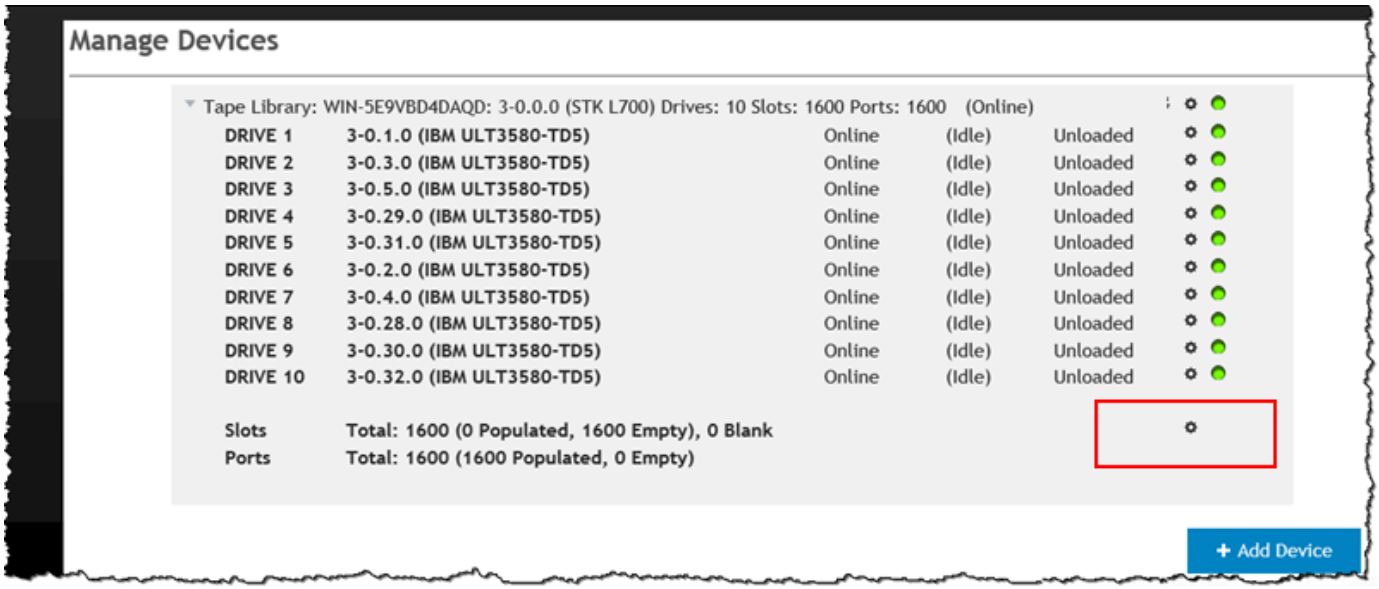
> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe fehl. Um die fehlgeschlagene Backup-Aufgabe abzuschließen, müssen Sie sie erneut übermitteln.

Archivieren eines Bands mithilfe der Bol NetVault Backup

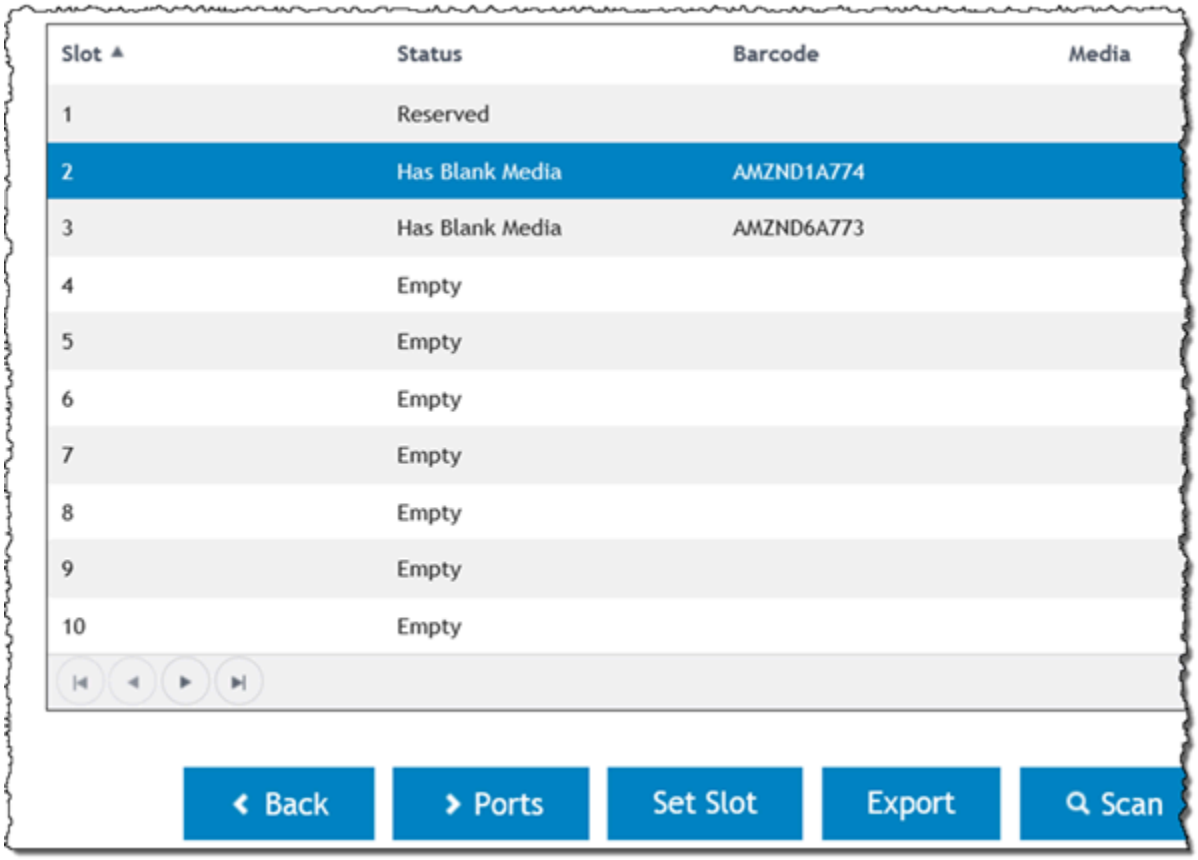
Wenn Sie ein Band archivieren, wirft Tape Gateway das Band aus der Bandbibliothek in den Speicherschacht aus. Anschließend wird das Band mithilfe Ihrer Sicherungsanwendung – d. h. der Bol NetVault Backup – aus dem Slot in das Archiv exportiert.

So archivieren Sie ein Band in Bol NetVault Backup

1. Wählen Sie auf der Registerkarte Bol NetVault Backup Configuration Ihren Medienwechsler aus und erweitern Sie ihn, um Ihre Bänder zu sehen.
2. Wählen Sie in der Reihe Slots (Slots) das Symbol für die Einstellungen aus, um den Slots Browser (Slots-Browser) für den Medienwechsler zu öffnen.



3. Suchen Sie in den Slots nach dem Band, das Sie archivieren möchten. Wählen Sie das Band und dann Export (Exportieren) aus.



Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach Abschluss der Archivierung wird das Band nicht mehr in der VTL aufgeführt.

Stellen Sie in der Software Bol NetVault Backup sicher, dass sich das Band nicht mehr im Speicher-Slot befindet.

Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Tapes aus. Überprüfen Sie, ob für das archivierte Band der Status ARCHIVED (ARCHIVIERT) angezeigt wird.

Wiederherstellen von Daten aus einem Band, das in Quest NetVault Backup archiviert wurde

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.

2. Verwenden Sie die Bol NetVault Backup-Anwendung, um die Daten wiederherzustellen. Dazu erstellen Sie einen Wiederherstellungsordner, wie bei der Wiederherstellung von Daten von physischen Bändern. Anweisungen zum Erstellen eines Wiederherstellungsauftrags finden Sie unter Quest NetVault Backup – Administration Guide.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen der Einrichtung mithilfe von Veeam Backup & Replication

Sie können Veeam Backup & Replication 11A verwenden, um Ihre Daten auf virtuellen Bändern zu sichern, diese Bänder zu archivieren und Ihre Virtual Tape Library(VTL)-Geräte zu verwalten. In diesem Thema finden Sie eine grundlegende Dokumentation zur Konfiguration der Veeam Backup & Replication-Software für ein Tape Gateway sowie zur Durchführung einer Sicherung und Wiederherstellung. Detaillierte Informationen zur Verwendung der Veeam-Software finden Sie unter About Backup & Replication im Veeam Help Center. Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

- Konfigurieren von Veeam für das Arbeiten mit VTL-Geräten
- Importieren eines Bands in Veeam
- Sichern von Daten auf einem Band in Veeam
- Archivieren eines Bands mithilfe von Veeam
- Wiederherstellen von Daten von einem in Veeam archivierten Band

Konfigurieren von Veeam für das Arbeiten mit VTL-Geräten

Sobald Sie die Verbindung von Ihren virtuellen Bandbibliotheken (VTL) Geräten zu Windows-Client hergestellt haben, konfigurieren Sie Veeam Backup & Replication um Ihre Geräte zu erkennen. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Verbinden von VTL-Geräten.

VTL-Gerätetreiber aktualisieren

Um die Software so zu konfigurieren, dass sie mit den Tape Gateway-Geräten zusammenarbeitet, aktualisieren Sie die Gerätetreiber für die VTL Geräte um Sie der Veeam Software zur Verfügung

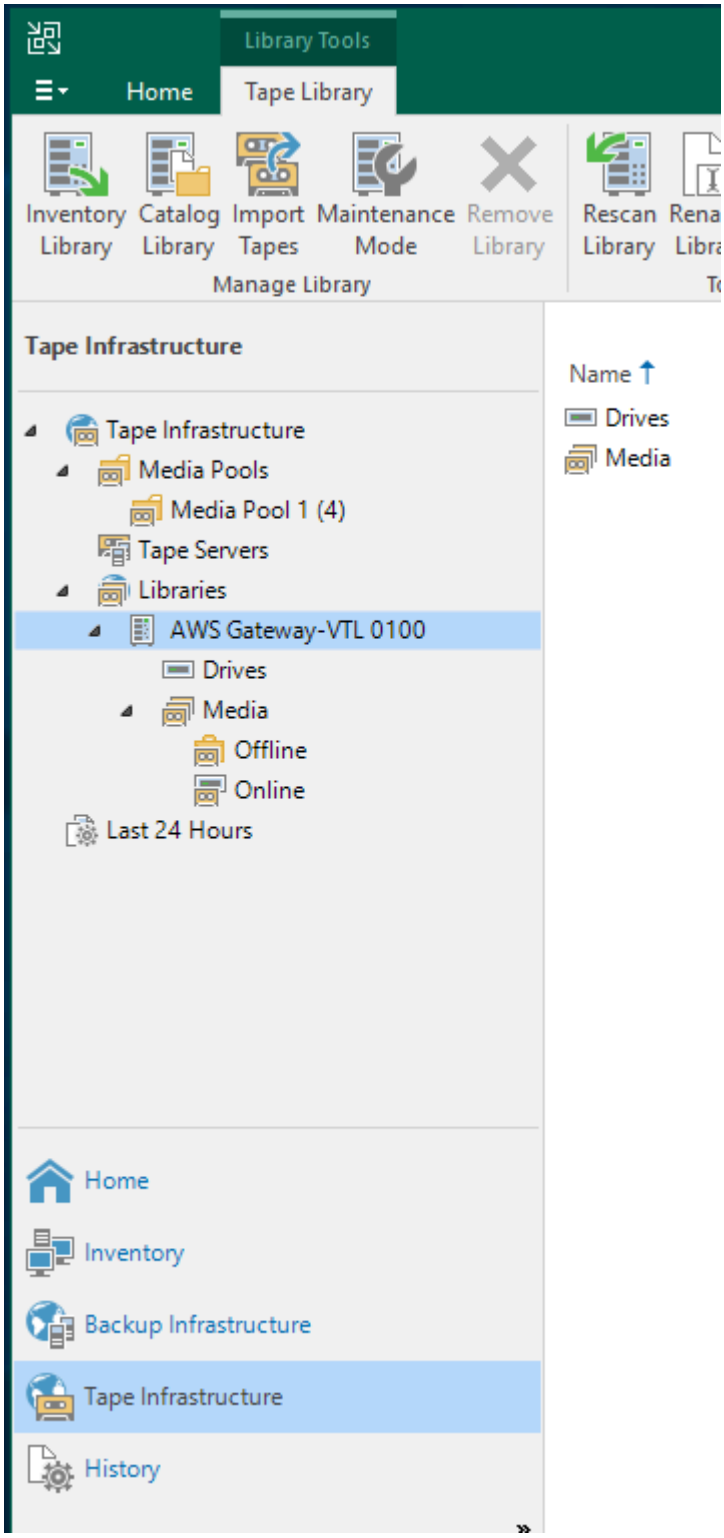
zu stellen und ermitteln Sie anschließend die VTL-Geräte. Aktualisieren Sie im Geräte-Manager den Treiber des Medienwechslers. Anweisungen finden Sie unter Aktualisieren des Gerätetreibers für den Medienwechsler.

Erkennen von VTL-Geräten

Sie müssen bei unbekanntem Medienwechsler native SCSI-Befehle anstelle eines Windows-Treibers verwenden, um die Bänderbibliothek zu ermitteln. Detaillierte Anweisungen finden Sie unter Bandbibliotheken.

So ermitteln Sie VTL-Geräte

1. Wählen Sie in der Veeam-Software Tape Infrastructure aus. Wenn das Tape Gateway verbunden ist, werden die virtuellen Bänder auf der Registerkarte Backup Infrastructure aufgelistet.



2. Erweitern Sie die Struktur Tape (Band), um die Bandlaufwerke und den Medienwechsler anzuzeigen.

3. Erweitern Sie den Medienwechsler-Baum. Wenn Ihre Bandlaufwerke dem Medienwechsler zugeordnet sind, werden die Laufwerke unter Drives (Laufwerke) angezeigt. Andernfalls werden die Bandbibliothek und die Bandlaufwerke als separate Geräte erscheinen.

   Wenn die Laufwerke nicht automatisch zugeordnet werden, folgen Sie den Anweisungen auf der Veeam-Webseite , um die Laufwerke zuzuordnen.

Importieren eines Bands in Veeam

Nun können Sie Bänder von Ihrem Tape Gateway in die Veeam-Sicherungsanwendungsbibliothek importieren.

Importieren eines Bands in die Veeam-Software-Bibliothek

1. Öffnen Sie das Kontextmenü (Rechtsklick) für den Medienwechsler und wählen Sie Import (Importieren) aus, um die Bänder in die I/E Steckplätze zu importieren.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für den Medienwechsler und wählen Sie Inventory Library (Inventarbibliothek) aus, um nicht erkannte Bänder zu identifizieren. Wenn Sie das erste Mal ein neues virtuelles Band in ein Bandlaufwerk laden, wird das Band von der Veeam-Sicherungs-Anwendung nicht erkannt. Um das nicht erkannte Band zu identifizieren, inventarisieren Sie die Bänder in der Bandbibliothek.

Sichern von Daten auf einem Band in Veeam

Das Sichern von Daten auf einem Band ist ein zweistufiger Prozess:

1. Sie erstellen einen Medienpool und fügen das Band zum Medienpool.
2. Schreiben Sie Daten auf das Band.

Erstellen Sie einen Medienpool und schreiben Sie Daten auf ein virtuelles Band indem Sie dieselben Verfahren wie bei physischen Bändern verwenden. Detaillierte Informationen zur Sicherung von Daten finden Sie unter Getting Started with Tapes im Veeam Help Center.

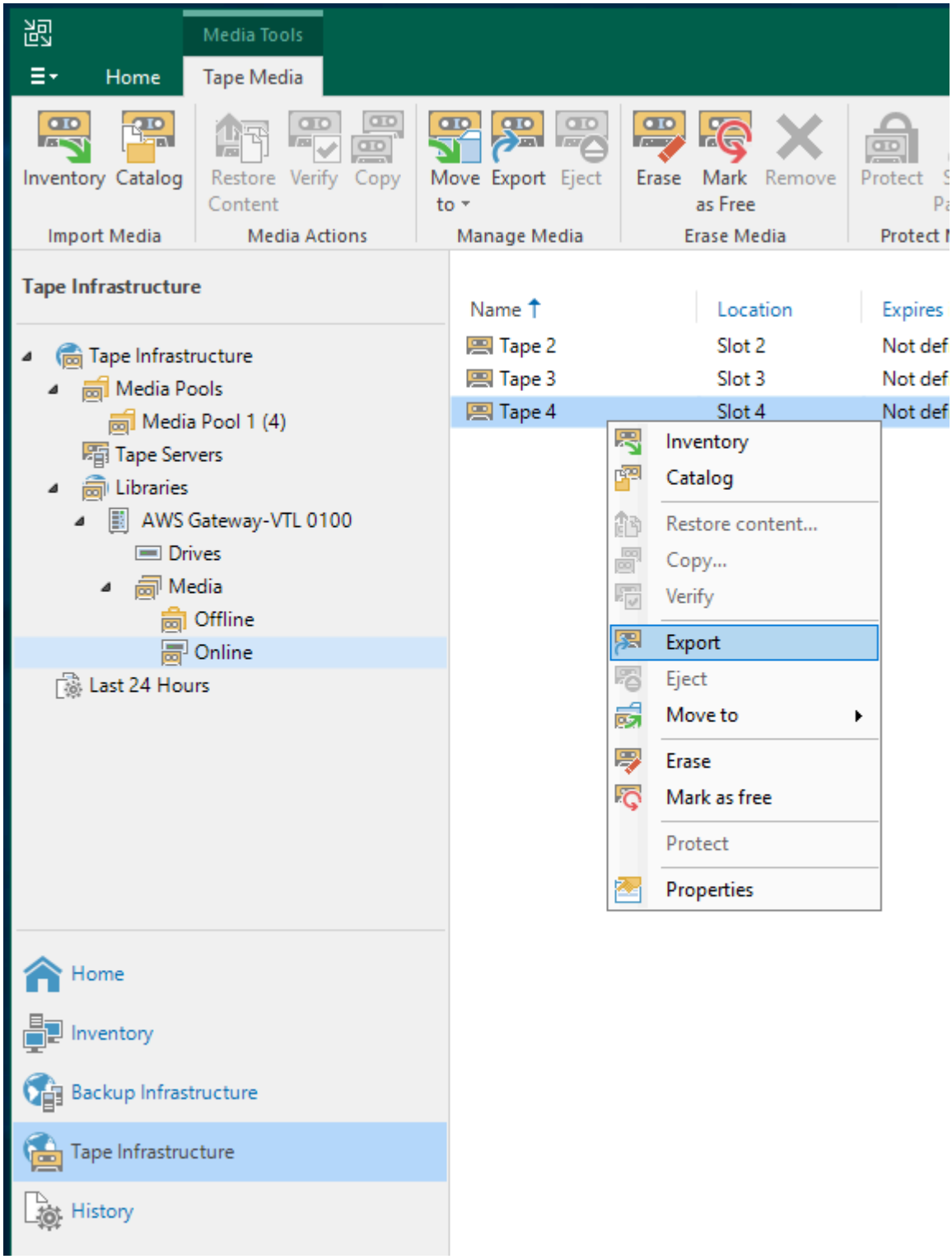
> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe fehl. Um die fehlgeschlagene Backup-Aufgabe abzuschließen, müssen Sie sie erneut übermitteln.

Archivieren eines Bands mithilfe von Veeam

Wenn Sie ein Band archivieren, verschiebt Tape Gateway das Band aus der Veeam-Bandbibliothek in den Offline-Speicher. Sie beginnen die Bandarchivierung durch Auswerfen vom Bandlaufwerk zum Steckplatz. Anschließend exportieren Sie das Band aus dem Steckplatz in das Archiv, indem Sie Ihre Sicherungsanwendung, in diesem Fall die Veeam-Software, verwenden.

Archivieren eines Bands in die Veeam-Bibliothek

1. Wählen Sie Tape Infrastructure Infrastructure und dann den Medienpool aus, der das Band enthält, das Sie archivieren möchten.



2. Öffnen Sie das Kontextmenü (Rechtsklick) für das Band, das Sie archivieren möchten, und wählen Sie dann Eject Tape (Band auswerfen) aus.
3. Wählen Sie in Ejecting tape (Band wird ausgeworfen) die Option Close (Schließen) aus. Der Speicherort des Band ändert sich von einem Bandlaufwerk zu einem Steckplatz.

4. Öffnen Sie das Kontextmenü (Rechtsklick) für das Band erneut und wählen Sie Export (Exportieren) aus. Der Status des Bands wird von Tape drive (Bandlaufwerk) in Offline (Offline) geändert.
5. Wählen Sie in Exporting tape (Band wird exportiert) die Option Close (Schließen) aus. Der Speicherort des Bands wird von Slot (Slot) in Offline (Offline) geändert.
6. Wählen Sie in der Storage-Konsole Ihr Gateway und dann VTL-Bandkartuschen aus. Überprüfen Sie den Status des virtuellen Bands, das Sie archivieren.

   Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach dem Archivieren wird das Band nicht mehr in der VTL aufgeführt, aber in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert.

Wiederherstellen von Daten von einem in Veeam archivierten Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie die Veeam-Software, um die Daten wiederherzustellen. Dazu erstellen Sie einen Wiederherstellungsordner, wie bei der Wiederherstellung von Daten von physischen Bändern. Anleitungen hierzu finden Sie unter Restoring Files from Tape im Veeam Help Center.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec

Sie können Veritas Backup Exec verwenden, um Ihre Daten auf virtuellen Bändern zu sichern, diese Bänder zu archivieren und Ihre Virtual Tape Library(VTL)-Geräte zu verwalten. In diesem Thema finden Sie eine grundlegende Anleitung zur Durchführung von Sicherungs- und Wiederherstellungsvorgängen mithilfe der folgenden Versionen von Backup Exec:

- Veritas Backup Exec 2014

- Veritas Backup Exec 15
- Veritas Backup Exec 16
- Veritas Backup Exec 20.x
- Veritas Backup Exec 22.x

Für alle diese Versionen gilt bei der Verwendung mit Tape Gateway dieselbe Anleitung. Auf der Support-Website von Veritas finden Sie ausführliche Informationen zur Verwendung von Backup Exec, darunter Erstellung sicherer Sicherungen mit Backup Exec, Software- und Hardwarekompatibilitätslisten und Administratorhandbücher für Backup Exec.

Weitere Informationen zu unterstützten Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

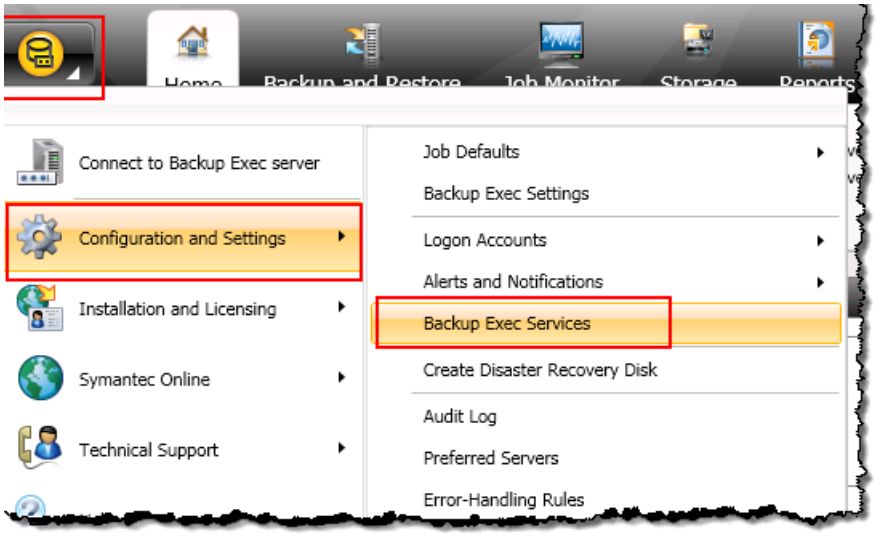
- Konfigurieren von Speicher in Backup Exec
- Importieren eines Bands in Backup Exec
- Schreiben von Daten auf ein Band in Backup Exec
- Archivieren eines Bands mithilfe von Backup Exec
- Wiederherstellen von Daten von einem in Backup Exec archivierten Band
- Deaktivieren eines Bandlaufwerks in Backup Exec

Konfigurieren von Speicher in Backup Exec

Sobald Sie die VTL (Virtual Tape Library)-Geräte mit dem Windows-Client verbunden haben, müssen Sie den Backup Exec-Speicher so konfigurieren, dass er Ihre Geräte erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Verbinden von VTL-Geräten.

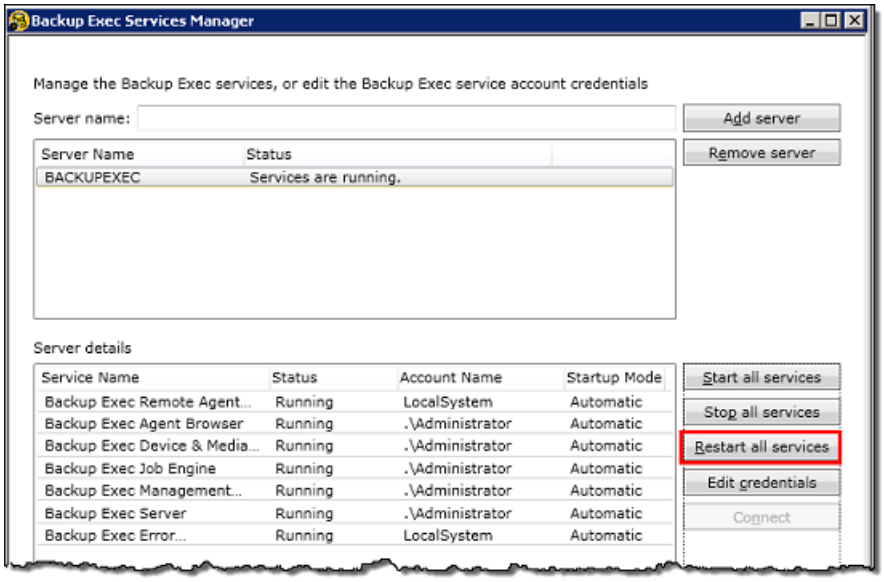
Konfigurieren Sie den Speicher wie folgt:

1. Starten Sie die Backup Exec-Software und klicken Sie links oben in der Symbolleiste auf das gelbe Symbol.
2. Klicken Sie auf Configuration and Settings (Konfiguration und Einstellungen) und anschließend auf Backup Exec Services (Backup Exec-Services), um den Backup Exec Service Manager zu öffnen.



3. Klicken Sie auf Restart All Services (Alle Services neu starten). Backup Exec erkennt nun die VTL-Geräte (also den Medienwechsler und die Bandlaufwerke). Der Neustart kann einige Minuten dauern.

> **Note**
>
> TapeGateway stellt 10 Bandlaufwerke bereit. Möglicherweise ist in Ihrem Backup-Exec-Lizenzvertrag jedoch festgeschrieben, dass Sie mit Ihrer Sicherungsanwendung nicht so viele Bandlaufwerke verwenden dürfen. In diesem Fall müssen Sie in der automatisierten Bibliothek (Wechsler) von Backup Exec die entsprechende Zahl von Bandlaufwerken deaktivieren. Es darf nur die laut Ihrem Lizenzvertrag zulässige Anzahl von Bandlaufwerken aktiviert sein. Anweisungen finden Sie unter Deaktivieren eines Bandlaufwerks in Backup Exec .



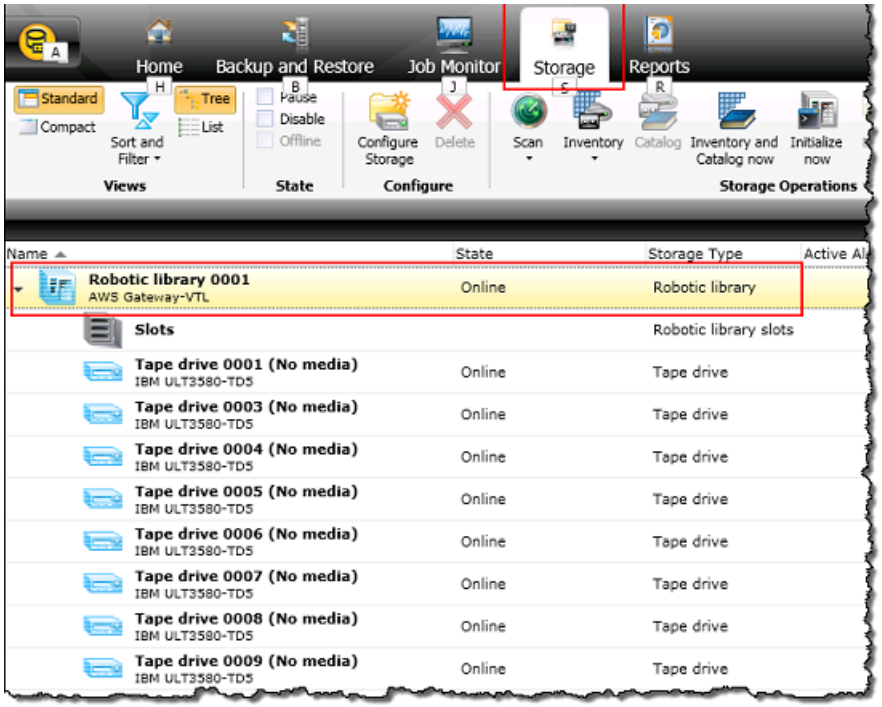
4. Schließen Sie nach dem Neustart den Backup Exec Service Manager.

Importieren eines Bands in Backup Exec

Nun können Sie ein Band von Ihrem Gateway in einen Schacht importieren.

1. Wählen Sie die Registerkarte Storage (Speicher) aus und erweitern Sie die Struktur Robotic library (Robotikbibliothek), um die VTL-Geräte anzuzeigen.

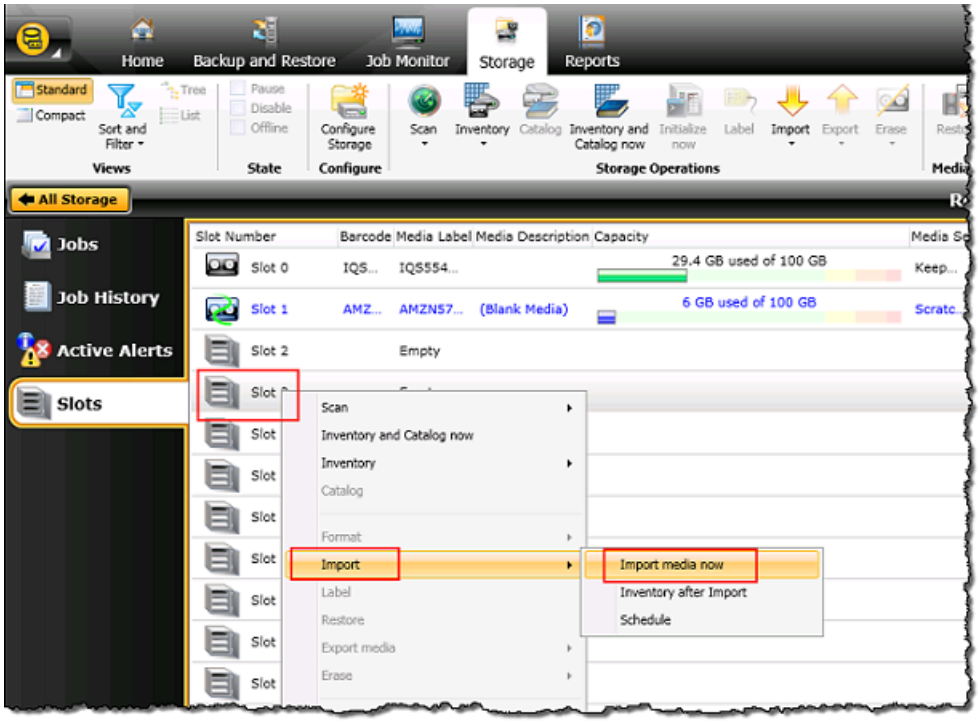
> **Important**
>
> Die Veritas Backup Exec-Software erfordert als Medienwechsler-Typ „Tape Gateway“. Wenn unter Robotic library nicht „TapeGateway“ als Medienwechsler-Typ aufgeführt ist, müssen Sie den Typ ändern, bevor Sie Speicher in der Sicherungsanwendung konfigurieren können. Weitere Informationen zur Auswahl eines anderen Medienwechsler-Typs finden Sie unter Auswählen eines Medienwechslers nach der Gateway-Aktivierung.



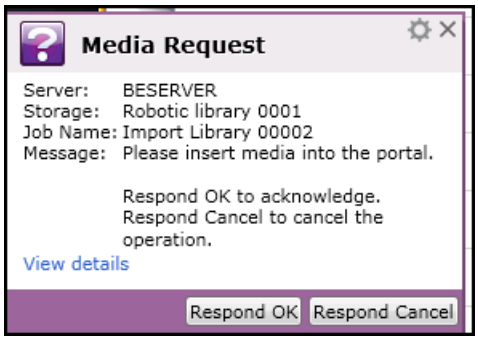
2. Wählen Sie das Symbol Slots (Slots) aus, um alle Slots anzuzeigen.

> **Note**
>
> Wenn Sie Bänder in den Wechsler importieren, werden diese Bänder in Schächten statt auf Bandlaufwerken gespeichert. Daher wird für die Bandlaufwerke möglicherweise gemeldet, dass sie keine Medien enthalten ("No media"). Wenn Sie einen Sicherungs- oder einen Wiederherstellungsauftrag anstoßen, werden die Bänder auf die Bandlaufwerke verschoben.
> In der Bandbibliothek Ihres Gateways müssen Bänder verfügbar sein, damit Sie ein Band in einen Speicherschacht importieren können. Eine Anleitung zur Erstellung von Bändern finden Sie unter Hinzufügen virtueller Bänder.

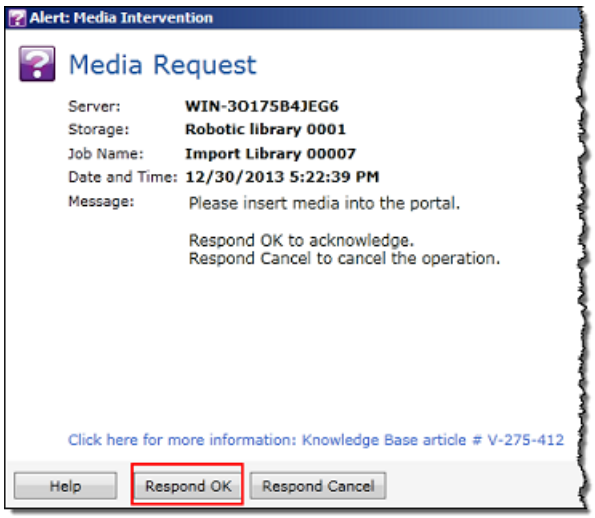
3. Öffnen Sie das Kontextmenü (Rechtsklick) eines leeren Slots und wählen Sie Import (Importieren) und dann Import media now (Medien jetzt importieren) aus. Im folgenden Screenshot ist der Slot Nummer 3 leer. Sie können im Rahmen einer einzigen Importoperation mehrere Schächte auswählen und mehrere Bänder importieren.



4. Wählen Sie im nun angezeigten Fenster Media Request (Medienanforderung) auf View details (Details anzeigen).



5. Wählen Sie im Fenster Action Alert: Media Intervention (Aktionsalarm: Medienintervention) auf Respond OK (Mit OK antworten), um das Medium in den Slot einzufügen.



Das Band wird nun in dem Schacht angezeigt, den Sie ausgewählt haben.

> **Note**
>
> Auch leere Bänder und Bänder, die aus dem Archiv auf das Gateway abgerufen wurden, können importiert werden.

Schreiben von Daten auf ein Band in Backup Exec

Beim Schreiben von Daten auf ein virtuelles Band auf einem Tape Gateway verwenden Sie dasselbe Verfahren und dieselben Sicherungsrichtlinien wie beim Schreiben auf physische Bänder. Detaillierte Informationen finden Sie im Backup Exec-Administrationsleitfaden im Dokumentationsabschnitt der Backup Exec-Software.

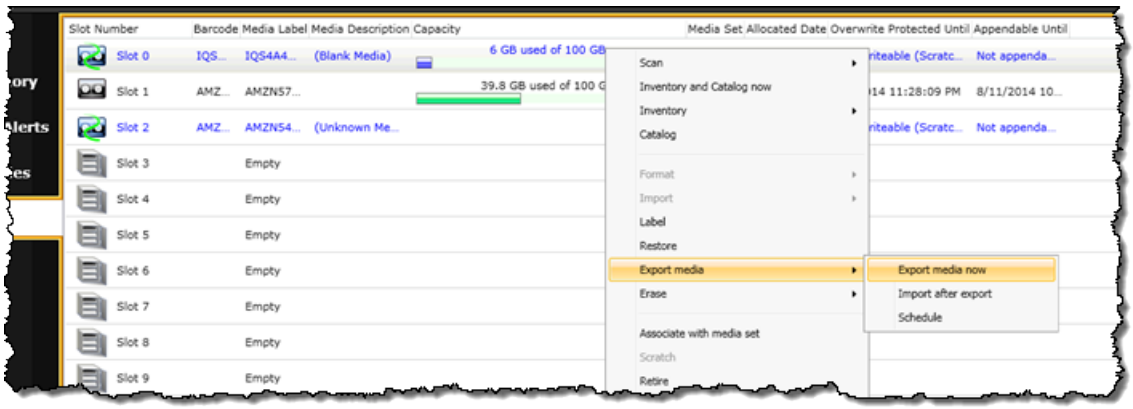
> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe möglicherweise fehl. Wenn die Backup-Aufgabe fehlschlägt, ändert sich der Bandstatus in Veritas Backup Exec in Not Appendable. Sie können das Band archivieren oder weiterhin Daten daraus lesen. Um die fehlgeschlagenen Backup-Aufgabe abzuschließen, müssen Sie sie erneut auf ein neues Band übermitteln.

Archivieren eines Bands mithilfe von Backup Exec

Wenn Sie ein Band archivieren, verschiebt Tape Gateway das Band aus der virtuellen Bandbibliothek Ihres Gateways in den Offline-Speicher. Der erste Schritt bei der Bandarchivierung besteht darin, das betreffende Band mithilfe der Backup Exec-Software zu exportieren.

Archivieren Sie Ihr Band wie folgt:

1. Wählen Sie im Menü Storage (Speicher) die Option Slots (Slots) aus, öffnen Sie das Kontextmenü (Rechtsklick) des Slots, aus dem Sie das Band exportieren möchten. Wählen Sie die Option Export media (Medien exportieren) und dann auf Export media now (Medien jetzt exportieren) aus. Sie können im Rahmen einer einzigen Exportoperation mehrere Schächte auswählen und mehrere Bänder exportieren.



2. Klicken Sie im Pop-up-Fenster Media Request auf View details. Klicken Sie anschließend im Fenster Alert: Media Intervention auf Respond OK.

   In der Storage-Gateway-Konsole können Sie den Status des Bands überprüfen, das archiviert wird. Das Hochladen der Daten in AWS kann einige Zeit dauern. Während des Hochladens wird in der VTL des Tape Gateway als Status für das exportierte Band IN TRANSIT TO VTS angezeigt. Wenn die Dateien hochgeladen wurden und die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach dem Archivieren der Daten wird das exportierte Band nicht mehr in der VTL aufgeführt, aber in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert.

3. Wählen Sie Ihr Gateway und anschließend VTL Tape Cartridges (VTL-Bandkartuschen) aus. Stellen Sie sicher, dass das virtuelle Band nicht mehr imGateway aufgelistet wird.

4. Klicken Sie im Navigationsbereich der Storage-Gateway-Konsole auf Bänder. Überprüfen Sie, ob als Status für das Band ARCHIVIERT angezeigt wird.

Wiederherstellen von Daten von einem in Backup Exec archivierten Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie Backup Exec, um die Daten wiederherzustellen. Der Vorgang ist identisch mit dem Vorgang zur Wiederherstellung von Daten von physischen Bändern. Anleitung hierfür finden Sie im Backup Exec Administrative Guide (Backup Exec-Administrationsleitfaden) im Dokumentationsabschnitt der Backup Exec-Software.

Deaktivieren eines Bandlaufwerks in Backup Exec

Ein Tape Gateway stellt zehn Bandlaufwerke bereit. Möglicherweise möchten Sie aber weniger Bandlaufwerke verwenden. In diesem Fall müssen Sie die Bandlaufwerke deaktivieren, die Sie nicht verwenden möchten.

1. Öffnen Sie Backup Exec und wählen Sie die Registerkarte Storage (Speicher) aus.
2. Öffnen Sie in der Struktur Robotikbibliothek das Kontextmenü des Bandlaufwerks (Rechtsklick), das Sie deaktivieren möchten, und wählen Sie dann Deaktivieren aus.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Testen Ihrer Einrichtung mithilfe von Ver Bols NetBackup

Sie können Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL)-Geräte mithilfe von Ver Bols verwalten NetBackup. In diesem Thema finden Sie eine grundlegende Dokumentation zur Konfiguration der NetBackup Anwendung für ein Tape Gateway und zur Durchführung eines Sicherungs- und Wiederherstellungsvorgangs. Dazu können Sie die folgenden Versionen von verwenden NetBackup:

- Ver Bols NetBackup 7.x
- Ver Bols NetBackup 8.x

Für alle diese Versionen von Backup Exec gilt bei der Verwendung mit einem Tape Gateway dieselbe Anleitung. Ausführliche Informationen zur Verwendung von NetBackupfinden Sie in den Tools für Ver Bols Services and Operations Readiness (SORT) auf der Ver Bols-Website. Informationen zur Unterstützung der Hardwarekompatibilität durch Ver Bols finden Sie in der NetBackup Hardwarekompatibilitätsliste 7.0–7.6.x, NetBackup Hardwarekompatibilitätsliste 8.0–8.1.x oder NetBackup Hardwarekompatibilitätsliste 8.2–8.x.x auf der Ver Bols-Website.

Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

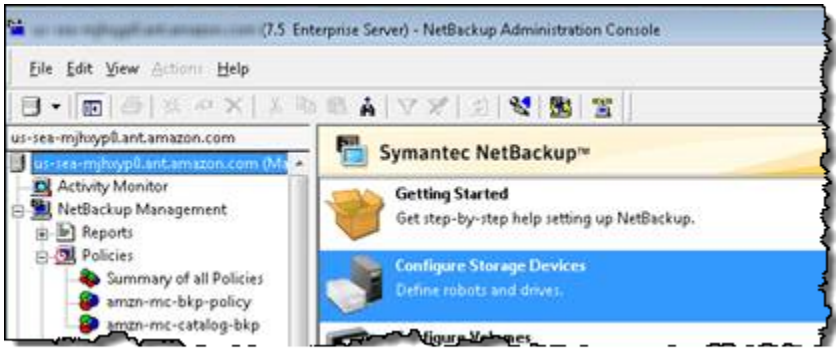
- Konfigurieren von NetBackup Speichergeräten
- Sichern von Daten auf einem Band
- Archivieren eines Bands
- Wiederherstellen von Daten von einem Band

Konfigurieren von NetBackup Speichergeräten

Nachdem Sie die Virtual Tape Library (VTL)-Geräte mit dem Windows-Client verbunden haben, konfigurieren Sie den Ver Bols- NetBackup Speicher so, dass er Ihre Geräte erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Verbinden von VTL-Geräten.

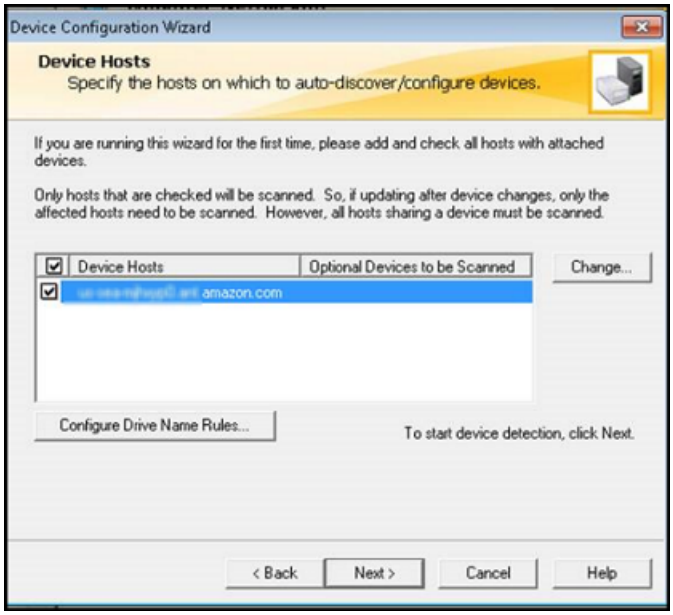
So konfigurieren Sie NetBackup für die Verwendung von Speichergeräten auf Ihrem Tape Gateway

1. Öffnen Sie die - NetBackup Administratorkonsole und führen Sie sie als Administrator aus.

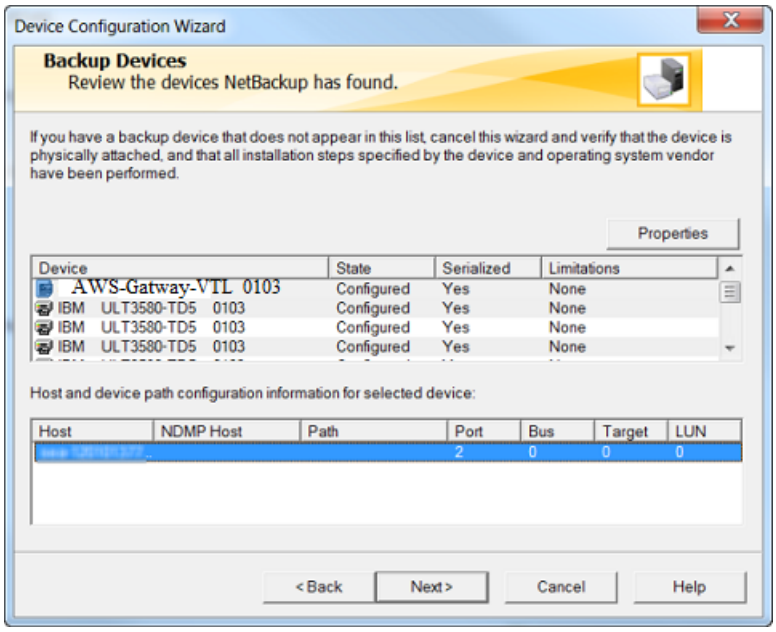


2. Wählen Sie Configure Storage Devices (Speichergeräte konfigurieren) aus, um den Assistenten für die Gerätekonfiguration zu öffnen.

3. Wählen Sie Weiter aus. Die NetBackup Anwendung erkennt Ihren Computer als Gerätehost.
4. Wählen Sie in der Spalte Device Hosts (Gerätehosts) Ihren Computer und dann Next (Weiter) aus. Die NetBackup Anwendung scannt Ihren Computer nach Geräten und erkennt alle Geräte.



5. Wählen Sie auf der Seite Scanning Hosts (Scanning-Hosts) auf Next (Weiter) und ein zweites Mal auf Next (Weiter). Die NetBackup Anwendung findet alle 10 Bandlaufwerke und den Medienwechsler auf Ihrem Computer.

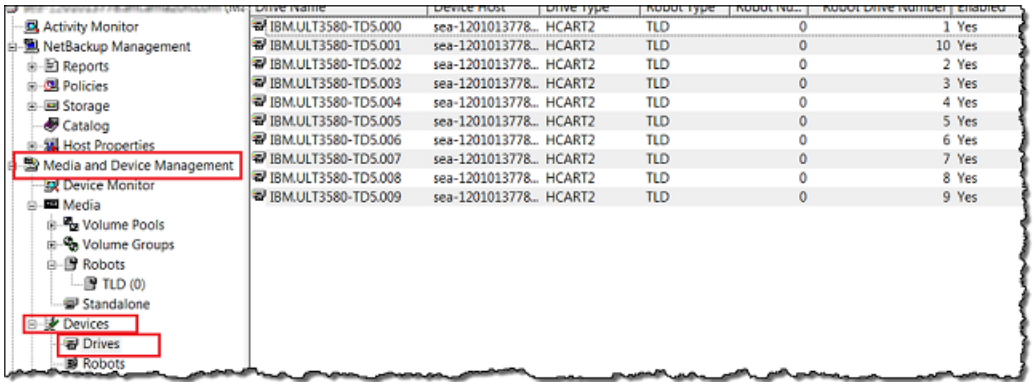


6. Wählen Sie im Fenster Backup Devices (Sicherungsgeräte) Next (Weiter) aus.

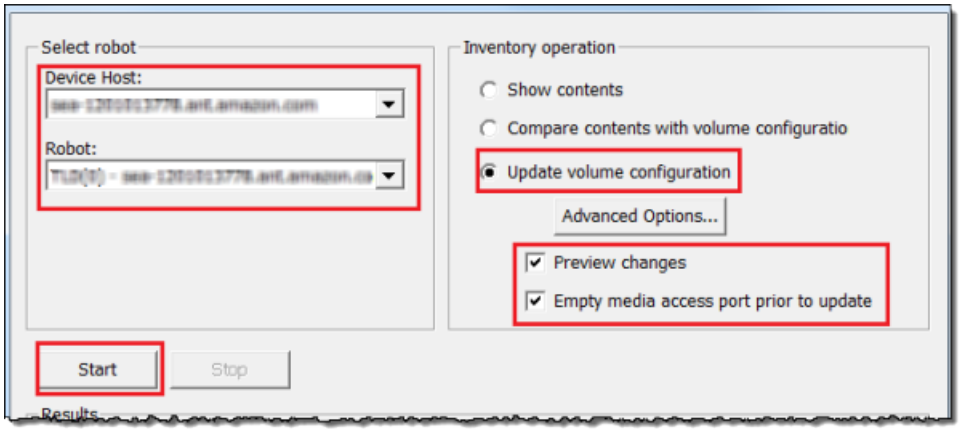
7. Überprüfen Sie im Fenster Drag and Drop Configuration (Drag-and-Drop-Konfiguration), ob Ihr Medienwechsler ausgewählt ist. Wählen Sie dann Next (Weiter) aus.
8. Wählen Sie im nun angezeigten Dialogfeld Yes (Ja) aus, um die Konfiguration auf Ihrem Computer zu speichern. Die NetBackup Anwendung aktualisiert die Gerätekonfiguration.
9. Wenn das Update abgeschlossen ist, wählen Sie Weiter, um die Geräte für die NetBackup Anwendung verfügbar zu machen.
10. Wählen Sie im Fenster Finished! (Fertig!) die Option Finish (Beenden) aus.

So überprüfen Sie Ihre Geräte in der NetBackup Anwendung

1. Erweitern Sie in der NetBackup Administration Console den Knoten Medien- und Geräteverwaltung und erweitern Sie dann den Knoten Geräte. Wählen Sie Drives (Laufwerke) aus, um alle Bandlaufwerke anzuzeigen.

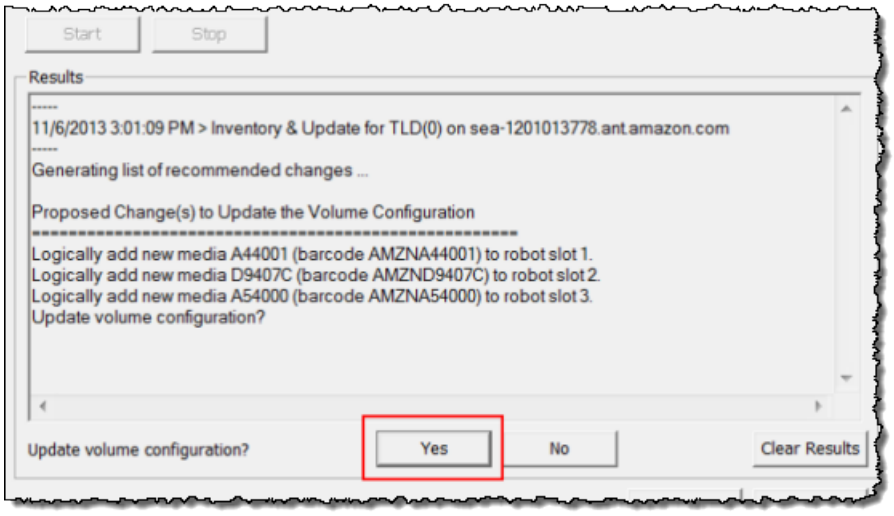


2. Wählen Sie im Knoten Devices (Geräte) Robots (Roboter) aus, um alle Medienwechsler anzuzeigen. In der NetBackup Anwendung wird der Medienwechsler als Roboter bezeichnet.
3. Öffnen Sie im Bereich All Robots (Alle Roboter) das Kontextmenü (Rechtsklick) für TLD(0) (d. h. Ihren Roboter) und wählen Sie dann Inventory Robot (Roboterinventar) aus.
4. Vergewissern Sie sich im Fenster Robot Inventory, dass in der Kategorie Select robot in der Liste Device Host Ihr Host ausgewählt ist.
5. Überprüfen Sie, ob in der Liste Robot (Roboter) Ihr Roboter ausgewählt ist.
6. Wählen Sie im Fenster Robot Inventory (Roboterinventar) die Option Update volume configuration (Volumekonfiguration aktualisieren), Preview changes (Änderungsvorschau anzeigen), Empty media access port prior to update (Medienzugriffsport vor Aktualisierung leeren) und dann Start (Starten) aus.

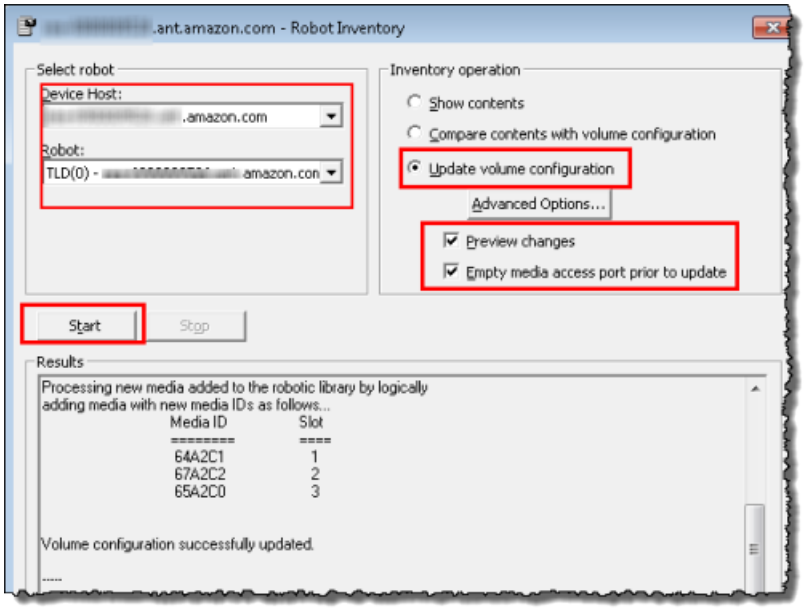


Der Prozess inventarisiert dann Ihre Medienwechsler und virtuellen Bänder in der NetBackup Enterprise Media Management (EMM)-Datenbank. NetBackup speichert Medieninformationen, Gerätekonfiguration und Bandstatus im EMM.

7. Wählen Sie nach Abschluss der Inventarisierung im Fenster Robot Inventory (Roboterinventar) Yes (Ja) aus. Durch die Wahl von Yes (Ja) an dieser Stelle werden die Konfiguration aktualisiert und die virtuellen Bänder in den Import/Export-Slots zur virtuellen Bandbibliothek verschoben.

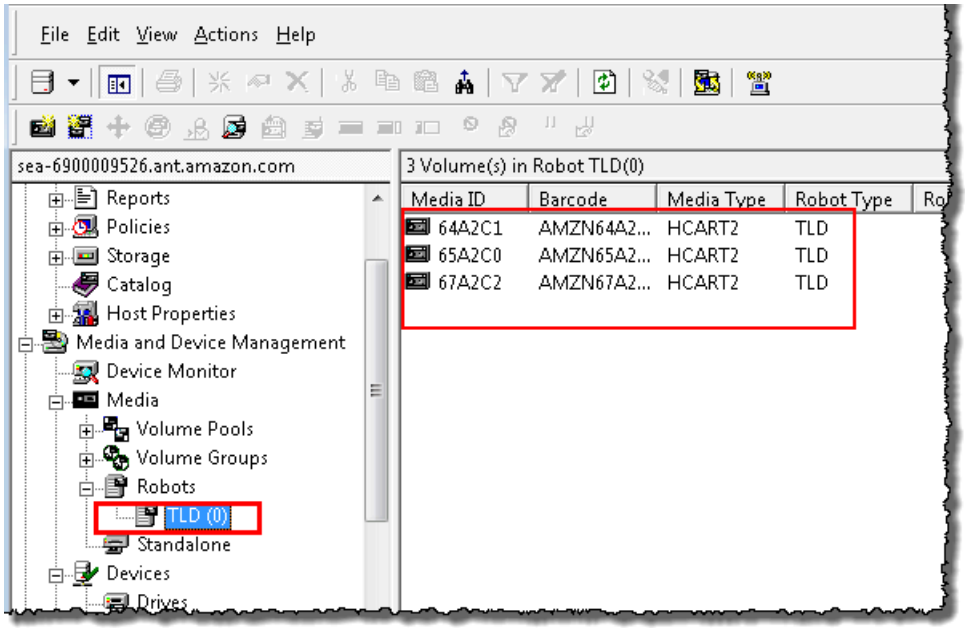


Auf dem Screenshot unten beispielsweise sehen Sie, dass drei virtuelle Bänder in den Import/Export-Slots erkannt wurden.



8. Schließen Sie das Fenster Robot Inventory (Roboterinventar).
9. Erweitern Sie im Knoten Media (Medien) den Knoten Robots (Roboter) und wählen Sie TLD(0) aus, um alle virtuellen Bänder anzuzeigen, die für Ihren Roboter (Medienwechsler) verfügbar sind.

> **Note**
>
> Wenn Sie zuvor andere Geräte mit der NetBackup Anwendung verbunden haben, haben Sie möglicherweise mehrere Roboter. Stellen Sie in diesem Fall sicher, dass Sie den richtigen Robot auswählen.



Ihre Geräte sind jetzt verbunden und für die Sicherungsanwendung verfügbar. Nun können Sie Ihr Gateway testen. Dazu sichern Sie Daten auf die virtuellen Bänder, die Sie erstellt haben, und archivieren diese Bänder.

Sichern von Daten auf einem Band

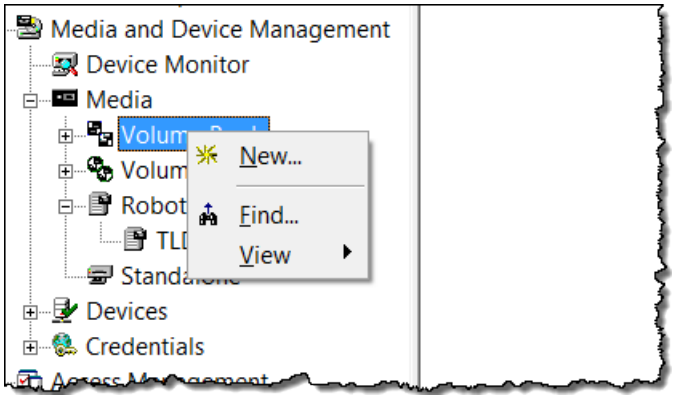
Zum Testen Ihrer Tape Gateway-Konfiguration sichern Sie Daten auf Ihre virtuellen Bänder.

> **Note**
>
> - Im Rahmen dieser Erste-Schritte-Übung sollten Sie nur eine kleine Menge Daten sichern, da sowohl die Speicherung und die Archivierung der Daten als auch der Datenabruf kostenpflichtig sind. Informationen zu den Preisen finden Sie unter Preise auf der Storage-Gateway-Detailseite.
> - Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, wird die Backup-Aufgabe unterbrochen. Die unterbrochene Backup-Aufgabe wird automatisch wieder aufgenommen, wenn Ihr Gateway den Neustart abgeschlossen hat.

Erstellen Sie wie folgt einen Volume-Pool:

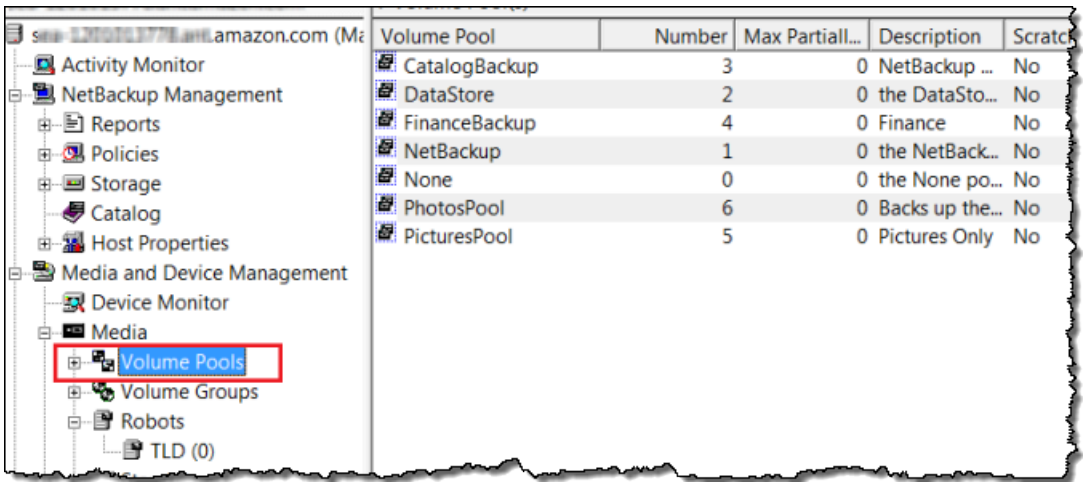
Ein Volume-Pool ist eine Sammlung von virtuellen Bändern, die für Sicherungen verwendet werden können.

1. Starten Sie die - NetBackup Administratorkonsole.
2. Erweitern Sie den Knoten Media (Medien), öffnen Sie das Kontextmenü (Rechtsklick) für Volume Pool (Volume-Pool) und wählen Sie dann New (Neu) aus. Anschließend wird das Dialogfeld New Volume Pool (Neuer Volume-Pool) angezeigt.



3. Geben Sie in das Feld Name (Name) einen Namen für den Volume-Pool ein.
4. Geben Sie in das Feld Description (Beschreibung) eine Beschreibung für den Volume-Pool ein und wählen Sie dann OK (OK) aus. Der Volume-Pool wird erstellt und der Volume-Pool-Liste hinzugefügt.

   Im Screenshot unten sehen Sie eine Liste von Volume-Pools.

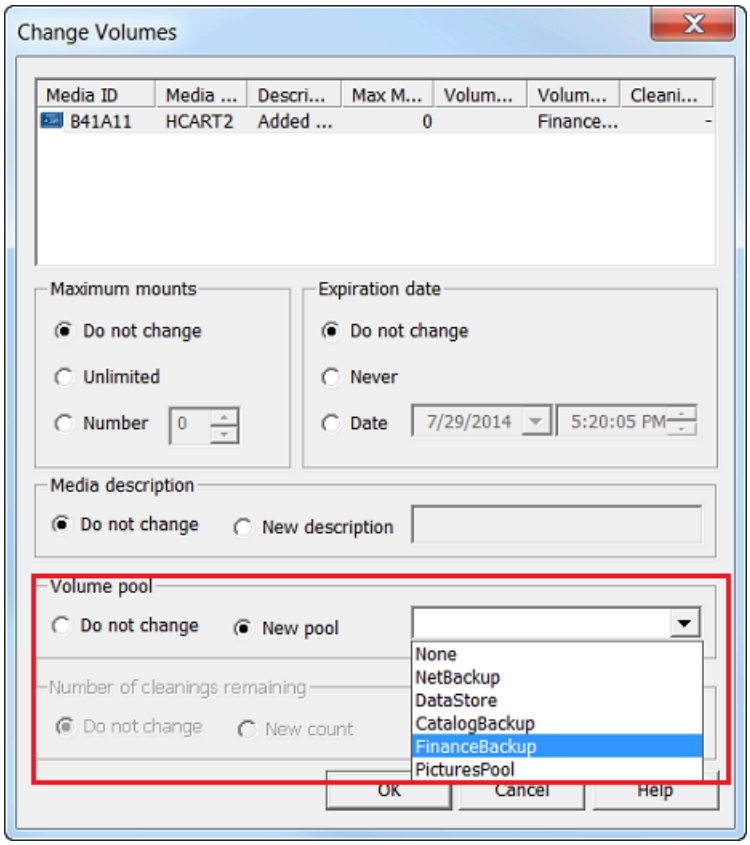


Fügen Sie dem Volume-Pool wie folgt virtuelle Bänder hinzu:

1. Erweitern Sie den Knoten Robots (Roboter) und wählen Sie den Roboter TLD(0) aus, um die virtuellen Bänder anzuzeigen, die dem Roboter bekannt sind.

   Wenn Sie bereits zuvor einen Robot verbunden haben, hat Ihr Tape Gateway-Robot möglicherweise einen anderen Namen.

2. Öffnen Sie in der Liste der virtuellen Bänder das Kontextmenü (Rechtsklick) des Bands, das Sie dem Volume-Pool hinzufügen möchten. Wählen Sie Change (Ändern) aus, um das Dialogfeld Change Volumes (Volumes ändern) zu öffnen. Der folgende Screenshot zeigt das Dialogfeld Change Volumes (Volumes ändern).



3. Wählen Sie in Volume Pool (Volume-Pool) die Option New pool (Neuer Pool) aus.

4. Wählen Sie in New pool (Neuer Pool) den Pool aus, den Sie gerade erstellt haben, und wählen Sie dann OK (OK) aus.

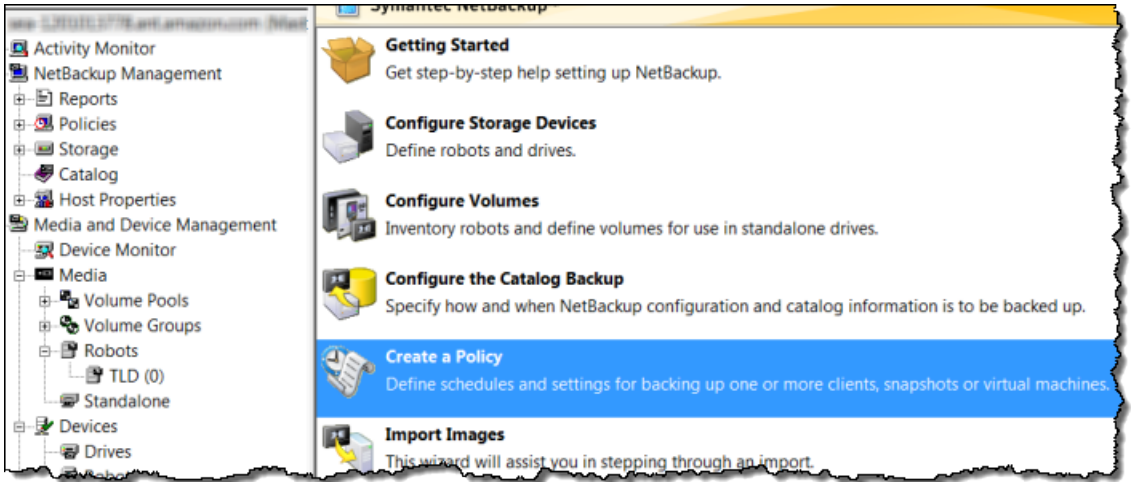
   Sie können überprüfen, ob Ihr Volume-Pool das virtuelle Band enthält, das Sie gerade hinzugefügt haben, indem Sie den Knoten Media (Medien) erweitern und Ihren Volume-Pool auswählen.

Erstellen Sie wie folgt eine Backup-Richtlinie:

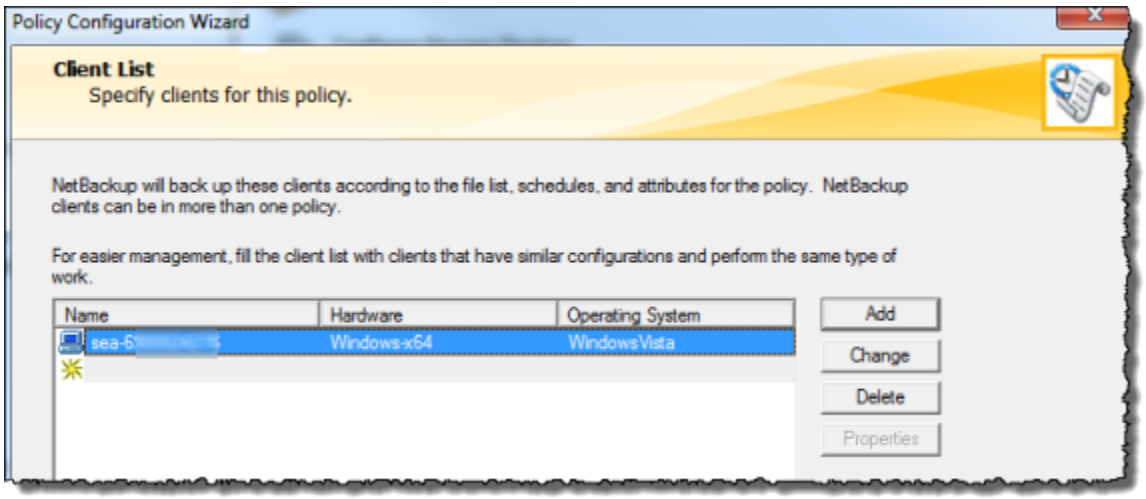
Die Sicherungsrichtlinie gibt an, welche Daten gesichert werden sollen, wann sie gesichert werden sollen und welcher Volume-Pool als Sicherungsziel verwendet werden soll.

1. Wählen Sie Ihren Masterserver aus, um zur Ver Bols- NetBackup Konsole zurückzukehren.

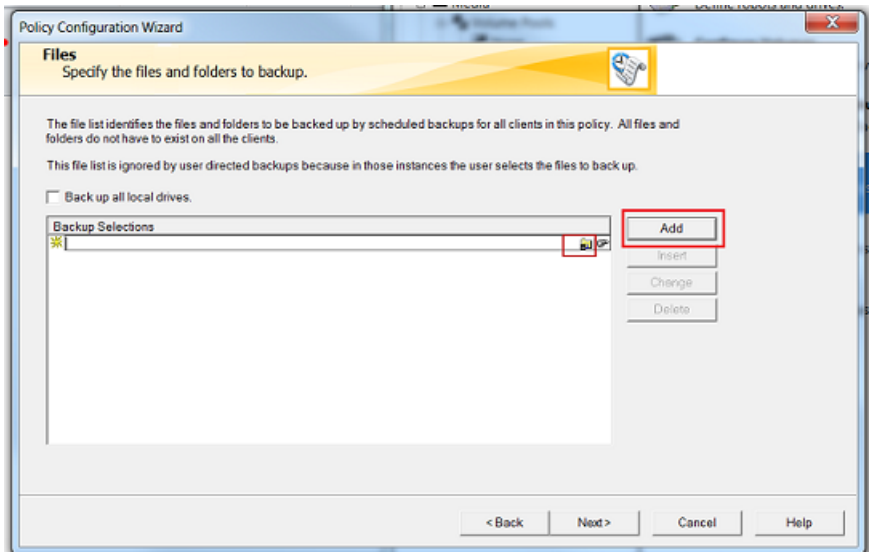
   Der folgende Screenshot zeigt die NetBackup Konsole mit ausgewählter Richtlinie erstellen.



2. Klicken Sie auf Create a Policy (Richtlinie erstellen), um das Fenster Policy Configuration Wizard (Assistent für die Richtlinienkonfiguration) zu öffnen.
3. Wählen Sie die Option File systems, databases, applications (Dateisysteme, Datenbanken, Anwendungen) aus und klicken Sie auf Next (Weiter).
4. Geben Sie in das Feld Policy Name einen Namen für Ihre Richtlinie ein und vergewissern Sie sich, dass in der Liste Select the policy type die Option MS-Windows ausgewählt ist. Klicken Sie dann auf Next.
5. Wählen Sie im Fenster Client List (Clientliste) die Option Add (Hinzufügen) aus. Geben Sie in der Spalte Name (Name) den Hostnamen Ihres Computers ein und wählen Sie Next (Weiter) aus. Die Richtlinie, die Sie gerade definieren, wird damit auf `localhost` (Ihren Client-Computer) angewendet.



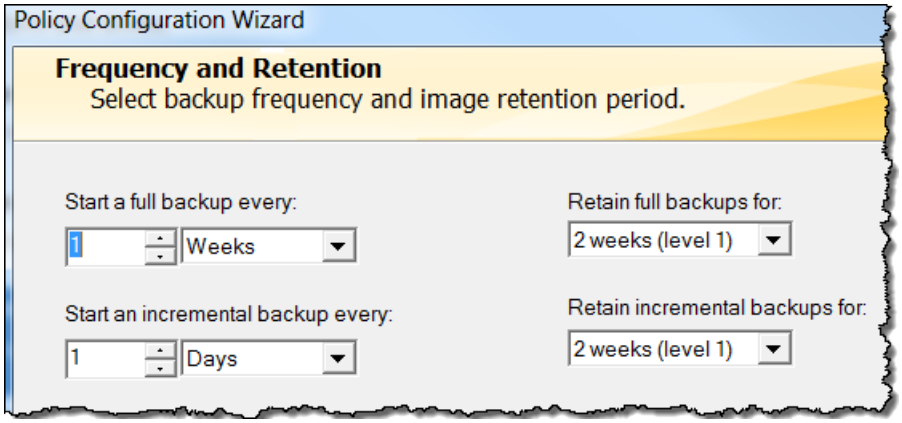
6. Wählen Sie im Fenster Files (Dateien) zunächst Add (Hinzufügen) und anschließend das Ordnersymbol aus.



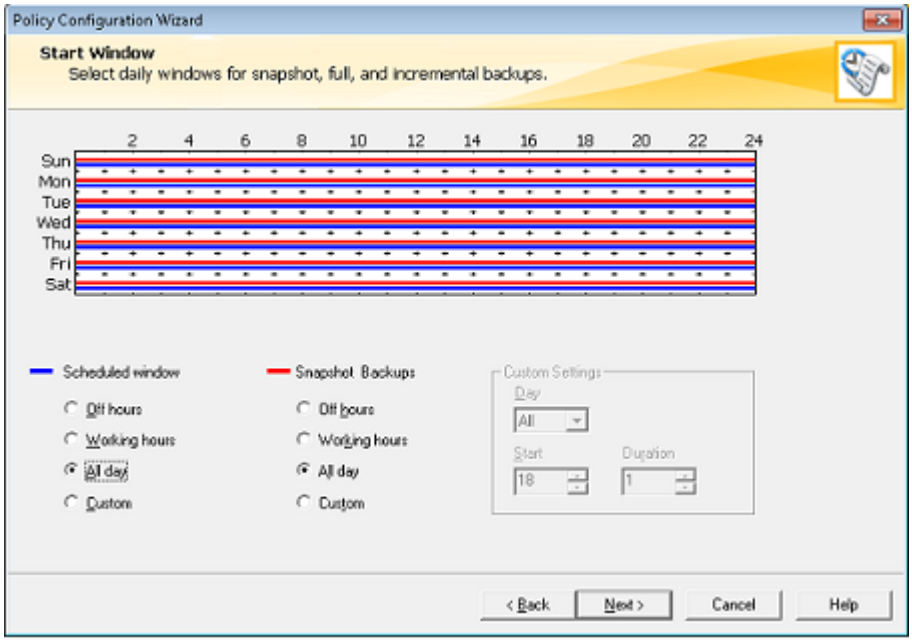
7. Navigieren Sie im Fenster Browse (Durchsuchen) zum Ordner oder zu den Dateien, den oder die Sie sichern möchten, und wählen Sie OK (OK) aus. Klicken Sie dann auf Next (Weiter).
8. Akzeptieren Sie im Fenster Backup Types (Sicherungstypen) die Standardeinstellungen und wählen Sie dann Next (Weiter) aus.

> **Note**
>
> Wenn Sie die Sicherung selbst initiieren möchten, aktivieren Sie das Kontrollkästchen User Backup (Benutzersicherung).

9. Legen Sie im Fenster Frequency and Retention (Häufigkeit und Aufbewahrung) fest, wie häufig die Sicherung ausgeführt werden soll und welche Aufbewahrungsrichtlinie für die Sicherung gelten soll. Für die Zwecke dieser Übung können Sie alle Standardeinstellungen akzeptieren und Next (Weiter) auswählen.



10. Wählen Sie im Fenster Start (Starten) die Option Off hours (Außerhalb der Geschäftszeiten) und dann Next (Weiter) aus. Mit dieser Auswahl legen Sie fest, dass Ihr Ordner nur außerhalb der Geschäftszeiten gesichert werden soll.

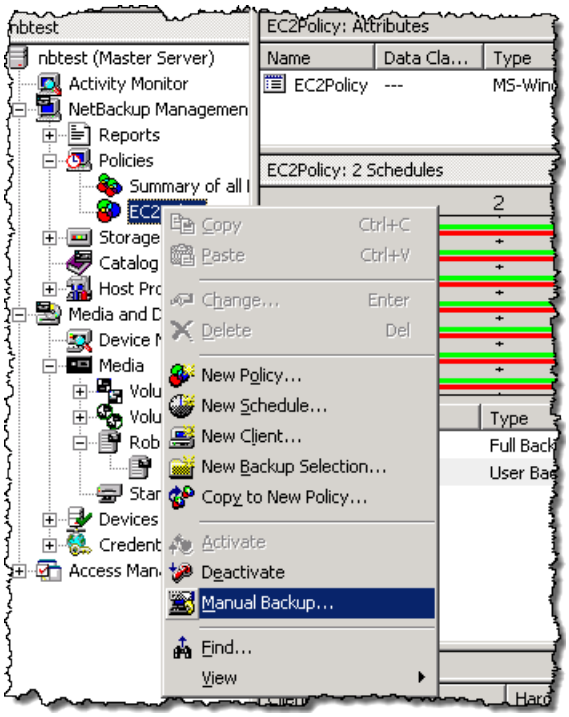


11. Wählen Sie im Policy Configuration Wizard (Assistent für Richtlinienkonfiguration) die Option Finish (Beenden) aus.

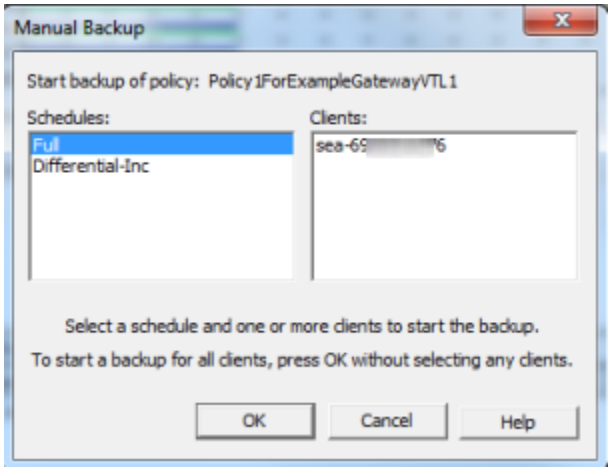
Die Richtlinie führt die Sicherung nun gemäß dem festgelegten Zeitplan durch. Daneben können Sie auch jederzeit eine manuelle Sicherung durchführen. Wie das geht, demonstrieren wir Ihnen im nächsten Schritt.

Führen Sie wie folgt eine manuelle Sicherung durch:

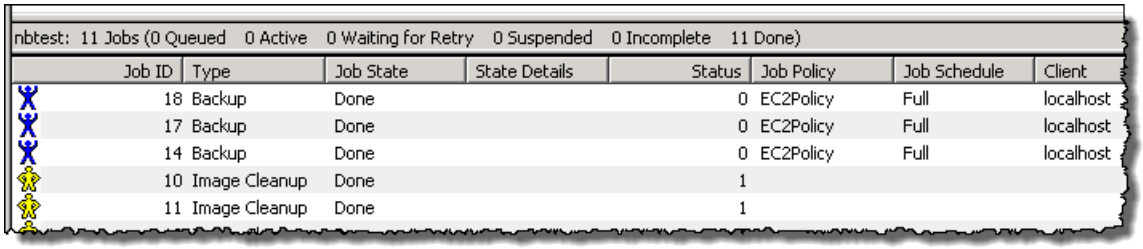
1. Erweitern Sie im Navigationsbereich der - NetBackup Konsole den NetBackup Verwaltungsknoten.
2. Erweitern Sie den Knoten Policies (Richtlinien).
3. Öffnen Sie das Kontextmenü (Rechtsklick) für Ihre Richtlinie und wählen Sie Manual Backup (Manuelle Sicherung) aus.



4. Wählen Sie im Fenster Manual Backup (Manuelle Sicherung) einen Zeitplan, einen Client und dann OK (OK) aus.



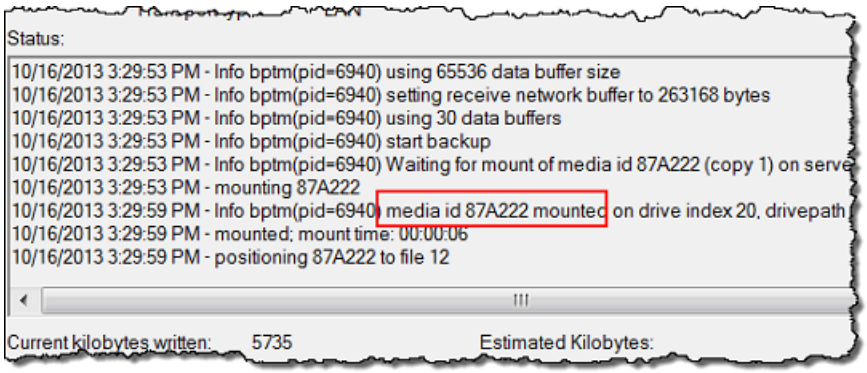
5. Wählen Sie im nun angezeigten Dialogfeld Manual Backup Started (Manuelle Sicherung gestartet) OK (OK) aus.
6. Wählen Sie im Navigationsbereich Activity Monitor (Aktivitätsüberwachung) aus, um in der Spalte Job ID (Auftrags-ID) den Status der Sicherung anzuzeigen.



Den Barcode des virtuellen Bands, in das die Dateidaten während des Backups NetBackup geschrieben hat, finden Sie im Fenster Auftragsdetails, wie im folgenden Verfahren beschrieben. Sie benötigen diesen Barcode für die Anleitung im nächsten Abschnitt, mit der Sie das Band archivieren.

Ermitteln Sie wie folgt den Barcode des Bands:

1. Öffnen Sie in Activity Monitor (Aktivitätsüberwachung) in der Spalte Job ID (Auftrags-ID) das Kontextmenü (Rechtsklick) des Bezeichners Ihres Sicherungsauftrags und wählen Sie dann Details (Details) aus.
2. Wählen Sie im Fenster Job Details (Auftragsdetails) die Registerkarte Detailed Status (Detaillierter Status) aus.
3. Suchen Sie im Feld Status (Status) die Medien-ID. Im folgenden Screenshot ist die Medien-ID beispielsweise 87A222. Anhand dieser ID können Sie ermitteln, auf welches Band die Daten geschrieben wurden.



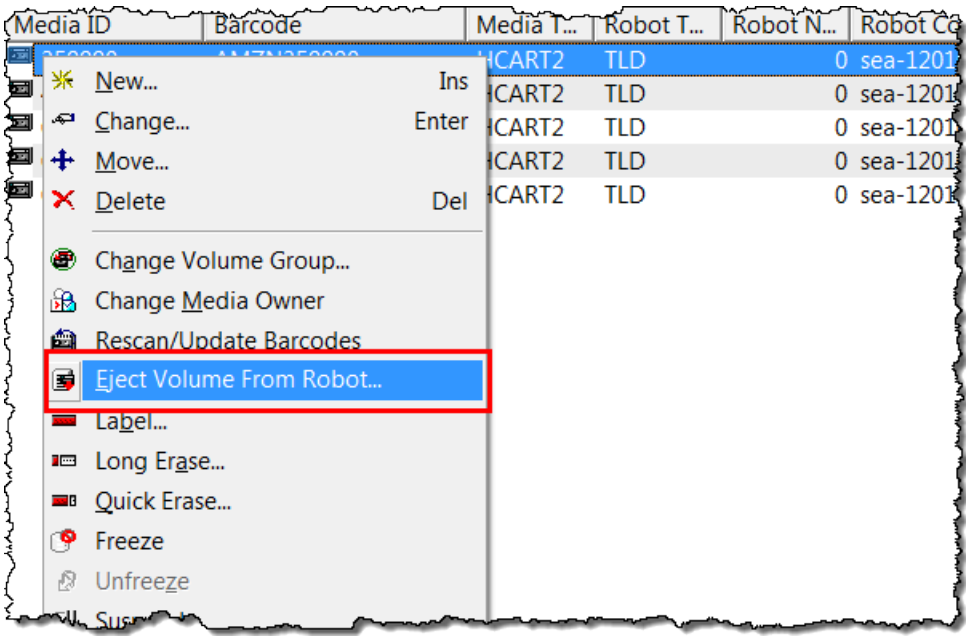
Damit haben Sie nun ein Tape Gateway bereitgestellt, virtuelle Bänder erstellt und Ihre Daten gesichert. Im nächsten Schritt zeigen wir Ihnen, wie Sie die virtuellen Bänder archivieren und wieder aus dem Archiv abrufen können.

Archivieren eines Bands

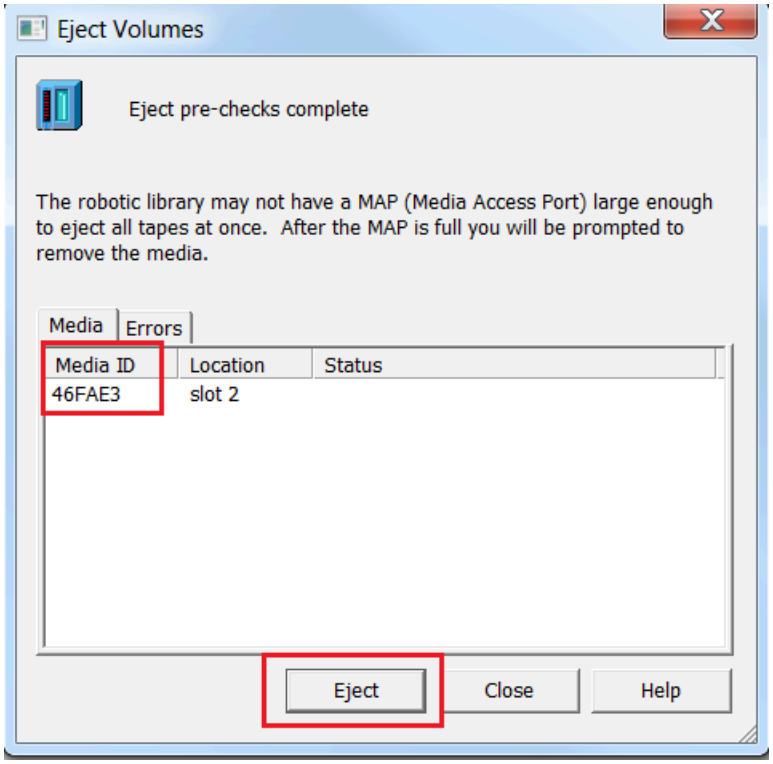
Wenn Sie ein Band archivieren, verschiebt Tape Gateway das Band aus der virtuellen Bandbibliothek (VTL) Ihres Gateways in das Archiv und damit in einen Offline-Speicher. Initiieren können Sie die Bandarchivierung, indem Sie das betreffende Band mithilfe Ihrer Sicherungsanwendung auswerfen.

Archivieren Sie wie folgt ein virtuelles Band:

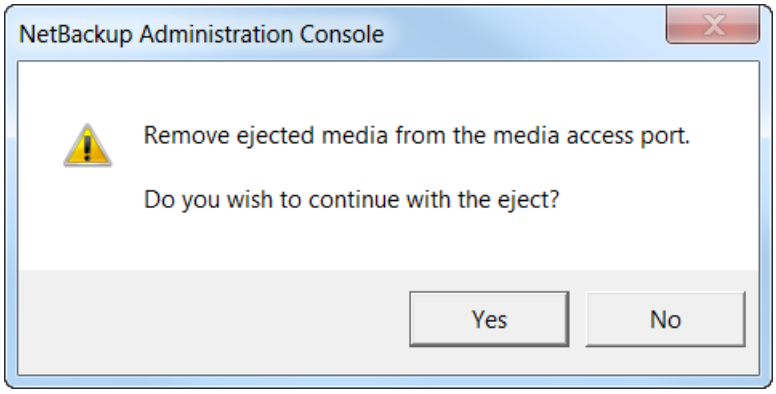
1. Erweitern Sie in der NetBackup Administrationskonsole den Knoten Medien und Geräteverwaltung und erweitern Sie den Knoten Medien.
2. Erweitern Sie Robots (Roboter) und wählen Sie TLD(0) aus.
3. Öffnen Sie das Kontextmenü (Rechtsklick) für das virtuelle Band, das Sie archivieren möchten, und wählen Sie Eject Volume From Robot (Volume aus Roboter auswerfen) aus.



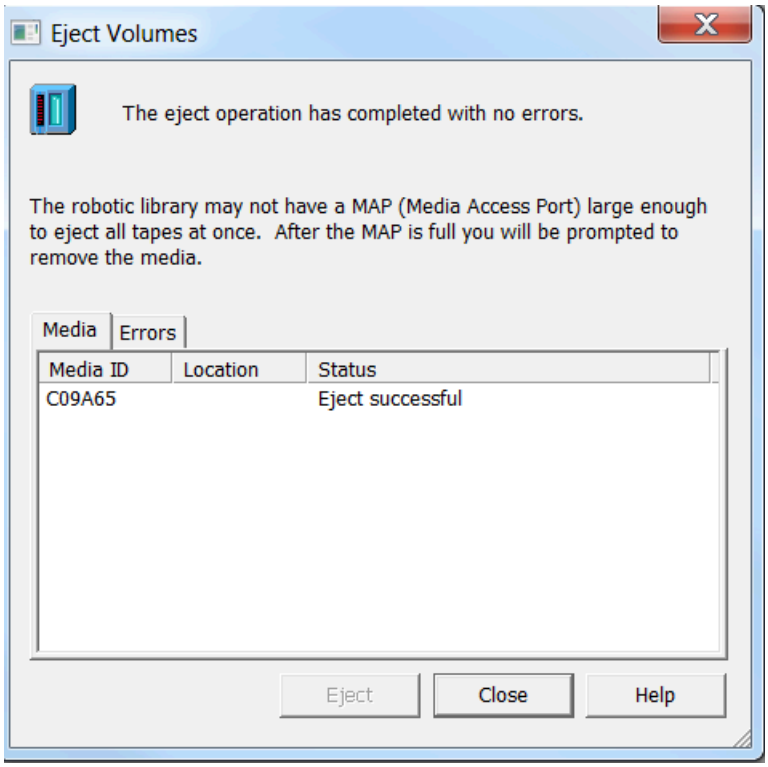
4. Stellen Sie im Fenster Eject Volumes (Volumes auswerfen) sicher, dass der Wert in der Spalte Media ID (Medien-ID) mit der ID des virtuellen Bands übereinstimmt, das Sie auswerfen möchten, und wählen Sie dann Eject (Auswerfen) aus.



5. Wählen Sie im Dialogfeld Yes (Ja) aus. Unten sehen Sie einen Screenshot des betreffenden Dialogfelds.



Wenn der Auswurfvorgang abgeschlossen ist, zeigt der Status des Bands im Dialogfeld Eject Volumes (Volumes auswerfen) an, dass das Auswerfen erfolgreich war.



6. Wählen Sie Close (Schließen) aus, um das Fenster Eject Volumes (Volumes auswerfen) zu schließen.
7. Überprüfen Sie in der Storage-Gateway-Konsole in der VTL des Gateways den Status des Bands, das Sie archivieren. Das Hochladen der Daten in AWS kann einige Zeit dauern. Während des Hochladens wird in der VTL des Gateways als Status für das ausgeworfene Band IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung beginnt, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach dem Hochladen der Daten

wird das ausgeworfene Band nicht mehr in der VTL aufgeführt, aber in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert.

8. Wählen Sie Ihr Gateway und dann VTL Tape Cartridges (VTL-Bandkartuschen) aus und überprüfen Sie, ob das virtuelle Band nicht mehr im Gateway aufgeführt wird.
9. Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Tapes aus. Überprüfen Sie, ob für das archivierte Band der Status ARCHIVED (ARCHIVIERT) angezeigt wird.

Wiederherstellen von Daten von einem Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

Stellen Sie die Daten wie folgt von einem archivierten Band wieder her:

1. Rufen Sie das archivierte Band auf ein Tape Gateway ab. Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie die Software Backup, Archive und Restore, die mit der Ver Bols- NetBackup Anwendung installiert wurde. Der Vorgang ist identisch mit dem Vorgang zur Wiederherstellung von Daten von physischen Bändern. Anleitung hierzu finden Sie unter Veritas Services and Operations Readiness Tools (SORT) auf der Veritas-Website.

Nächster Schritt

Bereinigen nicht benötigter Ressourcen

Wie geht es weiter?

Nachdem Ihr Tape Gateway in den Produktionsmodus übergegangen ist, können Sie verschiedene Verwaltungsaufgaben ausführen, wie z. B. Hinzufügen und Entfernen von Bändern, Überwachung und Optimierung der Gateway-Leistung sowie Problembehebung. Allgemeine Informationen zu diesen Verwaltungsaufgaben finden Sie unter Verwalten von Gateways.

Sie können einige der Tape Gateway-Wartungsaufgaben auf der ausführen AWS Management Console, z. B. die Bandbreitenratenlimits Ihres Gateways konfigurieren und Gateway-Softwareupdates verwalten. Wenn Ihr Tape Gateway On-Premises bereitgestellt wird, können Sie einige dieser Wartungsaufgaben mit der lokalen Gateway-Konsole ausführen. Hierzu gehört das Routing Ihres Tape Gateway über einen Proxy und das Konfigurieren Ihres Gateways für die Verwendung einer statischen IP-Adresse. Wenn Sie Ihr Gateway als Amazon-EC2-Instance

ausführen, können Sie bestimmte Wartungsaufgaben mit der Amazon-EC2-Konsole durchführen, wie beispielsweise das Hinzufügen und Entfernen von Amazon-EBS-Volumes. Weitere Informationen zur Verwaltung Ihres Tape Gateway finden Sie unter Verwalten von Tape Gateway.

Wenn Sie Ihr Gateway in der Produktionsumgebung bereitstellen möchten, sollten Sie beim Festlegen der Festplattengrößen den tatsächlichen Workload in Betracht ziehen. Weitere Informationen zum Bestimmen realer Datenträgergrößen finden Sie unter Verwaltung von lokalen Festplatten für Ihr Storage Gateway. Außerdem sollten Sie eine Bereinigung in Betracht ziehen, wenn Sie nicht planen, Ihr Tape Gateway weiterhin zu verwenden. Durch die Bereinigung können Sie Gebühren vermeiden. Weitere Informationen zur Bereinigung finden Sie unter Bereinigen nicht benötigter Ressourcen.

Bereinigen nicht benötigter Ressourcen

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

Wenn Sie Ihr Tape Gateway weiter verwenden möchten, finden Sie zusätzliche Informationen unter Wie geht es weiter?

So bereinigen Sie nicht benötigte Ressourcen

1. Löschen Sie Bänder aus der Virtual Tape Library (VTL) Ihres Gateways und aus dem Archiv. Weitere Informationen finden Sie unter Löschen des Gateways über die AWS Storage Gateway -Konsole und Bereinigen zugehöriger Ressourcen.
    a. Archivieren Sie alle Bänder, die in der VTL Ihres Gateways den Status RETRIEVED haben. Anweisungen finden Sie unter Archivieren von Bändern.
    b. Löschen Sie alle verbleibenden Bänder aus der Gateway-VTL. Anweisungen finden Sie unter Löschen von Bändern.
    c. Löschen Sie alle Bänder im Archiv. Anweisungen finden Sie unter Löschen von Bändern.
2. Löschen Sie das Tape Gateway, sofern Sie nicht vorhaben, es weiter zu verwenden. Anweisungen finden Sie unter Löschen des Gateways über die AWS Storage Gateway -Konsole und Bereinigen zugehöriger Ressourcen.
3. 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.

Aktivieren eines Gateways in einer Virtual Private 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 ihm die Übertragung von Daten in AWS Speicherdienste zu ermöglichen, ohne über das öffentliche Internet zu kommunizieren. Mit dem Amazon-VPC-Service können Sie - AWS Ressourcen, einschließlich privater Netzwerkschnittstellenendpunkte, 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 zu VPCs finden Sie unter Was ist Amazon VPC? im Amazon-VPC-Benutzerhandbuch.

Zum Aktivieren Ihres Gateways in einer VPC verwenden Sie die Amazon-VPC-Konsole, um einen VPC-Endpunkt für Storage Gateway 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 Verbinden Ihres Tape Gateways, um AWS .

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

Themen

Erstellen eines VPC-Endpunkts für Storage Gateway

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

So erstellen Sie einen VPC-Endpunkt für Storage Gateway

1. Melden Sie sich bei der an AWS Management Console 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 Enable Private DNS Name (Privaten DNS-Namen aktivieren) ausgewählt ist.
7. Wählen Sie in Security group (Sicherheitsgruppe) die Sicherheitsgruppe aus, die Sie für Ihre VPC verwenden möchten. Sie können die Standardsicherheitsgruppe akzeptieren. Stellen Sie sicher, dass alle der folgenden TCP-Ports in Ihrer Sicherheitsgruppe zulässig sind:

   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Wählen Sie 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 sieht ungefähr wie folgt aus: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Da Sie nun über einen VPC-Endpunkt verfügen, können Sie Ihr Gateway erstellen. Weitere Informationen finden Sie unter Erstellen eines Gateways.

Verwalten von Gateways

Zu den Aufgaben im Rahmen der Gateway-Verwaltung zählen die Konfiguration von Cache-Speicher und Upload-Puffer-Kapazität, die Arbeit mit Volumes und virtuellen Bändern sowie allgemeine Wartungsaufgaben. Falls Sie noch kein Gateway erstellt haben, lesen Sie Erste Schritte.

Gateway-Softwareversionen enthalten regelmäßig Betriebssystemupdates und Sicherheitspatches, die validiert wurden. Diese Updates werden im Rahmen des regulären Gateway-Aktualisierungsprozesses während eines geplanten Wartungsfensters installiert und in der Regel alle sechs Monate veröffentlicht. Hinweis: Benutzer sollten die Storage Gateway-Appliance als verwaltete virtuelle Maschine behandeln und nicht versuchen, auf die Storage Gateway-Appliance-Instance zuzugreifen oder diese zu ändern. Der Versuch, Softwarepakete mit anderen Methoden (z. B. SSM- oder Hypervisor-Tools) als dem normalen Gateway-Aktualisierungsmechanismus zu installieren oder zu aktualisieren, kann zu einer Störung der ordnungsgemäßen Funktion des Gateways führen.

Themen

Verwalten von Tape Gateway

In den folgenden Abschnitten erhalten Sie Informationen zum Verwalten Ihrer Tape-Gateway-Ressourcen in AWS Storage Gateway.

Themen

- Löschen von benutzerdefinierten Bandpools
- Deaktivieren Ihres Tape Gateways
- Grundlegendes zum Bandstatus

Bearbeiten grundlegender Gateway-Informationen

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

So bearbeiten Sie grundlegende Informationen für ein vorhandenes Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
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. Ändern Sie die Einstellungen, die Sie ändern möchten, und wählen Sie anschließend Speichern aus.

> **Note**
>
> Wenn Sie den Namen eines Gateways ändern, werden alle CloudWatch Alarme getrennt, die zur Überwachung des Gateways eingerichtet wurden. Um die Alarme erneut zu verbinden, aktualisieren Sie für GatewayName jeden Alarm in der - CloudWatch Konsole.

Hinzufügen virtueller Bänder

Sie können bei Bedarf Bänder in einem Tape Gateway hinzufügen Weitere Informationen zum Erstellen von Bändern finden Sie unter Erstellen von Bändern.

Nachdem Ihr Band erstellt wurde, finden Sie Informationen dazu auf der Seite Bandübersicht. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden,

um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren. Informationen zu Tape Gateway-Bandkontingenten finden Sie unter AWS Storage Gateway - Kontingente.

Verwalten der automatischen Banderstellung

Das Tape Gateway erstellt automatisch neue virtuelle Bänder, um die von Ihnen konfigurierte minimale Anzahl verfügbarer Bänder beizubehalten. Anschließend werden diese neuen Bänder für den Import durch die Sicherungsanwendung zur Verfügung gestellt, so dass Ihre Sicherungsaufgaben ohne Unterbrechung ausgeführt werden können. Durch die automatische Banderstellung wird neben dem manuellen Prozess zum Erstellen neuer virtueller Bänder keine benutzerdefinierten Skripterstellung mehr benötigt.

So ändern oder löschen Sie die Richtlinie für die automatische Banderstellung

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.
3. Wählen Sie das Gateway aus, für das Sie die automatische Banderstellung verwalten möchten.
4. Wählen Sie im Menü Actions (Aktionen) die Option Configure tape auto-create (Automatische Banderstellung konfigurieren).
5. Um eine Richtlinie für die automatische Banderstellung auf einem Gateway zu löschen, wählen Sie das Entfernen rechts neben der Richtlinie aus, die Sie löschen möchten.

   Um die automatische Banderstellung auf einem Gateway zu beenden, löschen Sie alle Richtlinien für die automatische Banderstellung für dieses Gateway.

   Wählen Sie Speichern auf, um das Löschen von Richtlinien für die automatische Banderstellung für das ausgewählte Tape Gateway zu bestätigen.

   > **Note**
   >
   > Das Löschen einer Richtlinie zur automatischen Banderstellung von einem Gateway kann nicht rückgängig gemacht werden.

So ändern Sie Richtlinien für die automatische Banderstellung für ein Tape Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.
3. Wählen Sie das Gateway aus, für das Sie die automatische Banderstellung verwalten möchten.
4. Wählen Sie im Menü Aktionen die Option Automatische Banderstellung konfigurieren und ändern Sie die Einstellungen auf der daraufhin angezeigten Seite.
5. Geben Sie unter Mindestanzahl von Bändern die Mindestanzahl von virtuellen Bändern ein, die auf dem Tape Gateway jederzeit verfügbar sein sollen. Der gültige Bereich für diesen Wert ist mindestens 1 und maximal 10.
6. Geben Sie unter Capacity (Kapazität) die Kapazität der virtuellen Bänder in Byte an. Der gültige Bereich für diesen Wert beträgt mindestens 100 GiB und maximal 15 TiB.
7. Geben Sie in Barcode-Präfix das Präfix an, das dem Barcode virtueller Bänder vorangestellt werden soll.

   > **Note**
   >
   > Virtuelle Bänder werden durch einen Barcode eindeutig identifiziert und Sie können diesem ein Präfix hinzufügen. Das Präfix ist optional, kann jedoch für die Identifizierung Ihrer virtuellen Bänder hilfreich sein. Das Präfix muss aus Großbuchstaben (A-Z) bestehen und ein bis vier Zeichen lang sein.

8. Wählen Sie für Pool entweder Glacier Pool oder Deep Archive Pool aus. Dieser Pool stellt die Speicherklasse dar, in der Ihre Bänder gespeichert werden, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

   - Wählen Sie Glacier Pool aus, wenn Sie Bänder in der Speicherklasse „S3 Glacier Flexible Retrieval“ archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Flexible Retrieval“ archiviert. Sie verwenden „S3 Glacier Flexible Retrieval“ für aktivere Archive, aus denen Sie ein Band in der Regel innerhalb von 3 bis 5 Stunden abrufen können. Ausführliche Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.
   - Wählen Sie Deep Archive Pool, wenn Sie die Bänder in „S3 Glacier Deep Archive“ archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Deep Archive“ archiviert. „S3 Glacier Deep Archive“ wird für die langfristige

Datenaufbewahrung und zur Erhaltung digitaler Daten verwendet, wo nur ein- oder zweimal im Jahr auf die Daten zugegriffen wird. Sie können ein in „S3 Glacier Deep Archive“ archiviertes Band in der Regel innerhalb von 12 Stunden abrufen. Ausführliche Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.

Sie können die in „S3 Glacier Flexible Retrieval“ archivierten Bänder zu einem späteren Zeitpunkt zu „S3 Glacier Deep Archive“ verschieben. Weitere Informationen finden Sie unter Verschieben eines Bands von der Speicherklasse „S3 Glacier Flexible Retrieval“ zur Speicherklasse „S3 Glacier Deep Archive“.

9. Informationen zu Ihren Bändern finden Sie auf der Seite Bandübersicht. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.

   Der Status der verfügbaren virtuellen Bänder wird zunächst auf CREATING (WIRD ERSTELLT) gesetzt, wenn die virtuellen Bänder erstellt werden. Nach der Erstellung der Bänder wird der Status in VERFÜGBAR geändert. Weitere Informationen finden Sie unter Verwalten von Tape Gateway.

   Weitere Informationen zum Aktivieren der automatischen Banderstellung finden Sie unter Automatisches Erstellen von Bändern.

Archivierung virtueller Bänder

Sie können Bänder in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archivieren. Wenn Sie ein Band erstellen, wählen Sie den Archiv-Pool, den Sie zum Archivieren des Bandes verwenden möchten.

Wählen Sie Glacier Pool, wenn Sie das Band in S3 Glacier Flexible Retrieval archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in S3 Glacier Flexible Retrieval archiviert. S3 Glacier Flexible Retrieval wird für aktivere Archive verwendet, in denen die Daten regelmäßig abgerufen und in wenigen Minuten benötigt werden. Detaillierte Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten.

Wählen Sie Deep Archive Pool, wenn Sie das Band in S3 Glacier Deep Archive archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in S3 Glacier Deep Archive archiviert. S3 Glacier Deep Archive wird für die langfristige Datenaufbewahrung und Erhaltung digitaler Daten zu sehr niedrigen Kosten verwendet. Daten in S3 Glacier Deep Archive werden nicht häufig bzw. selten abgerufen. Detaillierte Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten.

> **Note**
>
> Jedes vor dem 27. März 2019 erstellte Band wird direkt in S3 Glacier Flexible Retrieval archiviert, wenn es von Ihrer Sicherungssoftware ausgeworfen wird.

Wenn Ihre Sicherungssoftware ein Band auswirft, wird es automatisch in dem Pool archiviert, den Sie beim Erstellen des Bands gewählt haben. Der Ablauf beim Auswerfen eines Bands hängt von der verwendeten Sicherungssoftware ab. Manche Sicherungssoftware erfordert, dass Sie Bänder nach dem Auswurf exportieren, bevor Sie mit der Archivierung beginnen können. Weitere Informationen zu unterstützter Sicherungssoftware finden Sie unter Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung.

Verschieben eines Bands von der Speicherklasse „S3 Glacier Flexible Retrieval“ zur Speicherklasse „S3 Glacier Deep Archive“

Verschieben Sie Ihre Bänder für die langfristige Datenaufbewahrung und Erhaltung digitaler Daten zu sehr niedrigen Kosten von „S3 Glacier Flexible Retrieval“ zu „S3 Glacier Deep Archive“. „S3 Glacier Deep Archive“ wird für die langfristige Datenaufbewahrung und zur Erhaltung digitaler Daten verwendet, wobei nur ein- oder zweimal im Jahr auf die Daten zugegriffen wird. Detaillierte Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten.

So verschieben Sie ein Band von „S3 Glacier Flexible Retrieval“ zu „S3 Glacier Deep Archive“

1. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1.000 Bänder oder weniger enthält,

können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.

2. Aktivieren Sie die Kontrollkästchen für die Bänder, die Sie in „S3 Glacier Deep Archive“ verschieben möchten. In der Spalte Pool wird der Pool angezeigt, dem jedes Band zugeordnet ist.
3. Klicken Sie auf Pool zuweisen.
4. Überprüfen Sie im Dialogfeld „Band Pool zuweisen“ die Barcodes der Bänder, die Sie verschieben, und wählen Sie Zuweisen aus.

> **Note**
>
> Wenn ein Band von der Sicherungsanwendung ausgeworfen und in „S3 Glacier Deep Archive“ archiviert wurde, können Sie es nicht zurück zu „S3 Glacier Flexible Retrieval“ verschieben. Für das Verschieben Ihrer Bänder von „S3 Glacier Flexible Retrieval“ zu „S3 Glacier Deep Archive“ wird eine Gebühr erhoben. Wenn Sie Bänder vor Ablauf von 90 Tagen von „S3 Glacier Flexible Retrieval“ zu „S3 Glacier Deep Archive“ verschieben, wird für „S3 Glacier Deep Archive“ zudem eine Gebühr für das vorzeitige Löschen berechnet.

5. Nachdem das Band verschoben wurde, können Sie den aktualisierten Status in der Spalte Pool auf der Seite Bandübersicht sehen.

Abrufen archivierter Bänder

Um auf Daten zuzugreifen, die auf einem archivierten virtuellen Band gespeichert sind, müssen Sie zuerst das gewünschte Band in Ihr Tape Gateway abrufen. Das Tape Gateway stellt für jedes Gateway eine virtuelle Bandbibliothek (Virtual Tape Library, VTL) bereit.

Wenn Sie mehr als ein Tape Gateway in einem haben AWS-Region, können Sie ein Band nur an ein Gateway abrufen.

Das abgerufene Band ist schreibgeschützt. Sie können die Daten auf dem Band nur lesen.

> **Important**
>
> Wenn Sie ein Band in „S3 Glacier Flexible Retrieval“ archivieren, können Sie das Band in der Regel innerhalb von 3 bis 5 Stunden abrufen. Wenn Sie das Band in „S3 Glacier Deep Archive“ archivieren, können Sie es in der Regel innerhalb von 12 Stunden abrufen.

> **Note**
>
> Es wird eine Gebühr für das Abrufen von Bänder aus dem Archiv erhoben. Detaillierte Preisinformationen finden Sie unter Storage Gateway – Preise.

So rufen Sie ein archiviertes Band in ein Gateway ab

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.
3. Wählen Sie das abzurufende virtuelle Band auf der Registerkarte Virtuelles Bandregal aus und wählen Sie dann Band abrufen aus.

   > **Note**
   >
   > Der Status des abzurufenden virtuellen Bands muss ARCHIVED lauten.

4. Prüfen Sie im Dialogfeld Retrieve tape (Band abrufen) unter Barcode, dass der Barcode das abzurufende virtuelle Band identifiziert.
5. Wählen Sie für Gateway das Gateway, in das das archivierte Band abgerufen werden soll. Wählen Sie dann Retrieve tape (Band abrufen).

Der Status des Bands ändert sich von "ARCHIVED" zu "RETRIEVING". An diesem Punkt werden die Daten aus dem virtuellen Bandregal (gesichert mit „S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep Archive“) in die virtuelle Bandbibliothek (gesichert mit Amazon S3) verschoben. Nachdem alle Daten verschoben wurden, ändert sich der Status des virtuellen Bands im Archiv zu "RETRIEVED".

> **Note**
>
> Abgerufene virtuelle Bänder sind schreibgeschützt.

Anzeigen der Bandnutzung

Wenn Sie Daten auf ein Band schreiben, können Sie die gespeicherte Datenmenge auf dem Band in der Storage-Gateway-Konsole anzeigen. Die Registerkarte Details für jedes Band zeigt die Informationen zur Bandnutzung an.

So zeigen Sie die gespeicherte Datenmenge auf einem Band an

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.
3. Wählen Sie das gewünschte Band aus.
4. Die daraufhin angezeigte Seite enthält verschiedene Details und Informationen zum Band, darunter die folgenden Angaben:

    - Size (Größe): Die Gesamtkapazität des ausgewählten Bandes.
    - Used (Genutzt): Die Größe der Daten, die von der Sicherungsanwendung auf das Band geschrieben werden.

> **Note**
>
> Dieser Wert ist nicht für Bänder verfügbar, die vor dem 13. Mai 2015 erstellt wurden.

Löschen von Bändern

Sie können virtuelle Bänder mithilfe der Tape Gateway-Konsole aus den dem Storage Gateway löschen.

> **Note**
>
> Wenn das Band, das Sie aus dem Tape Gateway löschen möchten, den Status „RETRIEVED“ aufweist, müssen Sie das Band zuerst mithilfe der Sicherungsanwendung auswerfen, bevor Sie es löschen. Anweisungen zum Auswerfen eines Bands mit der Symantec- NetBackup Software finden Sie unter Archivieren des Bands. Nachdem das Band ausgeworfen wurde, ändert sich der Status zurück zu "ARCHIVED". Sie können das Band dann löschen.

Erstellen Sie Kopien Ihrer Daten, bevor Sie Bänder löschen. Nachdem Sie ein Band gelöscht haben, können Sie es nicht wiederherstellen.

So löschen Sie ein virtuelles Band

> **Warning**
>
> Mit diesem Verfahren wird das ausgewählte virtuelle Band endgültig gelöscht.

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält,

können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.

3. Wählen Sie einen oder mehrere Bänder aus, die gelöscht werden sollen.
4. Wählen Sie unter Aktionen die Option Band löschen aus. Das Bestätigungsdialogfeld wird angezeigt.
5. Vergewissern Sie sich, dass Sie die angegebenen Bänder löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen aus.

Nachdem das Band gelöscht wurde, verschwindet es aus dem Tape Gateway.

Löschen von benutzerdefinierten Bandpools

Sie können einen benutzerdefinierten Bandpool nur löschen, wenn sich keine archivierten Bänder im Pool befinden und dem Pool keine Richtlinien für die automatische Banderstellung zugeordnet sind.

So löschen Sie Ihren benutzerdefinierten Bandpool

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Pools aus, um die verfügbaren Pools anzuzeigen.
3. Wählen Sie einen oder mehrere Bandpools aus, die gelöscht werden sollen.

   Wenn die Bandanzahl für die Bandpools, die Sie löschen möchten, 0 ist und es keine Richtlinien für die automatische Banderstellung gibt, die auf den benutzerdefinierten Bandpool verweisen, können Sie die Pools löschen.
4. Wählen Sie Löschen aus. Das Bestätigungsdialogfeld wird angezeigt.
5. Vergewissern Sie sich, dass Sie die angegebenen Bandpools löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen aus.

   > ⚠ Warning
   >
   > Dieses Verfahren löscht die ausgewählten Bandpools dauerhaft und kann nicht rückgängig gemacht werden.

   Nachdem die Bandpools gelöscht wurden, werden sie aus der Bandbibliothek entfernt.

Deaktivieren Ihres Tape Gateways

Sie deaktivieren ein Tape Gateway wenn das Tape Gateway fehlgeschlagen ist und Sie die Bänder vom fehlgeschlagenen Gateway auf einem anderen Gateway wiederherstellen möchten.

Um die Bänder wiederherzustellen, müssen Sie zunächst das fehlgeschlagene Gateway deaktivieren. Deaktivieren eines Tape Gateway sperrt die virtuellen Bänder in diesem Gateway. Das bedeutet, dass alle Daten, die Sie auf diese Bänder schreiben, nachdem das Gateway deaktiviert wurde, nicht an AWS gesendet werden. Sie können ein Gateway nur über die Storage-Gateway-Konsole deaktivieren, und nur wenn das Gateway nicht mehr mit AWS verbunden ist. Wenn das Gateway mit verbunden ist AWS, können Sie das Tape Gateway nicht deaktivieren.

Sie deaktivieren ein Tape Gateway im Rahmen der Datenwiederherstellung. Weitere Informationen über die Wiederherstellung von Bändern finden Sie unter Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen..

So aktivieren Sie das Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und dann das fehlgeschlagene Gateway.
3. Wählen Sie die Registerkarte Details für das Gateway, um die Meldung zur Deaktivierung des Gateways anzuzeigen.
4. Wählen Sie Wiederherstellungsbänder erstellen.
5. Wählen Sie Gateway deaktivieren.

Grundlegendes zum Bandstatus

Jedes Band verfügt über einen zugeordneten Status, aus dem sich auf einen Blick der Zustand des Bands ersehen lässt. In den meisten Fällen gibt der Status an, dass das Band ordnungsgemäß funktioniert und Sie keine Aktion durchzuführen brauchen. In einigen Fällen gibt der Status ein Problem mit dem Band an, das eventuell eine Aktion Ihrerseits erforderlich macht. Die folgenden Informationen können Sie bei der Entscheidung unterstützen, ob Sie handeln müssen.

Themen

- Grundlegendes zu Bandstatusinformationen in einer VTL
- Bestimmen des Bandstatus in einem Archiv

Grundlegendes zu Bandstatusinformationen in einer VTL

Der Status eines Bands muss AVAILABLE sein, damit Sie auf dem Band lesen oder schreiben können. In der folgenden Tabelle werden mögliche Statuswerte aufgelistet und beschrieben.

Status	Description	Banddaten sind gespeichert auf
WIRD ERSTELLT	Das virtuelle Band wird erstellt. Das Band kann nicht in ein Bandlaufwerk geladen werden, da das Band erstellt wird.	—
VERFÜGBAR	Das virtuelle Band ist erstellt und zum Laden in ein Bandlaufwerk bereit.	Amazon S3
IN TRANSIT TO VTS	Das virtuelle Band wurde ausgeworfen wird für die Archivierung hochgeladen. An diesem Punkt lädt Ihr Tape Gateway Daten in hoch AWS. Wenn die Menge der hochgeladenen Daten gering ist, wird dieser Status möglicherweise nicht angezeigt. Nach Abschluss des Uploads wechselt der Status zu ARCHIVING.	Amazon S3
ARCHIVING	Das virtuelle Band wird vom Tape Gateway in das von „S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep Archive“ unterstützte Archiv verschoben. Dieser Vorgang erfolgt, nachdem der Daten-Upload in abgeschlossen AWS ist.	Daten werden von Amazon S3 in „S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep Archive“ verschoben.
WIRD GELÖSCHT	Das virtuelle Band wird gelöscht.	Daten werden aus Amazon S3 gelöscht.
GELÖSCHT	Das virtuelle Band wurde erfolgreich gelöscht.	—
RETRIEVING	Das virtuelle Band wird aus dem Archiv auf Ihr Tape Gateway abgerufen.	Daten werden von „S3 Glacier Flexible Retrieval “ oder „S3 Glacier Deep Archive“ nach Amazon S3 verschoben.

Status	Description	Banddaten sind gespeichert auf
	Note Das virtuelle Band kann nur auf ein Tape Gateway abgerufen werden.	
RETRIEVED	Das virtuelle Band wurde aus dem Archiv abgerufen. Das abgerufene Band ist schreibgeschützt.	Amazon S3
RECOVERED	Das virtuelle Band wurde wiederhergestellt und ist schreibgeschützt. Wenn aus irgend einem Grund nicht auf Ihr Tape Gateway zugegriffen werden kann, können Sie mit diesem Tape Gateway verknüpfte virtuelle Bänder auf einem anderen Tape Gateway wiederherstellen. Sie müssen das unzugängliche Tape Gateway deaktivieren, bevor Sie virtuelle Bänder wiederherstellen können.	Amazon S3
IRRECOVERABLE	Das virtuelle Band kann weder gelesen noch beschrieben werden. Dieser Status zeigt einen Fehler in Ihrem Tape Gateway an.	Amazon S3

Bestimmen des Bandstatus in einem Archiv

Sie können das folgende Verfahren verwenden, um den Status eines virtuellen Bands in einem Archiv zu ermitteln.

So bestimmen Sie den Status eines virtuellen Bands

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Tapes (Bänder).
3. Prüfen Sie in der Spalte Status des Bandbibliothek-Rasters den Status des Bands.

Der Bandstatus wird auch auf der Registerkarte Details jedes virtuellen Bands angezeigt.

Im Folgenden finden Sie eine Beschreibung der möglichen Statuswerte.

Status	Description
ARCHIVED	Das virtuelle Band wurde ausgeworfen und an das Archiv hochgeladen.
RETRIEVING	Das virtuelle Band wird aus dem Archiv abgerufen. **Note** Das virtuelle Band kann nur auf ein Tape Gateway abgerufen werden.
RETRIEVED	Das virtuelle Band wurde aus dem Archiv abgerufen. Das abgerufene Band ist schreibgeschützt.

Weitere Informationen zum Arbeiten mit Bänder und VTL-Geräten finden Sie unter Arbeiten mit Bändern.

Verschieben Ihrer Daten auf ein neues Gateway

Sie können Daten zwischen Gateways verschieben, wenn Ihre Daten- und Leistungsanforderungen zunehmen oder wenn Sie eine AWS Benachrichtigung zur Migration Ihres Gateways erhalten. Nachfolgend sind einige Gründe für diesen Vorgang ausgeführt:

- Verschieben Sie Ihre Daten zu besseren Host-Plattformen oder neueren Amazon-EC2-Instances.
- Aktualisieren der zugrunde liegenden Hardware für Ihren Server

Welche Schritte Sie befolgen müssen, um Ihre Daten auf ein neues Gateway zu verschieben, hängt von Ihrem Gateway-Typ ab.

Note

Daten können nur zwischen den gleichen Gateway-Typen verschoben werden.

Verschieben virtueller Bänder auf ein neues Tape Gateway

So verschieben Sie ein virtuelles Band auf ein neues Tape Gateway

1. Verwenden Sie Ihre Sicherungsanwendung, um alle Ihre Daten auf einem virtuellen Band zu sichern. Warten Sie, bis die Sicherung erfolgreich abgeschlossen ist.
2. Verwenden Sie Ihre Sicherungsanwendung, um das Band auszuwerfen. Das Band wird in einer Amazon-S3-Speicherklasse gespeichert. Ausgeworfene Bänder werden in „S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep Archive“ archiviert und sind schreibgeschützt.

   Bevor Sie fortfahren, vergewissern Sie sich, dass die ausgeworfenen Bänder archiviert wurden:

   a. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
   b. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.
   c. Prüfen Sie in der Spalte Status der Liste den Status des Bands.

      Der Bandstatus wird auch auf der Registerkarte Details jedes virtuellen Bands angezeigt.

      Weitere Informationen zum Ermitteln des Bandstatus in einem Archiv finden Sie unter Bestimmen des Bandstatus in einem Archiv.
3. Stellen Sie mit Ihrer Sicherungsanwendung sicher, dass keine aktiven Sicherungsaufträge an das vorhandene Tape Gateway gesendet werden, bevor Sie es beenden. Falls aktive Sicherungsaufträge vorhanden sind, warten Sie, bis diese abgeschlossen sind, und werfen Sie die Bänder aus (siehe vorherigen Schritt), bevor Sie das Gateway beenden.
4. Führen Sie die folgenden Schritte aus, um das vorhandene Tape Gateway zu beenden:

   a. Wählen Sie im Navigationsbereich Gateways und anschließend das alte Tape Gateway aus, das Sie beenden möchten. Der Status des Gateways ist Wird ausgeführt.
   b. Wählen Sie unter Aktionen die Option Gateway anhalten aus. Überprüfen Sie die ID des Gateways im Dialogfeld und wählen Sie dann Gateway anhalten aus.

Während das alte Tape Gateway angehalten wird, sehen Sie möglicherweise eine Meldung mit dem Status des Gateways. Wenn das Gateway heruntergefahren wird, werden eine Meldung und die Schaltfläche Gateway starten auf der Registerkarte Details angezeigt.

Weitere Informationen zum Anhalten von Gateways finden Sie unter Starten und Anhalten von Tape Gateway.

5. Erstellen Sie ein Tape Gateway. Detaillierte Anweisungen finden Sie unter Erstellen von Gateways.
6. Führen Sie die folgenden Schritte aus, um neue Bänder zu erstellen:

   a. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.

   b. Wählen Sie Bänder erstellen aus, um das Dialogfeld Bänder erstellen zu öffnen.

   c. Wählen Sie in Gateway (Gateway) einen Gateway aus. Das Band wird für dieses Gateway erstellt.

   d. Wählen Sie unter Number of tapes (Anzahl der Bänder) die Anzahl der Bänder aus, die Sie erstellen möchten. Weitere Informationen zu den Limits für Bänder finden Sie unter AWS Storage Gateway -Kontingente.

      Sie können an dieser Stelle auch die automatische Banderstellung einrichten. Weitere Informationen finden Sie unter Automatisches Erstellen von Bändern.

   e. Geben Sie unter Capacity (Kapazität) die Größe des virtuellen Bandes ein, das Sie erstellen möchten. Bänder müssen größer als 100 GiB sein. Weitere Informationen zu den Kapazitätslimits finden Sie unter AWS Storage Gateway -Kontingente.

   f. Geben Sie in Barcode-Präfix das Präfix an, das dem Barcode virtueller Bänder vorangestellt werden soll.

      > **Note**
      >
      > Virtuelle Bänder werden eindeutig durch einen Barcode identifiziert. Sie können dem Barcode ein Präfix voranstellen. Das Präfix ist optional, kann jedoch für die Identifizierung Ihrer virtuellen Bänder hilfreich sein. Das Präfix muss aus Großbuchstaben (A-Z) bestehen und ein bis vier Zeichen lang sein.

g. Wählen Sie für Pool entweder Glacier Pool oder Deep Archive Pool aus. Dieser Pool stellt die Speicherklasse dar, in der Ihr Band gespeichert wird, wenn es von Ihrer Sicherungssoftware ausgeworfen wird.

   Wählen Sie Glacier Pool, wenn Sie das Band in „S3 Glacier Flexible Retrieval“ archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Flexible Retrieval“ archiviert. Sie verwenden „S3 Glacier Flexible Retrieval“ für aktivere Archive, aus denen Sie ein Band in der Regel innerhalb von 3 bis 5 Stunden abrufen können. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.

   Wählen Sie Deep Archive Pool, wenn Sie das Band in „S3 Glacier Deep Archive“ archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Deep Archive“ archiviert. „S3 Glacier Deep Archive“ wird für die langfristige Datenaufbewahrung und zur Erhaltung digitaler Daten verwendet, wo nur ein- oder zweimal im Jahr auf die Daten zugegriffen wird. Sie können ein in „S3 Glacier Deep Archive“ archiviertes Band in der Regel innerhalb von 12 Stunden abrufen. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.

   Sie können die in „S3 Glacier Flexible Retrieval“ archivierten Bänder zu einem späteren Zeitpunkt zu „S3 Glacier Deep Archive“ verschieben. Weitere Informationen finden Sie unter Verschieben eines Bands von der Speicherklasse „S3 Glacier Flexible Retrieval“ zur Speicherklasse „S3 Glacier Deep Archive“.

   > **Note**
   >
   > Vor dem 27. März 2019 erstellte Bänder werden direkt in „S3 Glacier Flexible Retrieval“ archiviert, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

h. (Optional) Geben Sie unter Tags einen Schlüssel und einen Wert ein, um Ihrem Band Tags hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen Ihrer Bänder erleichtert.

i. Wählen Sie Create tapes (Bänder erstellen) aus.

7. Starten Sie mit Ihrer Sicherungsanwendung einen Sicherungsauftrag und sichern Sie Ihre Daten auf dem neuen Band.

8. (Optional) Wenn Ihr Band archiviert worden ist und Sie darauf vorhandene Daten wiederherstellen müssen, rufen Sie diese auf dem neuen Tape Gateway ab. Das Band befindet sich im schreibgeschützten Modus. Weitere Informationen zum Abrufen archivierter Bänder finden Sie unter Abrufen archivierter Bänder.

   > **Note**
   >
   > Es können Gebühren für ausgehende Daten anfallen.

   a. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1 000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.

   b. Wählen Sie das virtuelle Band aus, das Sie abrufen möchten. Wählen Sie unter Aktionen die Option Band abrufen aus.

      > **Note**
      >
      > Der Status des abzurufenden virtuellen Bands muss `ARCHIVED` lauten.

   c. Prüfen Sie im Dialogfeld Retrieve tape (Band abrufen) unter Barcode, dass der Barcode das abzurufende virtuelle Band identifiziert.

   d. Wählen Sie für Gateway das neue Tape Gateway aus, in das das archivierte Band abgerufen werden soll. Wählen Sie anschließend Band abrufen aus.

Wenn Sie sich vergewissert haben, dass Ihr neues Tape Gateway ordnungsgemäß funktioniert, können Sie das alte Tape Gateway löschen.

> **Important**
>
> Bevor Sie ein Gateway löschen, stellen Sie sicher, dass derzeit keine Anwendungen in die Volumes dieses Gateways schreiben. Wenn Sie ein Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten.

9. Gehen Sie folgendermaßen vor, um das alte Tape Gateway zu löschen:

> **Warning**
>
> Wenn ein Gateway gelöscht wurde, gibt es keine Möglichkeit, es wiederherzustellen.

   a. Wählen Sie im Navigationsbereich zunächst Gateways und anschließend das Gateway aus, das Sie löschen möchten.
   b. Wählen Sie für Aktionen die Option Gateway löschen aus.

      Vergewissern Sie sich im daraufhin angezeigten Bestätigungsdialogfeld, dass die angegebene Gateway-ID das alte Tape Gateway bezeichnet, das Sie löschen möchten, geben Sie **`delete`** in das Bestätigungsfeld ein, und wählen Sie dann Löschen.
   c. Löschen Sie die VM. Weitere Informationen zum Löschen einer VM finden Sie in der Dokumentation für Ihren Hypervisor.

Überwachen von Storage Gateway

In diesem Abschnitt wird beschrieben, wie Sie ein Gateway einschließlich der mit dem Gateway verknüpften Ressourcen mithilfe von Amazon überwachen CloudWatch. Sie können den Upload-Puffer und den Cache-Speicher des Gateways überwachen. Verwenden Sie die Storage Gateway-Konsole, um Metriken und Alarme für Ihr Gateway anzuzeigen. Sie können beispielsweise die für Lese- und Schreiboperationen verwendete Anzahl von Bytes, die für Lese- und Schreiboperationen aufgewendete Zeit und die Zeit für das Abrufen von Daten aus der Amazon Web Services Cloud 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 einen besseren Überblick darüber erhalten, wie das Gateway und die Volumes arbeiten. Storage Gateway bietet auch CloudWatch Alarme, außer hochauflösende Alarme, ohne zusätzliche Kosten. Weitere Informationen zu CloudWatch Preisen finden Sie unter Amazon- CloudWatch Preise. Weitere Informationen zu finden Sie CloudWatchim Amazon CloudWatch -Benutzerhandbuch.

Themen

Grundlagen zu Gateway-Metriken

Für die Diskussion in diesem Thema definieren wir Gateway-Metriken als Metriken, die sich auf das Gateway beziehen – das heißt, sie messen einen bestimmten Aspekt des Gateways. Da ein Gateway ein oder mehrere Volumes enthält, steht eine Gateway-spezifische Metrik stellvertretend

für alle Volumes auf dem Gateway. Die `CloudBytesUploaded`-Metrik stellt beispielsweise die Gesamtanzahl der Bytes dar, die das Gateway im Berichtszeitraum an die Cloud gesendet hat. Diese Metrik enthält die Aktivitäten aller Volumes auf dem Gateway.

Bei der Verwendung von Gateway-Metrikdaten geben Sie die eindeutige Identifikation des Gateways an, für das Sie Metriken anzeigen möchten. Zu diesem Zweck geben Sie die Werte `GatewayId` und `GatewayName` an. Wenn Sie mit einer Metrik für ein Gateway arbeiten möchten, geben Sie die Gateway-Dimension im Metrik-Namespace an, der eine Gateway-spezifische Metrik von einer Volume-spezifischen Metrik unterscheidet. Weitere Informationen finden Sie unter Verwenden von Amazon CloudWatch Metrics.

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

Metrik	Beschreibung
`AvailabilityNotifications`	Anzahl der vom Gateway generierten Zustandsbenachrichtigungen im Zusammenhang mit der Verfügbarkeit. Verwenden Sie diese Metrik zusammen mit der Statistik `Sum`, um zu beobachten, ob Ereignisse im Zusammenhang mit der Verfügbarkeit im Gateway auftreten. Weitere Informationen zu den Ereignissen finden Sie in Ihrer konfigurierten CloudWatch Protokollgruppe. Einheit: Zahl

Metrik	Beschreibung
CacheHitPercent	Prozentsatz der Lesevorgänge einer Anwendung, die aus dem Cache abgearbeitet wurden. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheit: Prozent
CacheUsed	Gesamtanzahl der im Gateway-Cache-Speicher verwendeten Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheit: Byte
IoWaitPercent	Prozentsatz der Zeit, die das Gateway auf eine Antwort vom lokalen Datenträger wartet. Einheit: Prozent
MemTotalBytes	Menge an RAM, das für die Gateway-VM bereitgestellt wird, in Bytes. Einheit: Byte
MemUsedBytes	Menge an RAM, das derzeit von der Gateway-VM verwendet wird, in Bytes. Einheit: Byte

Metrik	Beschreibung	
QueuedWrites	Die Anzahl der Bytes, die darauf warten, in geschrieb en zu werden AWS, die am Ende des Benachrichtigungsz eitraums für alle Volumes im Gateway erfasst werden. Diese Byte werden in Ihrem Gateway-Arbeitsspeicher gespeichert. Einheit: Byte	
TotalCacheSize	Die Gesamtgröße des Cache in Byte. Die Stichprobe wird am Ende des Berichtsz eitraums entnommen. Einheit: Byte	
UploadBufferPercen tUsed	Prozentuale Nutzung des Gateway-Upload-Puffers. Die Stichprobe wird am Ende des Berichtszeitraums entnommen . Einheit: Prozent	
UploadBufferUsed	Gesamtanzahl der im Gateway-Upload-Puffer verwendeten Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen . Einheit: Byte	

Metrik	Beschreibung	
`UserCpuPercent`	Prozentsatz der CPU-Zeit, die für die Gateway-Verarbeitung aufgewendet wurde, gemittelt über alle Kerne. Einheit: Prozent	

Dimensionen für Storage Gateway-Metriken

Der CloudWatch Namespace für den Storage Gateway-Service ist `AWS/StorageGateway`. Die Daten werden automatisch in 5-Minuten-Intervallen kostenlos zur Verfügung gestellt.

Dimension	Beschreibung
`GatewayId` , `GatewayName`	Diese Dimensionen filtern die angeforderten Daten nach Gateway-spezifischen Metriken. Sie können ein zu verwenden des Gateway anhand des Werts für `GatewayId` oder `GatewayName` identifizieren. Wenn das Gateways im Zeitraum, für den Sie Metriken anzeigen möchten, einen anderen Namen hatte, verwenden Sie die `GatewayId` . Die Durchsatz- und Latenzdaten eines Gateways basieren auf sämtlichen Volumes für dieses Gateway. Informationen zum Arbeiten mit Gateway-Metriken finden Sie unter Messen der Leistung zwischen Ihrem Gateway und AWS.

Überwachen des Upload-Puffers

Im Folgenden finden Sie Informationen zur Überwachung des Gateway-Upload-Puffers und zum Erstellen eines Alarms, sodass Sie eine Benachrichtigung erhalten, wenn der Puffer einen bestimmten Grenzwert überschreitet. Mit diesem Ansatz können Sie einem Gateway Pufferspeicher hinzufügen, bevor er vollständig belegt ist und Ihre Speicheranwendung die Sicherung auf AWS stoppt.

Sie überwachen den Upload-Puffer in Architekturen mit zwischengespeicherten Volumes und Tape Gateway-Architekturen auf dieselbe Weise. Weitere Informationen finden Sie unter So funktioniert Tape Gateway (Architektur).

> **Note**
>
> Die Metriken `WorkingStoragePercentUsed`, `WorkingStorageUsed` und `WorkingStorageFree` stellen den Upload-Puffer für gespeicherte Volumes nur bis zur Freigabe das Feature für zwischengespeicherte Volumes in Storage Gateway dar. Verwenden Sie jetzt die entsprechenden Upload-Puffer-Metriken `UploadBufferPercentUsed`, `UploadBufferUsed` und `UploadBufferFree`. Diese Metriken gelten für beide Gateway-Architekturen.

Interessierendes Element	Methode zum Messen
Nutzung des Upload-Puffers	Verwenden Sie die Metriken `UploadBufferPercentUsed` , `UploadBufferUsed` und `UploadBufferFree` mit der Statistik `Average`. Verwenden Sie z. B. `UploadBufferUsed` mit der `Average`-Statistik für die Analyse der Speichernutzung über einen Zeitraum.

So messen Sie den verwendeten Prozentsatz des Upload-Puffers.

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Gateway, mit dem Sie arbeiten möchten.
3. Wählen Sie die Metrik `UploadBufferPercentUsed` aus.
4. Wählen Sie einen Wert für Zeitraum aus.
5. Wählen Sie die `Average`-Statistik aus.
6. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

Die resultierende zeitlich sortierte Gruppe von Datenpunkten enthält die prozentuale Nutzung des Upload-Puffers.

Mit dem folgenden Verfahren können Sie mithilfe der CloudWatch Konsole einen Alarm erstellen. Weitere Informationen zu Alarmen und Schwellenwerten finden Sie unter Erstellen von CloudWatch Alarmen im Amazon- CloudWatch Benutzerhandbuch.

So richten Sie einen Obergrenzenalarm für den Gateway-Upload-Puffer ein

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Alarm erstellen, um den Assistenten zum Erstellen von Alarmen zu starten.
3. Geben Sie eine Metrik für den Alarm an:
   a. Wählen Sie auf der Seite Metrik auswählen des Assistenten zum Erstellen von Alarmen die Dimension AWS/StorageGateway:GatewayId,GatewayName aus und suchen Sie dann das Gateway, mit dem Sie arbeiten möchten.
   b. Wählen Sie die Metrik `UploadBufferPercentUsed` aus. Verwenden Sie die `Average`-Statistik und einen Zeitraum von 5 Minuten.
   c. Klicken Sie auf Weiter.
4. Definieren Sie den Namen, die Beschreibung und den Schwellenwert für den Alarm:
   a. Identifizieren Sie den Alarm auf der Seite Define Alarm (Alarm definieren) des Assistenten zum Erstellen von Alarmen, indem Sie in den Feldern Name und Description (Beschreibung) einen Namen und eine Beschreibung eingeben.
   b. Definieren Sie den Schwellenwert für den Alarm.
   c. Klicken Sie auf Weiter.
5. Konfigurieren Sie eine E-Mail-Aktion für den Alarm:
   a. Wählen Sie auf der Seite Configure Actions (Aktionen konfigurieren) des Assistenten zum Erstellen von Alarmen die Option Alarm für Alarm State (Alarmstatus) aus.
   b. Wählen Sie Choose or create email topic (E-Mail-Thema wählen oder erstellen) für Topic (Thema) aus.

      Das Erstellen eines E-Mail-Themas bedeutet, dass Sie ein Amazon-SNS-Thema einrichten. Weitere Informationen zu Amazon SNS finden Sie unter Einrichten von Amazon SNS im Amazon CloudWatch -Benutzerhandbuch.
   c. Geben Sie unter Topic (Thema) einen aussagekräftigen Namen für das Thema ein.
   d. Wählen Sie Add Action (Aktion hinzufügen) aus.

e. Klicken Sie auf Weiter.

6. Überprüfen Sie die Alarmeinstellungen und erstellen Sie den Alarm:

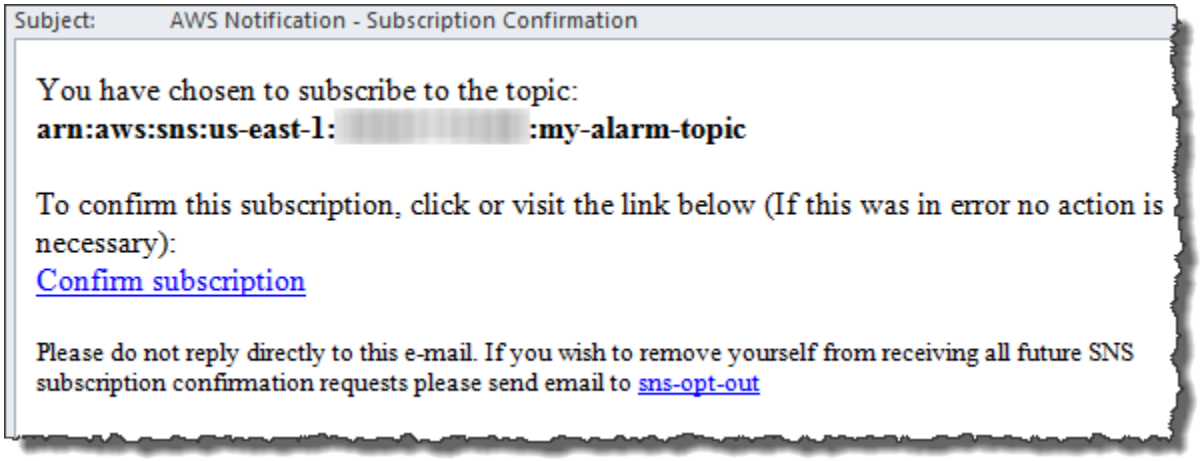
   a. Überprüfen Sie auf der Seite Review (Überprüfen) des Assistenten zum Erstellen von Alarmen die Alarmdefinition, die Metrik und die zugehörigen Aktionen (z. B. das Senden einer E-Mail-Benachrichtigung).

   b. Nach dem Überprüfen der Alarmzusammenfassung wählen Sie Save Alarm (Alarm speichern).

7. Bestätigen Sie das Abonnement des Alarmthemas:

   a. Öffnen Sie die Amazon-SNS-E-Mail, die an die E-Mail-Adresse gesendet wurde, die Sie beim Erstellen des Themas angegeben haben.

      Die folgende Abbildung zeigt eine typische E-Mail-Benachrichtigung.



   b. Bestätigen Sie Ihr Abonnement, indem Sie auf den Link in der E-Mail klicken.

      Eine Abonnement-Bestätigung wird angezeigt.

Überwachen des Cache-Speichers

Im Folgenden finden Sie Informationen zur Überwachung des Gateway-Cache-Speichers und zum Erstellen eines Alarms, sodass Sie eine Benachrichtigung erhalten, wenn Parameter des Caches bestimmte Schwellenwerte überschreiten. Durch diesen Alarm werden Sie benachrichtigt, wenn Sie einem Gateway Cache-Speicher hinzufügen sollten.

Cache-Speicher kann nur in der Cached-Volumes-Architektur überwacht werden. Weitere Informationen finden Sie unter So funktioniert Tape Gateway (Architektur).

Interessierendes Element	Methode zum Messen
Gesamtnutzung des Caches	Verwenden Sie die Metriken `CachePercentUsed` und `TotalCacheSize` mit der Statistik `Average`. Verwenden Sie z. B. `CachePercentUsed` mit der `Average`-Statistik für die Analyse der Cache-Nutzung über einen Zeitraum. Die `TotalCacheSize` -Metrik ändert sich nur, wenn Sie Cache zum Gateway hinzufügen.
Prozentsatz der aus dem Cache bedienten Leseanfragen	Verwenden Sie die `CacheHitPercent` -Metrik mit der `Average`-Statistik. In der Regel soll `CacheHitPercent` auf einem hohen Wert bleiben.
Prozentsatz des Cache, der nicht mehr aktuell ist, d. h. er enthält Inhalte, die nicht in hochgeladen wurden AWS	Verwenden Sie die `CachePercentDirty` -Metrik mit der `Average`-Statistik. In der Regel soll `CachePercentDirty` auf einem niedrigen Wert bleiben.

So messen Sie den Prozentsatz eines Caches mit geänderten Daten für ein Gateway und alle zugehörigen Volumes

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Dimension StorageGateway: Gateway-Metriken und suchen Sie das Gateway, mit dem Sie arbeiten möchten.
3. Wählen Sie die Metrik `CachePercentDirty` aus.
4. Wählen Sie einen Wert für Zeitraum aus.
5. Wählen Sie die `Average`-Statistik aus.
6. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

Die resultierende zeitlich sortierte Gruppe von Datenpunkten enthält den Prozentsatz des Caches mit geänderten Daten über den Zeitraum von 5 Minuten.

So messen Sie den Prozentsatz des Caches mit geänderten Daten für ein Volume

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Dimension StorageGateway: Volume Metrics und suchen Sie das Volume, mit dem Sie arbeiten möchten.
3. Wählen Sie die Metrik `CachePercentDirty` aus.
4. Wählen Sie einen Wert für Zeitraum aus.
5. Wählen Sie die `Average`-Statistik aus.
6. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

Die resultierende zeitlich sortierte Gruppe von Datenpunkten enthält den Prozentsatz des Caches mit geänderten Daten über den Zeitraum von 5 Minuten.

Grundlegendes zu CloudWatch Alarmen

CloudWatch Alarme überwachen Informationen über Ihr Gateway basierend auf Metriken und Ausdrücken. Sie können CloudWatch Alarme für Ihr Gateway hinzufügen und deren Status in der Storage Gateway-Konsole anzeigen. Weitere Informationen zu den Metriken, die zur Überwachung von Tape Gateway verwendet werden, finden Sie unter Grundlegendes zu Gateway-Metriken und Grundlegendes zu Metriken für virtuelle Bänder. Für jeden Alarm geben Sie Bedingungen an, unter denen der ALARM-Status ausgelöst wird. 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 Amazon CloudWatch-Alarmen im Amazon- CloudWatch Benutzerhandbuch.

> **Note**
>
> Wenn Sie nicht über die Berechtigung zum Anzeigen von verfügen CloudWatch, können Sie die Alarme nicht anzeigen.

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
- Zustandsbenachrichtigungen: `HealthNotifications` >= 1 für 1 Datenpunkt innerhalb von 5 Minuten Stellen Sie bei der Konfiguration dieses Alarms die Option Behandlung fehlender Daten auf notBreaching ein.

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

Für Gateways auf VMware-Hostplattformen mit aktiviertem HA-Modus empfehlen wir auch diesen zusätzlichen CloudWatch Alarm:

- 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 wird der Status eines Alarms beschrieben.

Status	Beschreibung
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

Status	Beschreibung
	neuen Alarms finden Sie unter Erstellen eines benutzerdefinierten CloudWatch Alarms für Ihr Gateway.
Nicht verfügbar	Der Status des Alarms ist unbekannt. Wählen Sie Nicht verfügbar aus, um Fehlerinformationen auf der Registerkarte Überwachung anzuzeigen.

Erstellen empfohlener CloudWatch Alarme für Ihr Gateway

Wenn Sie ein neues Gateway mit der Storage Gateway-Konsole erstellen, können Sie im Rahmen des ersten Einrichtungsprozesses alle empfohlenen CloudWatch Alarme automatisch erstellen. Weitere Informationen finden Sie unter Konfigurieren von Tape Gateway . Wenn Sie empfohlene CloudWatch Alarme für ein vorhandenes Gateway hinzufügen oder aktualisieren möchten, gehen Sie wie folgt vor.

So fügen Sie empfohlene CloudWatch Alarme für ein vorhandenes Gateway hinzu oder aktualisieren sie

> **Note**
>
> Diese Funktion erfordert CloudWatch Richtlinienberechtigungen, die nicht automatisch als Teil der vorkonfigurierten Storage 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 deaktiveren
> - `cloudwatch:EnableAlarmActions` – Alarmaktionen aktiveren
> - `cloudwatch:DeleteAlarms` – Alarme löschen

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

2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie empfohlene CloudWatch Alarme erstellen möchten.
3. Wählen Sie auf der Seite mit Gateway-Details die Registerkarte Überwachung aus.
4. Wählen Sie unter Alarme die Option Empfohlene Alarme erstellen aus. Die empfohlenen Alarme werden automatisch erstellt.

   Der Abschnitt Alarme listet alle CloudWatch Alarme für ein bestimmtes Gateway auf. Hier können Sie einen oder mehrere Alarme auswählen und löschen, Alarmaktionen ein- oder ausschalten und neue Alarme erstellen.

Erstellen eines benutzerdefinierten CloudWatch Alarms für Ihr Gateway

CloudWatch verwendet Amazon Simple Notification Service (Amazon SNS), um Alarmbenachrichtigungen zu senden, wenn sich ein Alarm 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-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-Konsole

1. Öffnen Sie die Storage Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home/.
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-Zustand über, wenn die Metrik für eine bestimmte Anzahl von Auswertungszeiträumen den Schwellenwert überschreitet.

Informationen zum Erstellen eines statischen Schwellenwertalarms finden Sie unter Erstellen eines CloudWatch Alarms basierend auf einem statischen Schwellenwert im Amazon-CloudWatch 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 Anomalieerkennung fest und CloudWatch verwenden diesen Schwellenwert 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 zur Anomalieerkennung finden Sie unter Erstellen eines CloudWatch Alarms basierend auf Anomalieerkennung im Amazon- CloudWatch 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 mathematische Metrikausdrücke finden Sie unter Erstellen eines CloudWatch Alarms basierend auf einem mathematischen Metrikausdruck im Amazon- CloudWatch 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 Amazon- CloudWatch Benutzerhandbuch.

6. Nachdem Sie den Alarm in der CloudWatch Konsole erstellt haben, kehren Sie zur Storage 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 CloudWatch die Option Alarme aus.
   - Wählen Sie im Navigationsbereich zunächst Gateways, dann das Gateway, für das Sie Alarme anzeigen möchten, und schließlich die Registerkarte Überwachung aus.

Der Abschnitt Alarme listet alle CloudWatch Alarme für ein bestimmtes Gateway auf. Hier können Sie einen oder mehrere Alarme auswählen und löschen, Alarmaktionen ein- oder ausschalten 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 Bearbeiten oder Löschen eines CloudWatch Alarms.

> **Note**
>
> Wenn Sie ein Gateway über die Storage Gateway-Konsole löschen, werden auch alle dem Gateway zugeordneten CloudWatch Alarme automatisch gelöscht.

Überwachen von Tape Gateway

In diesem Abschnitt finden Sie Informationen zur Überwachung von Tape Gateway, der mit Tape Gateway verknüpften virtuellen Bänder, des Cache-Speichers und des Upload-Puffers. Sie verwenden die AWS Management Console , um Metriken für Ihr Tape Gateway anzuzeigen. Mit Metriken können Sie den Zustand von Tape Gateway verfolgen und Alarme festlegen, sodass Sie benachrichtigt werden, wenn 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 Verlaufsinformationen zugreifen und sich einen besseren Überblick über die Leistung von Tape Gateway und der virtuellen Bänder verschaffen. Ausführliche Informationen zu CloudWatchfinden Sie im Amazon CloudWatch-Benutzerhandbuch.

Themen

- Abrufen von Zustandsprotokollen für Tape Gateways mit CloudWatch-Protokollgruppen
- Verwenden von Amazon CloudWatch Metrics
- Grundlegendes zu Metriken für virtuelle Bänder
- Messung der Leistung zwischen Ihrem Tape Gateway und AWS

Abrufen von Zustandsprotokollen für Tape Gateways mit CloudWatch-Protokollgruppen

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

Nehmen wir beispielsweise an, dass Ihr Gateway in einem mit VMware HA aktivierten Cluster bereitgestellt wird und Sie sich über eventuelle Fehler informieren möchten. Sie können eine CloudWatch Protokollgruppe konfigurieren, um Ihr Gateway zu überwachen und benachrichtigt zu werden, wenn Ihr Gateway auf einen Fehler stößt. Sie können die Gruppe entweder beim Aktivieren des Gateways konfigurieren oder nachdem das Gateway aktiviert wurde und in Betrieb ist. Informationen zum Konfigurieren einer CloudWatch Protokollgruppe beim Aktivieren eines Gateways finden Sie unter Konfigurieren Ihres Tape Gateways. Allgemeine Informationen zu CloudWatch Protokollgruppen finden Sie unter Arbeiten mit Protokollgruppen und Protokollstreams im Amazon CloudWatch -Benutzerhandbuch.

Weitere Informationen zum Beheben von Fehlern dieser Art finden Sie unter Beheben von Problemen mit virtuellen Bändern.

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

So konfigurieren Sie eine CloudWatch Protokollgruppe für die Arbeit mit Ihrem File Gateway

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Storage Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
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 oder wählen Sie auf der Registerkarte Details unter Zustandsprotokolle und Nicht aktiviert die Option Protokollgruppe konfigurieren aus, um das Dialogfeld Bearbeiten CustomerGatewayName zu öffnen.
4. Wählen Sie für Gateway-Zustandsprotokollgruppe eine der folgenden Optionen aus:

- Deaktivieren Sie die Protokollierung, wenn Sie Ihr Gateway nicht mithilfe von CloudWatch Protokollgruppen überwachen möchten.
- 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.

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 unter Zustandsprotokolle die Option CloudWatch Protokolle aus. Die Seite Protokollgruppendetails wird in der CloudWatch -Konsole geöffnet.

Im Folgenden finden Sie ein Beispiel für eine Tape Gateway-Ereignismeldung, die an gesendet wird CloudWatch. In diesem Beispiel wird eine `TapeStatusTransition`-Meldung angezeigt.

```
{
"severity": "INFO",
"source": "FZTT16FCF5",
"type": "TapeStatusTransition",
"gateway": "sgw-C51DFEAC",
"timestamp": "1581553463831",
"newStatus": "RETRIEVED"
}
```

Verwenden von Amazon CloudWatch Metrics

Sie können Überwachungsdaten für Ihr Tape Gateway abrufen, indem Sie entweder die AWS Management Console oder die CloudWatch API verwenden. Die Konsole zeigt eine Reihe von Graphen an, die auf den unformatierten Daten aus der CloudWatch -API basieren. Die CloudWatch API kann auch über eines der Amazon AWS Software Development Kits (SDKs) oder die Amazon

CloudWatch -API-Tools verwendet werden. Je nach Anforderungen können Sie entweder die in der Konsole angezeigten oder die mit der API aufgerufenen Graphen verwenden.

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

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

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

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

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

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

Grundlegendes zu Metriken für virtuelle Bänder

Im Folgenden finden Sie Informationen über die Storage-Gateway-Metriken, die virtuelle Bänder betreffen. Jedem Band ist eine Reihe von Metriken zugeordnet.

Einige bandspezifische Metriken können denselben Namen wie bestimmte Gateway-spezifische Metriken haben. Diese Metriken stellen die gleichen Messungsarten dar, beziehen sich jedoch auf ein Band anstatt auf ein Gateway. Geben Sie vor Beginn der Arbeit an, ob Sie mit einer Gateway-Metrik oder einer Bandmetrik arbeiten möchten. Geben Sie beim Arbeiten mit Bandmetriken die Band-ID für das Band an, für das Sie Metriken anzeigen möchten. Weitere Informationen finden Sie unter Verwenden von Amazon CloudWatch Metrics.

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

Die folgende Tabelle enthält die Storage-Gateway-Metriken, die Sie zum Abrufen von Informationen über Ihre Bänder verwenden können.

Metrik	Beschreibung
`CachePercentDirty`	Der Anteil des Bands am Gesamtprozentsatz des Gateway-Caches, der nicht dauerhaft in AWS gespeichert wird. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Verwenden Sie die Metrik `CachePercentDirty` des Gateways, um den Gesamtprozentsatz des Gateway-Caches anzuzeigen, der nicht dauerhaft in AWS gespeichert

Metrik	Beschreibung
	wird. Weitere Informationen finden Sie unter Grundlagen zu Gateway-Metriken. Einheiten: Prozent
`CloudTraffic`	Die Anzahl der hochgeladenen und von der Cloud auf das Band heruntergeladenen Bytes. Einheiten: Byte
`IoWaitPercent`	Der Prozentsatz der zugewiesenen IoWait Einheiten, die derzeit vom Band verwendet werden. Einheiten: Prozent
`HealthNotification`	Die Anzahl der vom Band gesendeten Zustandsbenachrichtigungen. Einheiten: Anzahl
`MemUsedBytes`	Der Prozentsatz des zugewiesenen Speichers, der gegenwärtig vom Band verwendet wird. Einheiten: Byte
`MemTotalBytes`	Der Prozentsatz des Gesamtspeichers, der gegenwärtig vom Band verwendet wird. Einheiten: Byte

Metrik	Beschreibung
`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
`UserCpuPercent`	Der Prozentsatz der dem Benutzer zugewiesenen CPU-Datenverarbeitungseinheiten, die gegenwärtig vom Band verwendet werden. Einheiten: Prozent
`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

Messung der Leistung zwischen Ihrem Tape Gateway und AWS

Datendurchsatz, Datenlatenz und Operationen pro Sekunde sind Maßzahlen, mit denen Sie die Leistung des Anwendungsspeichers, der Ihr Tape Gateway verwendet, beurteilen können. Wenn Sie die richtige Aggregationsstatistik verwenden, können diese Werte mit den Storage-Gateway-Metriken gemessen werden, die für Sie bereitgestellt werden.

Eine Statistik ist eine Aggregation einer Metrik über einen bestimmten Zeitraum. Wenn Sie die Werte einer Metrik in anzeigen CloudWatch, verwenden Sie die `Average` -Statistik für die Datenlatenz

(Millisekunden) und die `Samples` -Statistik für Eingabe-/Ausgabevorgänge pro Sekunde (IOPS). Weitere Informationen finden Sie unter Statistiken im Amazon- CloudWatch Benutzerhandbuch.

In der folgenden Tabelle werden die Metriken und die entsprechenden Statistiken zusammengefasst, mit denen Sie Durchsatz, Latenz und IOPS zwischen Ihrem Tape Gateway und AWS messen können.

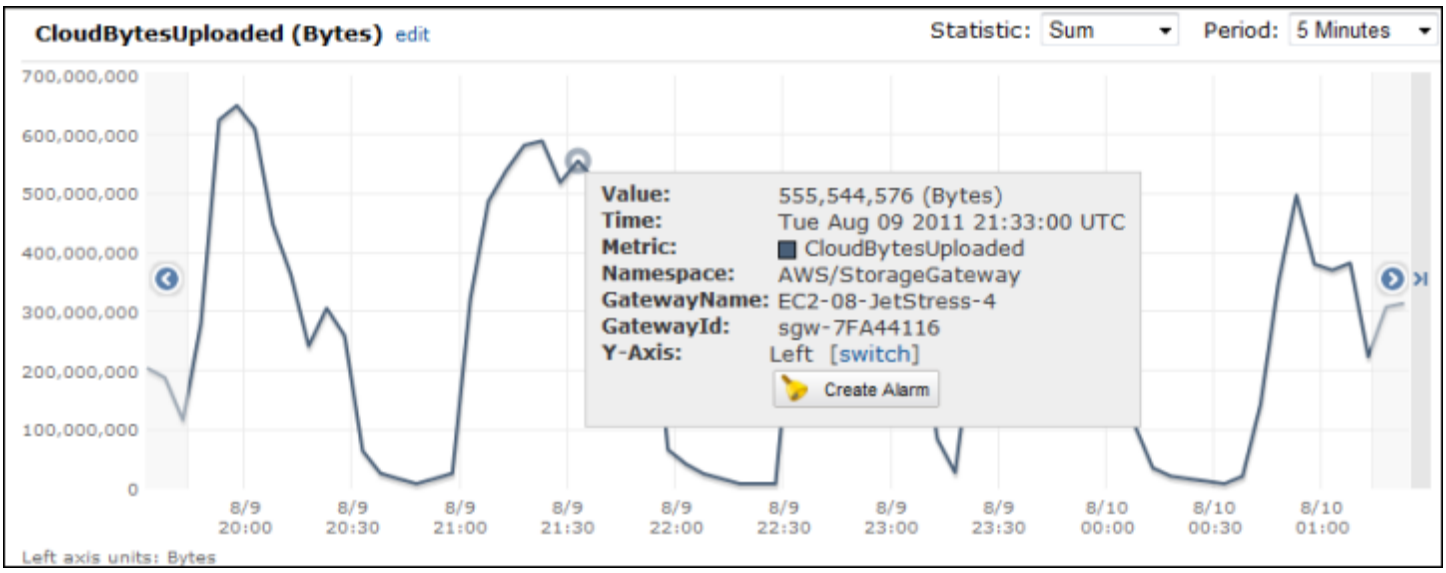
Interessierendes Element	Methode zum Messen
Latency	Verwenden Sie die Metriken `ReadTime` und `WriteTime` mit der Statistik `Average` CloudWatch . Beispiel: Der `Average`-Wert der `ReadTime`-Metrik gibt die Latenz pro Operation über den Stichprobenzeitraum an.
Durchsatz zu AWS	Verwenden Sie die `CloudBytesUploaded` Metriken `CloudBytesDownloaded` und mit der `Sum` - CloudWatch Statistik. Der `Sum` Wert der `CloudBytesDownloaded` Metrik über einen Stichprobenzeitraum von 5 Minuten geteilt durch 300 Sekunden gibt Ihnen beispielsweise den Durchsatz von AWS zum Tape Gateway als Rate in Byte pro Sekunde.
Latenz der Daten in AWS	Verwenden Sie die `CloudDownloadLatency` -Metrik mit der `Average`-Statistik. Beispiel: Die `Average`-Statistik der `CloudDownloadLatency` -Metrik gibt die Latenz pro Operation an.

So messen Sie den Upload-Datendurchsatz von einem Tape Gateway zu AWS

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Registerkarte Metriken.
3. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudBytesUploaded` aus.
5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die `Sum`-Statistik aus.
7. Wählen Sie für Zeitraum einen Wert von 5 Minuten oder mehr.

8. Dividieren Sie in der resultierenden zeitlich sortierten Gruppe von Datenpunkten jeden Datenpunkt durch den Zeitraum (in Sekunden), um den Durchsatz in diesem Stichprobenzeitraum zu erhalten.

In der folgenden Abbildung ist die Metrik `CloudBytesUploaded` für ein Gateway-Band mit der Statistik `Sum` dargestellt. In der Abbildung zeigt der Cursor beim Platzieren über einem Datenpunkt Informationen zu dem Datenpunkt wie den Wert und die Anzahl hochgeladener Bytes an. Dividieren Sie diesen Wert durch den Wert für Period (Zeitraum) (5 Minuten), um den Durchsatz an diesem Stichprobenpunkt zu erhalten. Für den hervorgehobenen Punkt AWS beträgt der Durchsatz vom Tape Gateway zu 555.544.576 Byte geteilt durch 300 Sekunden, was 1,7 Megabyte pro Sekunde entspricht.



So messen Sie die Datenlatenz von einem Tape Gateway zu AWS

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Registerkarte Metriken.
3. Wählen Sie die Dimension StorageGateway: GatewayMetrics und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudDownloadLatency` aus.
5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die `Average`-Statistik aus.
7. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

Die resultierende zeitlich sortierte Gruppe von Datenpunkten enthält die Latenz in Millisekunden.

So legen Sie einen oberen Schwellenwert für den Durchsatz eines Tape Gateways auf fest AWS

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Alarm erstellen, um den Assistenten zum Erstellen von Alarmen zu starten.
3. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudBytesUploaded` aus.
5. Definieren Sie den Alarm durch Festlegen des Alarmstatus, wenn die `CloudBytesUploaded`-Metrik für eine bestimmte Zeit größer als oder gleich einem angegebenen Wert ist. Sie können beispielsweise einen Alarmstatus festlegen, wenn die `CloudBytesUploaded`-Metrik für 60 Minuten größer als 10 MB ist.
6. Konfigurieren Sie die auszuführenden Aktionen für den Alarmstatus. Sie können beispielsweise eine E-Mail-Benachrichtigung an sich selbst senden lassen.
7. Wählen Sie Alarm erstellen.

So legen Sie einen oberen Schwellenwert für das Lesen von Daten aus fest AWS

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Alarm erstellen, um den Assistenten zum Erstellen von Alarmen zu starten.
3. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudDownloadLatency` aus.
5. Definieren Sie den Alarm durch Festlegen des Alarmstatus, wenn die `CloudDownloadLatency`-Metrik für eine bestimmte Zeit größer als oder gleich einem angegebenen Wert ist. Sie können beispielsweise einen Alarmstatus definieren, wenn `CloudDownloadLatency` für mehr als 2 Stunden größer als 60.000 Millisekunden ist.
6. Konfigurieren Sie die auszuführenden Aktionen für den Alarmstatus. Sie können beispielsweise eine E-Mail-Benachrichtigung an sich selbst senden lassen.
7. Wählen Sie Alarm erstellen.

Warten eines Gateways

Zu den Aufgaben im Rahmen der Gateway-Wartung zählen die Konfiguration von Cache-Speicher und Upload-Puffer-Speicher sowie allgemeine Wartungsaufgaben im Hinblick auf die Gateway-Leistung. Diese Aufgaben sind für alle Gateway-Typen gleich. Falls Sie noch kein Gateway erstellt haben, lesen Sie Erstellen eines Gateways.

Themen

Herunterfahren der Gateway-VM

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

> **Important**
>
> Wenn Sie ein Amazon-EC2-Gateway, das flüchtigen Speicher verwendet, anhalten und starten, ist das Gateway dauerhaft offline. Dies geschieht, weil der physische Speicherdatenträger ersetzt wird. Dieses Problem lässt sich nicht umgehen. Die einzige Lösung besteht darin, das Gateway zu löschen und ein neues Gateway auf einer neuen EC2-Instance zu aktivieren.

> **Note**
>
> Wenn Sie Ihr Gateway anhalten, während Ihre Sicherungssoftware auf einem Band liest oder schreibt, kann der Lese- oder Schreibvorgang fehlschlagen. Bevor Sie Ihr Gateway anhalten, sollten Sie Ihre Sicherungssoftware und den Sicherungszeitplan auf laufende Aufgaben prüfen.

- Lokale Gateway-VM-Konsole: siehe Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen.
- Storage Gateway-API – siehe ShutdownGateway

Für das File Gateway fahren Sie einfach Ihre VM herunter. Sie beenden das Gateway nicht.

Starten und Anhalten von Tape Gateway

So beenden Sie ein Tape Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und wählen Sie dann das anzuhaltende Gateway. Der Status des Gateways ist Wird ausgeführt.
3. Wählen Sie für Actions (Aktionen) die Option Stop gateway (Gateway anhalten) aus und überprüfen Sie die ID des Gateways im Dialogfeld. Wählen Sie dann Stop gateway (Gateway anhalten) aus.

   Während das Gateway angehalten wird, sehen Sie möglicherweise eine Meldung mit dem Status des Gateways. Wenn das Gateway ausgeschaltet wird, werden eine Meldung und die Schaltfläche Start gateway (Gateway starten) auf der Registerkarte Details angezeigt.

Wenn Sie Ihr Gateway anhalten, kann nicht auf die Speicherressourcen zugegriffen werden, bis Sie den Speicher starten. Wenn das Gateway zum Zeitpunkt des Anhaltens Daten hochlud, wird der Upload fortgesetzt, nachdem Sie das Gateway gestartet haben.

So starten Sie ein Tape Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und wählen Sie dann das zu startende Gateway. Der Status des Gateways ist Shutdown (Herunterfahren).
3. Wählen Sie Details und dann Start gateway (Gateway starten).

Verwaltung von lokalen Festplatten für Ihr Storage Gateway

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

Themen

Bestimmen der Größe des lokalen Festplattenspeichers

Sie müssen die Anzahl und Größe von Festplatten bestimmen, die Sie Ihrem Gateway zuweisen möchten. Abhängig von der bereitgestellten Speicherlösung (siehe Planen Ihrer Storage-Gateway-Bereitstellung) erfordert das Gateway folgenden zusätzlichen Speicher:

- Tape Gateways benötigen mindestens zwei Festplatten. Ein für die Verwendung als Cache, und eine als Upload-Puffer.

In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt. Nach dem Einrichten des Gateways können Sie entsprechend der steigenden Auslastung weiteren lokalen Speicher zuweisen.

Lokaler Speicher	Beschreibung
Upload-Puffer	Der Upload-Puffer stellt einen Staging-Bereich für die Daten bereit, bevor das Gateway die Daten an Amazon S3 hochlädt. Ihr Gateway lädt diese Pufferdaten über eine verschlüsselte Secure Sockets Layer (SSL)-Verbindung an AWS hoch.
Cache-Speicher	Der Cache-Speicher fungiert als dauerhafter On-Premises-Speicher für Daten mit ausstehen dem Upload an Amazon S3 aus dem Upload-Puffer. Wenn Ihre Anwendung einen E/A-Vorgang auf einem Volume oder Band ausführt, speichert das Gateway die Daten im Cache-Speicher, um einen Zugriff mit geringer Latenz zu ermöglich en. Wenn die Anwendung Daten von einem Volume oder Band anfordert, überprüft das Gateway zunächst den Cache-Speicher auf Daten, bevor die Daten von AWS heruntergeladen werden.

Note

Bei der Bereitstellung von Festplatten wird dringend empfohlen, keine lokalen Festplatten für den Upload-Puffer und Cache-Speicher bereitzustellen, die die gleiche physische Speicherressource (d. h. die gleiche Festplatte) verwenden. Zugrunde liegende physische Speicherressourcen werden als Datenspeicher in VMware dargestellt. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-

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

Nach der ersten Konfiguration und Bereitstellung Ihres Gateways können Sie den lokalen Speicher anpassen, indem Sie Festplatten für einen Upload-Puffer hinzufügen oder entfernen. Sie können auch Datenträger für den Cache-Speicher hinzufügen.

Optimieren der Gateway-Leistung

Um eine optimale Leistung zu erzielen, verwenden Sie SSD-Festplatten mit hohem Durchsatz sowohl als Cache als auch als Upload-Puffer.

- Verwenden Sie unterschiedliche Festplatten für Cache und Upload-Puffer. Wenn Sie RAID verwenden, stellen Sie sicher, dass Cache- und Upload-Puffer-Festplatten separate RAID-Controller auf Hardwareebene verwenden.
- Fügen Sie mindestens 2 verschiedene Upload-Puffer-Festplatten hinzu.
- Verwenden Sie die Striped-RAID-Konfiguration RAID 0 für Cache- und Upload-Puffergeräte, um den Durchsatz zu verbessern. Dies ist besonders wichtig für die Cache-Festplatte.

Bestimmen der Größe des zuzuordnenden Upload-Puffers

Sie können die Größe Ihres zuzuordnenden Upload-Puffers festlegen, indem Sie eine Upload-Pufferformel verwenden. Es wird dringend empfohlen, dem Upload-Puffer mindestens 150 GiB zuzuweisen. Wenn die Formel einen Wert von weniger als 150 GiB zurückgibt, verwenden Sie 150 GiB als dem Upload-Puffer zuzuweisende Kapazität. Sie können bis zu 2 TiB Upload-Pufferkapazität für jedes Gateway konfigurieren.

> **Note**
>
> Im Fall von Tape Gateways können die Anwendungen, wenn der Upload-Puffer seine Kapazität erreicht hat, weiter Daten aus Ihren Speicher-Volumes lesen und in diese Volumes schreiben. Das Tape Gateway schreibt jedoch keine Ihrer Volume-Daten in seinen Upload-Puffer und lädt keine dieser Daten in hoch, AWS bis Storage Gateway die lokal gespeicherten Daten mit der Kopie der in gespeicherten Daten synchronisiert AWS. Diese Synchronisation erfolgt, wenn die Volumes sich im Status BOOTSTRAPPING befinden.

Zur Schätzung der Menge des zuzuordnenden Upload-Puffers können Sie die erwarteten eingehenden und ausgehenden Datenraten bestimmen und in der folgenden Formel verwenden.

Rate der eingehenden Daten

Diese Rate bezieht sich auf den Anwendungsdurchsatz, die Rate, zu der die lokalen Anwendungen Daten in einem bestimmten Zeitraum an das Gateway schreiben.

Rate der ausgehenden Daten

Diese Rate bezieht sich auf die Netzwerkdurchsatz, die Rate, mit der das Gateway Daten an AWS hochladen kann. Diese Rate hängt von Ihrer Netzwerkgeschwindigkeit und der Auslastung sowie davon ab, ob Sie die Bandbreitendrosselung aktiviert haben. Diese Rate sollte unter Berücksichtigung der Komprimierung angepasst werden. Beim Hochladen von Daten in wendet AWS das Gateway nach Möglichkeit Datenkomprimierung an. Wenn die Anwendungsdaten nur aus Text bestehen, können Sie eine effektive Komprimierungsrate von etwa 2:1 erhalten. Wenn Sie jedoch Videos schreiben, kann das Gateway möglicherweise gar keine Datenkomprimierung erzielen und benötigt mehr Upload-Puffer für das Gateway.

Es wird dringend empfohlen, dass Sie mindestens 150 GiB Upload-Pufferspeicher zuweisen, wenn einer der folgenden Punkte zutrifft:

- Ihre eingehende Rate ist höher als die ausgehende Rate.
- Die Formel gibt einen Wert kleiner als 150 GiB zurück.

$$\left(\text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor}\right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

Beispiel: Ihre Geschäftsanwendungen schreiben Textdaten mit einer Rate von 40 MB pro Sekunde während 12 Stunden täglich an das Gateway und der Netzwerkdurchsatz beträgt 12 MB pro Sekunde. Bei einem Komprimierungsfaktor von 2:1 für die Textdaten müssten Sie etwa 690 GiB Speicherplatz für den Upload-Puffer zuweisen.

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

Sie können diese Schätzung auch anfangs zur Bestimmung der Festplattengröße verwenden, die Sie dem Gateway als Upload-Pufferspeicherplatz zuweisen. Mithilfe der Storage-Gateway-Konsole können Sie nach Bedarf weiteren Upload-Pufferspeicherplatz hinzufügen. Außerdem können Sie die CloudWatch Betriebsmetriken von Amazon verwenden, um die Nutzung des Upload-Puffers zu überwachen und zusätzliche Speicheranforderungen zu ermitteln. Weitere Informationen zu Metriken und dem Festlegen von Alarmen finden Sie unter Überwachen des Upload-Puffers.

Bestimmen der Größe des zuzuordnenden Cache-Speichers

Ihr Gateway nutzt seinen Cache-Speicher, um Zugriff mit niedriger Latenz auf Daten bereitzustellen, auf die kürzlich zugegriffen wurde. Der Cache-Speicher fungiert als dauerhafter On-Premises-Speicher für Daten mit ausstehendem Upload an Amazon S3 aus dem Upload-Puffer. Normalerweise sollte die Größe des Cache-Speicher das 1,1-fache der Upload-Puffergröße betragen. Weitere Informationen dazu, wie Sie Ihre Cache-Speichergröße abschätzen können, finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.

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

Konfigurieren zusätzlichen Upload-Puffers oder Cache-Speichers

Wenn sich Ihre Anwendungsanforderungen ändern, können sie die Upload-Puffer- oder Cache-Speicherkapazität für das Gateway 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 oder Upload-Puffer hinzufügen, müssen Sie neue Festplatten auf dem Gateway-Host-Hypervisor oder in der Amazon-EC2-Instance erstellen. Entfernen Sie keine Festplatten oder ändern Sie nicht die Größe vorhandener Festplatten, die bereits als Cache- oder Upload-Puffer zugewiesen wurden.

So konfigurieren Sie zusätzlichen Upload-Puffer oder Cache-Speicher für Ihr Gateway

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 diesen Datenträger als Upload-Puffer oder Cache-Speicher.
2. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
3. Wählen Sie im Navigationsbereich Gateways aus.
4. Suchen Sie nach Ihrem Gateway und wählen Sie es aus der Liste aus.
5. Wählen Sie im Menü Aktionen die Option Testereignis konfigurieren aus.
6. Identifizieren Sie im Abschnitt 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 jedes Laufwerk aus dem Dropdown-Menü Zugewiesen für entweder UPLOAD-PUFFER oder CACHE-SPEICHER aus.
7. Wählen Sie Änderungen speichern aus, um die Konfigurationseinstellungen zu speichern.

Verwaltung der Bandbreite für Ihr Tape Gateway

Sie können den Upload-Durchsatz vom Gateway zu AWS oder den Download-Durchsatz von AWS zu Ihrem Gateway begrenzen (oder drosseln). Mit der Bandbreitendrosselung können Sie steuern, wie viel Netzwerkbandbreite ein Gateway nutzt. Standardmäßig gibt es bei einem aktivierten Gateway keine Beschränkung für Upload oder Download.

Sie können das Ratenlimit entweder über die AWS Management Console oder programmgesteuert über die Storage Gateway-API (siehe UpdateBandwidthRateLimit) oder ein AWS Software Development Kit (SDK) angeben. Durch die programmgesteuerte Drosselung der Bandbreite können Sie die Limits im Laufe des Tages automatisch ändern, z. B. durch die Planung von Aufgaben zum Ändern der Bandbreite.

Sie können auch eine zeitplanbasierte Bandbreitendrosselung für Ihr Gateway definieren. Sie planen die Bandbreitendrosselung, indem Sie ein oder mehrere bandwidth-rate-limit Intervalle definieren. Weitere Informationen finden Sie unter Zeitplanbasierte Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole.

Die Konfiguration einer einzelnen Einstellung für die Bandbreitendrosselung ist das funktionale Äquivalent der Definition eines Zeitplans mit einem einzigen bandwidth-rate-limit Intervall, das für Everyday festgelegt ist, mit einer Startzeit von `00:00` und einer Endzeit von `23:59`.

> **Note**
>
> Die Informationen in diesem Abschnitt beziehen sich speziell auf Tape und Volume Gateways. Informationen zur Verwaltung der Bandbreite für ein Amazon S3 File Gateway finden Sie unter Verwalten von Bandbreite für Ihr Amazon S3 File Gateway. Bandbreitenlimits werden derzeit für Amazon FSx File Gateway nicht unterstützt.

Themen

- Ändern der Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole
- Zeitplanbasierte Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole
- Aktualisieren von Gateway-Bandbreitenratenlimits mithilfe der AWS SDK for Java
- Aktualisieren von Gateway-Bandbreitenratenlimits mithilfe der AWS SDK for .NET
- Aktualisieren von Gateway-Bandbreitenratenlimits mithilfe der AWS Tools for Windows PowerShell

Ändern der Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole

Das folgende Verfahren veranschaulicht, wie Sie die Drosselung der Bandbreite eines Gateways mit der Storage-Gateway-Konsole ändern.

So ändern Sie die Bandbreitendrosselung eines Gateways mithilfe der Konsole

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im linken Navigationsbereich erst Gateways und anschließend das Gateway aus, das Sie verwalten möchten.
3. Wählen Sie für Aktionen die Option Bandbreitenraten-Limit bearbeiten aus.
4. Geben Sie im Dialogfeld Ratenlimits bearbeiten neue Grenzwerte ein und wählen Sie anschließend Speichern. Ihre Änderungen werden auf der Registerkarte Details für das Gateway angezeigt.

Zeitplanbasierte Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole

Im folgenden Abschnitt erfahren Sie, wie Sie die Drosselung der Bandbreite eines Gateways mit der Storage-Gateway-Konsole ändern.

So können Sie einen Zeitplan für die Gateway-Bandbreitendrosselung hinzufügen oder ändern

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

   Der bandwidth-rate-limit Zeitplan des Gateways wird im Dialogfeld Zeitplan für Bandbreitenratenlimit bearbeiten angezeigt. Standardmäßig ist ein neuer Gateway- bandwidth-rate-limit Zeitplan leer.
4. Wählen Sie im Dialogfeld Zeitplan für Bandbreitenratenlimit bearbeiten die Option Neues Element hinzufügen aus, um ein neues bandwidth-rate-limit Intervall hinzuzufügen. Geben Sie die folgenden Informationen für jedes bandwidth-rate-limit Intervall ein:

   - Wochentage – Sie können das bandwidth-rate-limit Intervall für Wochentage (Montag bis Freitag), für Wochenenden (Samstag und Sonntag), für jeden Wochentag oder für einen oder mehrere bestimmte Wochentage erstellen.

- Startzeit: Geben Sie die Startzeit für das Bandbreitenintervall in der lokalen Zeitzone des Gateways im Format HH:MM ein.

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

- Endzeit – Geben Sie die Endzeit für das bandwidth-rate-limit Intervall in der lokalen Zeitzone des Gateways im Format HH:MM ein.

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

- Download-Geschwindigkeit: Geben Sie die Download-Geschwindigkeitsbegrenzung in Kilobit pro Sekunde (Kbit/s) ein, oder wählen Sie Keine Begrenzung aus, um die Bandbreitendrosselung für Downloads zu deaktivieren. Der Mindestwert für die Downloadrate beträgt 100 Kbit/s.
- Uploadrate: Geben Sie das Upload-Ratenlimit in Kbit/s ein oder wählen Sie Kein Limit aus, um die Bandbreitendrosselung für Uploads zu deaktivieren. Der Mindestwert für die Upload-Rate beträgt 50 Kbit/s.

Um Ihre bandwidth-rate-limit Intervalle zu ändern, können Sie überarbeitete Werte für die Intervallparameter eingeben.

Um Ihre bandwidth-rate-limit Intervalle zu entfernen, können Sie rechts neben dem zu löschenden Intervall Entfernen auswählen.

Wenn Sie Ihre Änderungen abgeschlossen haben, wählen Sie Speichern aus.

5. Fahren Sie mit dem Hinzufügen von bandwidth-rate-limit Intervallen fort, indem Sie Neues Element hinzufügen auswählen und den Tag, die Start- und Endzeiten sowie die Download- und Upload-Ratenlimits eingeben.

> **Important**
>
> B-andwidth-rate-limit Intervalle dürfen sich nicht überschneiden. Die Startzeit eines Intervalls muss nach der Endzeit eines vorherigen Intervalls und vor der Startzeit eines nachfolgenden Intervalls liegen.

6. Nachdem Sie alle bandwidth-rate-limit Intervalle eingegeben haben, wählen Sie Änderungen speichern, um Ihren bandwidth-rate-limit Zeitplan zu speichern.

Wenn der bandwidth-rate-limit Zeitplan erfolgreich aktualisiert wurde, können Sie die aktuellen Download- und Upload-Ratenlimits im Bereich Details für das Gateway sehen.

Aktualisieren von Gateway-Bandbreitenratenlimits mithilfe der AWS SDK for Java

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

Example : Aktualisieren der Gateway-Bandbreitenratenlimits mithilfe der AWS SDK for Java

Mit dem folgenden Java-Codebeispiel werden die Bandbreitenlimits eines Gateways aktualisiert. Um diesen Beispielcode zu verwenden, müssen Sie den Code aktualisieren und den Service-Endpunkt, den Amazon-Ressourcennamen (ARN) des Gateways sowie die Upload- und Download-Limits angeben. Eine Liste der AWS Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente im Allgemeine AWS-Referenz.

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;
```

```
public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

    // Rates
    static long uploadRate = 51200;  // Bits per second, minimum 51200
    static long downloadRate = 102400;   // Bits per second, minimum 102400

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

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

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

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
 sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
 returnGatewayARN);
            System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
 second");
```

```
            System.out.println("Download bandwidth limit = " + downloadRate + " bits
 per second");
        }
        catch (AmazonClientException ex)
        {
            System.err.println("Error updating gateway bandwith.\n" + ex.toString());
        }
    }
}
```

Aktualisieren von Gateway-Bandbreitenratenlimits mithilfe der AWS SDK for .NET

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

Example : Aktualisieren der Gateway-Bandbreitenratenlimits mithilfe der AWS SDK for .NET

Mit dem folgenden C#-Codebeispiel werden die Bandbreitenlimits eines Gateways aktualisiert. Um diesen Beispielcode zu verwenden, müssen Sie den Code aktualisieren und den Service-Endpunkt, den Amazon-Ressourcennamen (ARN) des Gateways sowie die Upload- und Download-Limits angeben. Eine Liste der AWS Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente im Allgemeine AWS-Referenz.

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

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

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

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

        // Rates
        static long uploadRate = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
```

```
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

Aktualisieren von Gateway-Bandbreitenratenlimits mithilfe der AWS Tools for Windows PowerShell

Durch die programmgesteuerte Aktualisierung von Bandbreitenlimits können Sie die Limits automatisch über einen bestimmten Zeitraum hinweg anpassen, z. B. durch die Verwendung von geplanten Aufgaben. Im folgenden Beispiel wird gezeigt, wie Sie die Bandbreitenlimits eines Gateways mit AWS Tools for Windows PowerShell aktualisieren. Um den Beispielcode zu verwenden, sollten Sie mit der Ausführung eines PowerShell Skripts vertraut sein. Weitere Informationen finden Sie unter Erste Schritte im AWS Tools for Windows PowerShell - Benutzerhandbuch.

Example : Aktualisieren der Gateway-Bandbreitenratenlimits mithilfe der AWS Tools for Windows PowerShell

Im folgenden PowerShell Skriptbeispiel werden die Bandbreitenlimits eines Gateways aktualisiert. Um dieses Beispielskript zu verwenden, müssen Sie das Skript aktualisieren und den Amazon-Ressourcennamen (ARN) des Gateways sowie die Upload- und Download-Limits angeben.

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

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

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

$UploadBandwidthRate = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

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

Storage Gateway veröffentlicht in regelmäßigen Abständen wichtige Software-Updates für Ihr Gateway. Sie können Updates auch in der Storage-Gateway-Managementkonsole manuell anwenden. Es ist auch möglich, die Updates während der konfigurierten Wartungszeit automatisch anzuwenden. Storage Gateway überprüft jede Minute, ob Updates vorliegen, führt jedoch Wartung und Neustart nur durch, wenn Updates vorhanden sind.

Gateway-Softwareversionen enthalten regelmäßig Betriebssystemupdates und Sicherheitspatches, die von AWS validiert wurden. Diese Updates werden in der Regel alle sechs Monate veröffentlicht und als Teil des normalen Gateway-Aktualisierungsprozesses während der geplanten Wartungsfenster installiert.

> **Note**
>
> Sie sollten die Storage-Gateway-Appliance wie eine verwaltete virtuelle Maschine behandeln und nicht versuchen, auf ihre Installation zuzugreifen oder sie in irgendeiner Weise zu ändern. Der Versuch, Softwarepakete mit anderen Methoden als dem normalen Gateway-

Aktualisierungsmechanismus (z. B. SSM oder Hypervisor-Tools) zu installieren oder zu aktualisieren, kann zu Fehlfunktionen des Gateways führen.
Um die E-Mail-Adresse zu ändern, an die Software-Update-Benachrichtigungen gesendet werden, gehen Sie zur Seite Verwalten eines AWS Kontos und aktualisieren Sie den alternativen Kontakt für „Operationen“.

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

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

Important

Sie können das Risiko einer Unterbrechung Ihrer Anwendungen wegen des Gateway-Neustarts minimieren, indem Sie die Timeouts des iSCSI-Initiators erhöhen. Weitere Informationen zum Erhöhen der iSCSI-Initiator-Timeouts für Windows und Linux finden Sie unter Anpassen der Windows iSCSI-Einstellungen und Anpassen Ihrer Linux iSCSI-Einstellungen.

So ändern Sie den Wartungsplan

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsmenü erst Gateways und anschließend das Gateway, für das Sie den Aktualisierungszeitplan ändern möchten.
3. Wählen Sie im Menü Actions (Aktionen) die Option Edit maintenance window (Wartungsfenster bearbeiten) aus, um das Dialogfeld „Edit maintenance start time (Wartungsstartzeit bearbeiten)“ zu öffnen.

4. Wählen Sie für Schedule (Zeitplan) die Option Weekly (Wöchentlich) oder Monthly (Monatlich) aus, um Aktualisierungen zu planen.
5. Wenn Sie Weekly (Wöchentlich) auswählen, ändern Sie die Werte für Day of the week (Tag der Woche) und Time (Zeit).

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

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

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

Ausführen von Wartungsaufgaben in der lokalen Konsole

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

Ausführen von Aufgaben in der lokalen VM-Konsole von

Für ein lokal bereitgestelltes Gateway können Sie die folgenden Wartungsaufgaben mit der lokalen VM-Host-Konsole durchführen. Diese Aufgaben sind für VMware, Hyper-V und Linux Kernel-basierte virtuelle Maschine (KVM)-Hosts üblich.

Themen

- Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen
- Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole
- Weiterleiten Ihres lokalen Gateways über einen Proxy
- Konfigurieren Ihres Gateway-Netzwerks

- Testen der Gateway-Internetverbindung
- Synchronisieren der Gateway-VM-Zeit
- Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole
- Anzeigen des Gateway-Systemressourcen-Status
- Konfigurieren von Networkadaptern für Ihr Gateway

Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen

Sobald Sie sich an die VM anmelden können, wird der Anmeldebildschirm angezeigt. Wenn Sie sich zum ersten Mal bei der lokalen Konsole anmelden, melden Sie sich unter Verwendung der Standard-Anmeldeinformationen an. Mit diesen Standard-Anmeldeinformationen haben Sie Zugriff auf Menüs, in denen sie die Gateway-Netzwerkeinstellungen konfigurieren und das Passwort aus der lokalen Konsole ändern können. Mit Storage Gateway können Sie Ihr eigenes Passwort über die AWS Storage Gateway Konsole festlegen, anstatt das Passwort über die lokale Konsole zu ändern. Sie müssen das Standardpasswort nicht kennen, um ein neues Passwort einzustellen. Weitere Informationen finden Sie unter Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole.

So melden Sie sich an die lokale Konsole des Gateways an

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

   Verwenden Sie andernfalls Ihre Anmeldeinformationen.

   > **Note**
   >
   > Wir empfehlen, das 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 Ihr eigenes Passwort auch über die AWS Storage Gateway Konsole festlegen. Weitere Informationen finden Sie unter Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole.

> **Important**
>
> Bei älteren Versionen von Volume oder Tape Gateway lautet der Benutzername `sguser` und das Passwort `sgpassword`. Wenn Sie Ihr Passwort zurücksetzen und Ihr Gateway auf eine neuere Version aktualisiert wird, ändert sich der Benutzername in admin, das Passwort wird jedoch beibehalten.

2. Nach der Anmeldung wird das Hauptmenü AWS Storage Gateway – Konfiguration angezeigt, wo Sie verschiedene Aufgaben ausführen können.

Für weitere Informationen zu dieser Aufgabe	Siehe folgendes Thema
Konfigurieren eines SOCKS-Proxy für Ihr Gateway	Weiterleiten Ihres lokalen Gateways über einen Proxy.
Konfigurieren Ihres Netzwerks	Konfigurieren Ihres Gateway-Netzwerks.
Testen der Netzwerkverbindung	Testen der Gateway-Internetverbindung.
VM-Zeit verwalten	Synchronisieren der Gateway-VM-Zeit.
Ausführen von Storage-Gateway-Konsolenbefehlen	Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole.
Anzeigen einer Systemressourcenprüfung	Anzeigen des Gateway-Systemressourcen-Status.

Wenn Sie das Gateway beenden möchten, geben Sie **0** ein.

Zum Beenden der Konfigurationssitzung geben Sie **X** ein.

Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole

Wenn Sie sich zum ersten Mal bei der lokalen Konsole anmelden, melden Sie sich mit den Standard-Anmeldeinformationen (der Benutzername lautet `admin` und das Passwort lautet `password`) bei der VM an. Wir empfehlen, immer direkt ein neues Passwort festzulegen, wenn Sie ein neues

Gateway erstellt haben. Sie können dieses Passwort aus der AWS Storage Gateway -Konsole heraus festlegen, statt die lokale Konsole zu verwenden. Sie müssen das Standardpasswort nicht kennen, um ein neues Passwort einzustellen.

So legen Sie das Passwort für die lokale Konsole auf der Storage-Gateway-Konsole fest

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsfenster Gateways und anschließend das Gateway, für das Sie ein neues Passwort festlegen möchten.
3. Wählen Sie im Menü Actions (Aktionen) die Option Set Local Console Password (Passwort für lokale Konsole einrichten) aus.
4. Geben Sie im Dialogfeld Set Local Console Password (Passwort für lokale Konsole einrichten) ein neues Passwort ein, bestätigen Sie das Passwort, und wählen Sie anschließend Save (Speichern). Das neue Passwort ersetzt das Standard-Passwort. Storage Gateway speichert das Passwort nicht, sondern überträgt es sicher an die VM.

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

Weiterleiten Ihres lokalen Gateways über einen Proxy

Volume-Gateways und Tape-Gateways unterstützen die Konfiguration eines Socket Secure Version 5 (SOCKS5) Proxy zwischen dem lokalen Gateway und AWS.

> **Note**
>
> Die einzige unterstützte Proxy-Konfiguration ist SOCKS5.

Wenn das Gateway einen Proxy-Server für die Kommunikation mit dem Internet verwenden muss, müssen Sie die SOCKS-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 HTTPS-Datenverkehr über Ihren Proxy-Server weiter. Weitere

Informationen zu den Netzwerk-Anforderungen für Ihr Gateway finden Sie unter Netzwerk- und Firewall-Anforderungen.

Das folgende Verfahren zeigt, wie Sie einen SOCKS-Proxy für Volume Gateway und Tape Gateway konfigurieren.

So konfigurieren Sie einen SOCKS5-Proxy für Volume- und Tape-Gateways

1. Melden Sie sich bei der lokalen Konsole des Gateways an.
   - VMware ESXi: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - KVM: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Geben Sie im Hauptmenü AWS Storage Gateway – Konfiguration die entsprechende Zahl ein, um SOCKS-Proxy-Konfiguration auszuwählen.
3. Geben Sie im Menü AWS Storage Gateway – SOCKS-Proxy-Konfiguration die entsprechende Zahl ein, um eine der folgenden Aufgaben auszuführen:

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren eines SOCKS-Proxys	Geben Sie die entsprechende Zahl ein, um SOCKS-Proxy konfigurieren auszuwählen. Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
Anzeigen der aktuellen SOCKS-Proxy-Konfiguration	Geben Sie die entsprechende Zahl ein, um Aktuelle SOCKS-Proxykonfiguration anzeigen auszuwählen. Wenn kein SOCKS-Proxy konfiguriert ist, wird die Meldung `SOCKS Proxy not configured` angezeigt. Ist ein SOCKS-Proxy konfiguri

Zur Ausführung dieser Aufgabe	Vorgehensweise
	ert, werden der Hostname und Port des Proxys angezeigt.
Entfernen einer SOCKS-Proxy-Konfiguration	Geben Sie die entsprechende Zahl ein, um SOCKS-Proxykonfiguration entfernen auszuwählen. Die Meldung `SOCKS Proxy Configuration Removed` wird angezeigt.

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

Konfigurieren Ihres Gateway-Netzwerks

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.

   - VMware ESXi: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - KVM: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.

2. Geben Sie im Hauptmenü AWS Storage Gateway – Konfiguration die entsprechende Zahl ein, um Netzwerkkonfiguration auszuwählen.
3. Führen Sie im Menü Netzwerkkonfiguration AWS von Storage Gateway eine der folgenden Aufgaben aus:

Zur Ausführung dieser Aufgabe	Vorgehensweise
Beschreiben des Netzwerkadapters	Geben Sie die entsprechende Zahl ein, um Adapter beschreiben auszuwählen. Eine Liste der Adapternamen wird angezeigt, und Sie werden aufgefordert, einen Adaptername n 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-aktivierter Status Sie verwenden die hier aufgeführten Adapternamen, wenn Sie eine statische IP-Adresse konfigurieren oder den Standardadapter Ihres Gateways festlegen.
Konfigurieren von DHCP	Geben Sie die entsprechende Zahl ein, um DHCP konfigurieren auszuwählen. Sie werden aufgefordert, die Netzwerkschnittstelle für die Verwendung von DHCP zu konfigurieren.

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 Herunterfahren der Gateway-VM.

Zur Ausführung dieser Aufgabe	Vorgehensweise
	Wenn Ihr Gateway mehrere Netzwerkschnittstellen verwendet, müssen Sie alle aktivierten Schnittstellen für die Verwendung von DHCP- oder statischen IP-Adressen einrichten. Angenommen, Ihre Gateway-VM verwendet als DHCP konfigurierte Schnittstellen. Wenn Sie später eine Schnittstelle für eine statische IP einrichten, wird die andere Schnittstelle deaktiviert. Um die Schnittstelle in diesem Fall zu 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. **Note** Wenn Sie einen statischen Hostnamen für Ihr Gateway konfigurieren, müssen Sie in Ihrem DNS-System einen A-Eintrag erstellen, in dem die IP-Adresse des Gateways auf den statischen Hostnamen verweist.

Zur Ausführung dieser Aufgabe	Vorgehensweise
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 Herunterfahren der Gateway-VM.
Einrichten des Standard-Routing-Adapters Ihres Gateways	Geben Sie die entsprechende Zahl ein, um Standardadapter festlegen auszuwählen. Die Adapter, die für Ihr Gateway verfügbar sind, werden angezeigt, und Sie werden aufgefordert, einen der Adapter auszuwählen, z. B. **`eth0`**.
Anzeigen der DNS-Konfiguration Ihres Gateways	Geben Sie die entsprechende Zahl ein, um DNS-Konfiguration anzeigen auszuwählen. Die IP-Adressen des primären und sekundären DNS-Namenservers werden angezeigt.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Anzeigen von Routing-Tabellen	Geben Sie die entsprechende Zahl ein, um Routen anzeigen auszuwählen. Die Standard-Route Ihres Gateways wird angezeigt.

Testen der Gateway-Internetverbindung

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

So testen Sie die Gateway-Internetverbindung

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

   - VMware ESXi: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - KVM: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Geben Sie im Hauptmenü AWS Storage Gateway – 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 und angeben, AWS-Region wie in den folgenden Schritten beschrieben.
3. Wenn Ihr Gateway noch nicht aktiviert ist, geben Sie die entsprechende Zahl ein, um den Endpunkttyp für Ihr Gateway auszuwählen.
4. Wenn Sie den öffentlichen Endpunkttyp ausgewählt haben, geben Sie die entsprechende Zahl ein, um die auszuwählen AWS-Region , die Sie testen möchten. Unterstützte AWS-Regionen und eine Liste der AWS Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter -AWS Storage Gateway Endpunkte und -Kontingente im 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	Beschreibung
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über Netzwerkkonnektivität.
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway hat keine Netzwerkkonnektivität.

Synchronisieren der Gateway-VM-Zeit

Nachdem Sie Ihr Gateway bereitgestellt und aktiviert haben, kann die Gateway-VM-Zeit in manchen Fällen abweichen. Wenn zum Beispiel ein längerer Netzwerkausfall auftritt und die Zeit Ihres Hypervisor-Netzwerk und Ihres Gateways nicht aktualisiert wird, weicht die Zeit der VM von der tatsächlichen Zeit ab. Bei einer Abweichung besteht eine Diskrepanz den angegebenen Zeiten von Vorgängen wie Snapshots und den tatsächlichen Zeiten, zu denen die Vorgänge ausgeführt wurden.

Bei einem Gateway, das auf einem VMware ESXi bereitgestellt wird, reicht es aus, die Hypervisor-Host-Zeit einzustellen und die VM-Zeit mit dem Host zu synchronisieren, um eine Abweichung zu verhindern. Weitere Informationen finden Sie unter Synchronisieren der VM-Zeit mit der Host-Zeit.

Bei einem Gateway, das auf Microsoft Hyper-V bereitgestellt wird, sollten Sie die Zeit Ihrer VM in regelmäßigen Abständen überprüfen. Weitere Informationen finden Sie unter Synchronisieren der Gateway-VM-Zeit.

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. Mit den lokalen Konsolenbefehlen können Sie Wartungsaufgaben wie das Speichern von Routing-Tabellen, das AWS Support Herstellen einer Verbindung mit usw. ausführen.

So führen Sie eine Konfiguration oder einen Diagnosebefehl aus

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

- Weitere Informationen zum Anmelden bei der lokalen VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
- Weitere Informationen 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 Konfigurieren Ihres Gateway-Netzwerks.

Befehl	Funktion
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 Konfigurieren Ihres Gateway-Netzwerks.
iptables	Verwaltungstool 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	Stellen Sie eine Verbindung zum - AWS Support her.
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.

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.

Wenn Sie weitere Informationen zu einem Befehl erhalten möchten, geben Sie in der Befehlszeile **man** und *Name des Befehls* ein.

Anzeigen des Gateway-Systemressourcen-Status

Beim Starten überprüft Ihr Gateway seine virtuellen CPU-Kerne, Stamm-Volume-Größe und RAM. Er kann dann bestimmen, ob ausreichend Systemressourcen für die ordnungsgemäße Funktionsweise Ihres Gateways verfügbar sind. Sie können die Ergebnisse dieser Prüfung auf der lokalen Gateway-Konsole anzeigen.

So zeigen Sie den Status einer Systemressourcenprüfung an

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

   - Weitere Informationen zum Anmelden bei der VMware ESXi-Konsole finden Sie unter Zugreifen auf die lokale Konsole mit VMware ESXi.
   - Weitere Informationen 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	Beschreibung
[OK]	Die Ressource hat die Systemressourcenprüfung bestanden.
[WARNING] ([WARNUNG])	Die Ressource erfüllt nicht die empfohlenen Anforderungen, aber das Gateway ist weiterhin funktionsfähig. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.

Fehlermeldung	Beschreibung
[FAIL] ([FEHLGESCHLAGEN])	Die Ressource erfüllt nicht die Mindestan forderungen. Das Gateways funktioniert möglicherweise nicht ordnungsgemäß. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressource nprüfung an.

Die Konsole zeigt die Anzahl der Fehler und Warnungen neben der Menüoption für die Ressourcenprüfung an.

Konfigurieren von Networkadaptern für Ihr Gateway

Standardmäßig ist Storage Gateway für die Verwendung eines Netzwerkadapters des Typs E1000 konfiguriert, aber Sie können Ihr Gateway auch für die Verwendung eines Netzwerkadapters des Typs VMXNET3 (10 GbE) konfigurieren. Sie können Storage Gateway auch so konfigurieren, dass mehrere IP-Adressen darauf zugreifen können. Konfigurieren Sie hierzu Ihr Gateway für die Verwendung mehrerer Netzwerkadapter.

Themen

- Konfigurieren Ihres Gateways für die Verwendung eines VMXNET3-Netzwerkadapters
- Konfigurieren Ihres Gateways für mehrere NICs

Konfigurieren Ihres Gateways für die Verwendung eines VMXNET3-Netzwerkadapters

Storage Gateway unterstützt den E1000-Netzwerkadaptertyp in VMware ESXi- und Microsoft Hyper-V Hypervisor-Hosts. Allerdings werden VMXNET3-Netzwerkadapter (10 GbE) nur von VMware ESXi-Hypervisor unterstützt. In einem VMware ESXi-Hypervisor gehostete Gateways können jetzt so konfiguriert werden, dass sie den Adaptertyp VMXNET3 (10 GbE) verwenden. Weitere Informationen zu diesem Adapter finden Sie auf der VMware-Website.

> **Important**
>
> Um VMXNET3 zu wählen, muss Ihr Gast-Betriebssystem Other Linux64 (Andere Linux64) sein.

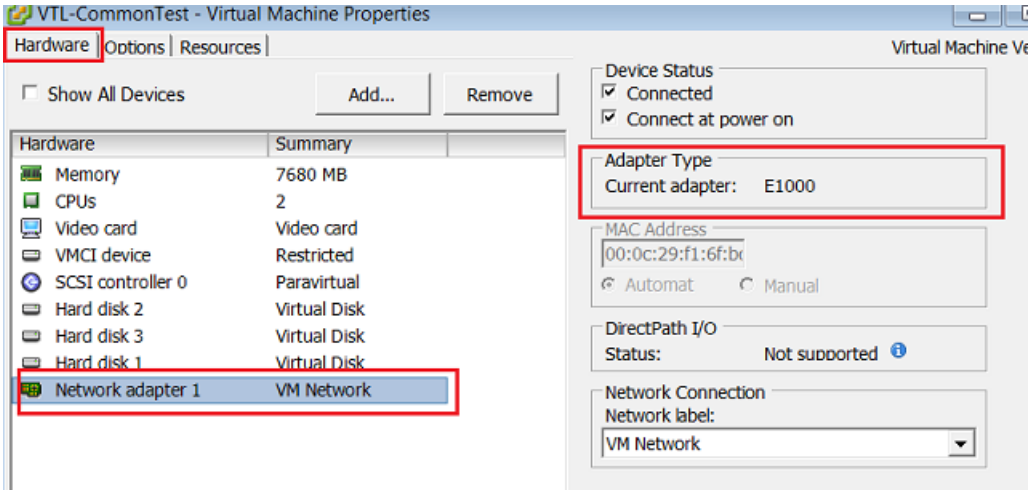
In den folgenden Abschnitten werden die Schritte beschrieben, mit denen Sie Ihr Gateway für die Verwendung eines VMXNET3-Adapter konfigurieren:

1. Entfernen Sie die Standard-E1000 Adapter.
2. Fügen Sie den VMXNET3-Adapter hinzu.
3. Starten Sie Ihr Gateway neu.
4. Konfigurieren Sie den Adapter für das Netzwerk.

Nähere Informationen über die Ausführung der einzelnen Schritte finden Sie im Folgenden.

So entfernen Sie einen Standard-E1000-Adapter und konfigurieren Ihr Gateway für die Verwendung eines VMXNET3-Adapters

1. Öffnen Sie in VMware das Kontextmenü (Klick mit der rechten Maustaste) für Ihr Gateway und wählen Sie Edit Settings (Einstellungen bearbeiten).
2. Wählen Sie im Fenster Virtual Machine Properties (Eigenschaften der virtuellen Maschine) die Registerkarte Hardware.
3. Wählen Sie für Hardware die Option Network Adapter (Netzwerkadapter). Beachten Sie, dass der aktuelle Adapter im Abschnitt Adapter Type (Adaptertyp) ein E1000 ist. Ersetzen Sie diesen Adapter mit dem VMXNET3-Adapter.



4. Wählen Sie den E1000-Netzwerkadapter und wählen Sie Remove (Entfernen). In diesem Beispiel ist der E1000-Netzwerkadapter Network Adapter 1 (Netzwerkadapter 1).

> **Note**
>
> Obwohl Sie den E1000- und den VMXNET3-Netzwerkadapter in Ihrem Gateway gleichzeitig ausführen können, wird dies nicht empfohlen, da es zu Netzwerkproblemen kommen kann.

5. Wählen Sie zum Öffnen des Assistenten zum Hinzufügen von Hardware die Option Add (Hinzufügen).
6. Wählen Sie Ethernet Adapter (Ethernet-Adapter) und anschließend Next (Weiter).
7. Wählen Sie im Netzwerktyp-Assistenten **VMXNET3** für Adapter Type (Adaptertyp) aus und wählen Sie anschließend Next (Weiter).
8. Prüfen Sie im Assistenten für die Eigenschaften der virtuellen Maschine im Abschnitt Adapter Type (Adaptertyp), ob Current Adapter (Aktueller Adapter) auf VMXNET3 eingestellt ist, und wählen Sie anschließend OK.
9. Deaktivieren Sie Ihr Gateway im VMware VSphere-Client.
10. Starten Sie Ihr Gateway im VMware VSphere-Client neu.

Konfigurieren Sie nach dem Neustart Ihres Gateways den Adapter neu, den Sie gerade hinzugefügt haben, um sicherzustellen, dass die Netzwerkverbindung mit dem Internet hergestellt wird.

So konfigurieren Sie den Adapter für das Netzwerk

1. Wählen Sie im VSphere-Client die Registerkarte Console (Konsole), um die lokale Konsole zu starten. Verwenden Sie die Standard-Anmeldeinformationen für die Anmeldung bei der lokalen Konsole des Gateways für diese Konfigurationsaufgabe. Informationen zur Anmeldung mit den Standardanmeldedaten finden Sie unter Anmelden bei der lokalen Konsole mit Standardanmeldedaten.
2. Geben Sie an der Eingabeaufforderung die entsprechende Zahl ein, um Netzwerkkonfiguration auszuwählen.
3. Geben Sie an der Eingabeaufforderung die entsprechende Zahl ein, um Alle auf DHCP zurücksetzen auszuwählen. Geben Sie dann an der Eingabeaufforderung **y** (für „Ja“) ein, um alle Adapter auf die Verwendung von DHCP (Dynamic Host Configuration Protocol) festzulegen. Alle verfügbaren Adapter werden für die Verwendung von DHCP eingestellt.

Wenn Ihr Gateway bereits aktiviert ist, müssen Sie es über die Managementkonsole des Storage Gateway beenden und neu starten. Nach dem Neustart des Gateways müssen Sie die Netzwerkverbindung mit dem Internet testen. Informationen zum Testen der Netzwerkkonnektivität finden Sie unter Testen der Internet-Verbindung Ihres Gateways.

Konfigurieren Ihres Gateways für mehrere NICs

Wenn Sie Ihr Gateway für mehrere Netzwerkadapter (NICs) konfigurieren, können mehrere IP-Adressen auf Ihr Gateway zugreifen. Dies kann in den folgenden Situationen wünschenswert sein:

- Maximieren des Durchsatzes – Wenn Netzwerkadapter einen Engpass darstellen, möchten Sie Ihren Durchsatz durch ein Gateway möglicherweise erhöhen.
- 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.
- Netzwerk-Einschränkungen – Ihre Anwendungsumgebung erfordert möglicherweise, dass Sie Ihre iSCSI-Ziele und die Initiatoren, die mit diesen verbunden sind, in einem isolierten Netzwerk halten, das sich von dem Netzwerk unterscheidet, über das das Gateway mit AWS kommuniziert.

In einem typischen Anwendungsfall mit mehreren Adaptern ist ein Adapter als Route konfiguriert, über die das Gateway mit kommuniziert AWS (d. h. als Standard-Gateway). Abgesehen von diesem einen Adapter müssen sich die Initiatoren im selben Subnetz wie der Adapter befinden, der die iSCSI-Ziele enthält, zu denen eine Verbindung aufgebaut wird. Andernfalls ist die Kommunikation mit den vorgesehenen Zielen vielleicht nicht möglich. Wenn ein Ziel auf demselben Adapter konfiguriert ist, der für die Kommunikation mit verwendet wird AWS, fließt der iSCSI-Datenverkehr für dieses Ziel und der AWS Datenverkehr durch denselben Adapter.

Wenn Sie einen Adapter so konfigurieren, das er eine Verbindung mit der Storage-Gateway-Konsole herstellt, und wenn Sie dann einen zweiten Adapter hinzufügen, konfiguriert das Storage Gateway die Routing-Tabelle automatisch so, dass der zweite Adapter als bevorzugte Route verwendet wird. Anleitungen zur Konfiguration von Mehrfachadaptern finden Sie in den folgenden Abschnitten.

- Konfigurieren des Gateways für mehrere NICs in einem VMware-ESXi-Host
- Konfigurieren des Gateways für mehrere NICs in einem Microsoft-Hyper-V-Host

Ausführen von Aufgaben in der lokalen Amazon-EC2-Konsole

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.

Themen

Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways

Sie können über einen Secure Shell (SSH)-Client eine Verbindung mit der Amazon-EC2-Instance herstellen. Detaillierte Informationen finden Sie unter Verbinden mit der Instance im Amazon-EC2-Benutzerhandbuch. Für diese Art des Verbindungsaufbaus benötigen Sie das SSH-Schlüsselpaar, das Sie beim Starten der Instance angegeben haben. Weitere Informationen über Amazon-EC2-Schlüsselpaare finden Sie unter Amazon-EC2-Schlüsselpaare im Amazon- EC2- Benutzerhandbuch.

So melden Sie sich bei der lokalen Konsole des Gateways an

1. Melden Sie sich bei der lokalen Konsole an. Wenn Sie auf einem Windows-Computer eine Verbindung zu Ihrer EC2-Instance herstellen, melden Sie sich als admin an.
2. Nach der Anmeldung wird das Hauptmenü AWS Storage Gateway – Konfiguration angezeigt, wo Sie verschiedene Aufgaben ausführen können.

Für weitere Informationen zu dieser Aufgabe	Siehe folgendes Thema
Konfigurieren eines SOCKS-Proxy für Ihr Gateway	Weiterleitung des auf EC2 bereitgestellten Gateways über einen HTTP-Proxy
Testen der Netzwerkverbindung	Testen der Netzwerkkonnektivität Ihres Gateways

Für weitere Informationen zu dieser Aufgabe	Siehe folgendes Thema
Ausführen von Storage-Gateway-Konsolenbefehlen	Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole
Anzeigen einer Systemressourcenprüfung	Anzeigen des Gateway-Systemressourcen-Status.

Wenn Sie das Gateway beenden möchten, geben Sie **0** ein.

Zum Beenden der Konfigurationssitzung geben Sie **X** ein.

Weiterleitung des auf 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 Proxy-Server 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. Anweisungen finden Sie unter Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
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. Anweisungen finden Sie unter Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
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 und angeben, AWS-Region wie in den folgenden Schritten beschrieben.
3. Wenn Ihr Gateway noch nicht aktiviert ist, geben Sie die entsprechende Zahl ein, um den Endpunkttyp für Ihr Gateway auszuwählen.
4. Wenn Sie den öffentlichen Endpunkttyp ausgewählt haben, geben Sie die entsprechende Zahl ein, um die auszuwählen AWS-Region , die Sie testen möchten. Unterstützte AWS-Regionen und eine Liste der AWS Service-Endpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter -AWS Storage Gateway Endpunkte und -Kontingente im 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	Beschreibung
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über Netzwerkkonnektivität.

Fehlermeldung	Beschreibung
[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. Anweisungen finden Sie unter Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
2. Geben Sie im Hauptmenü AWS -Geräteaktivierung – 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	Beschreibung
[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	Beschreibung
	Beschreibung der Ergebnisse der Ressource nprüfung an.

Die Konsole zeigt die Anzahl der Fehler und Warnungen neben der Menüoption für die Ressourcenprüfung an.

Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole

Die AWS Storage Gateway Konsole bietet eine sichere Umgebung für die Konfiguration und Diagnose von Problemen mit Ihrem Gateway. Mit den Konsolenbefehlen können Sie Wartungsaufgaben wie das Speichern von Routing-Tabellen oder das Herstellen einer Verbindung mit durchführen AWS Support.

So führen Sie eine Konfiguration oder einen Diagnosebefehl aus

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Anweisungen finden Sie unter Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
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 konfiguri eren.

Befehl	Funktion
	Note Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren.
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.
iptables	Verwaltungstool 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	Stellen Sie eine Verbindung zum - AWS Support her.
save-iptables	IP-Tabellen speichern.
save-routing-table	Speichern Sie den neu hinzugefügten Eintrag in der Routingtabelle.

Befehl	Funktion
sslcheck	Überprüfen Sie die SSL-Gültigkeit zur Fehlerbehebung im Netzwerk.
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 den Befehlsnamen gefolgt von der Option `-h` ein, beispielsweise: `sslcheck -h`.

Zugreifen auf die lokale Konsole des Gateways

Auf welche Weise Sie auf die lokale Konsole der VM zugreifen, ist davon abhängig, auf welcher Art von Hypervisor Sie Ihre Gateway-VM bereitgestellt haben. In diesem Abschnitt finden Sie Informationen zum Zugriff auf die lokale VM-Konsole mit Linux Kernel-basierter virtueller Maschine (KVM), VMware ESXi und Microsoft Hyper-V Manager.

Themen

- Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
- Zugreifen auf die lokale 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

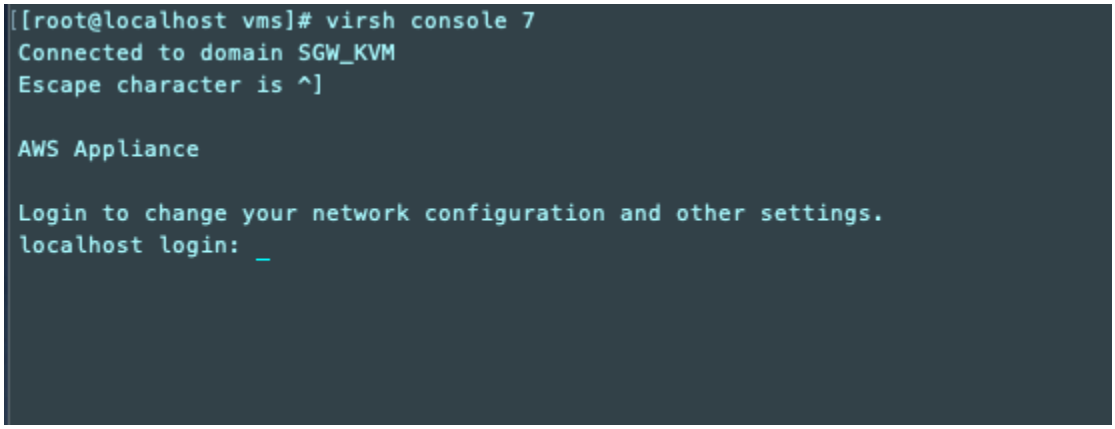
1. Verwenden Sie den folgenden Befehl, um die VMs aufzulisten, die derzeit in KVM verfügbar sind.

```
# virsh list
```

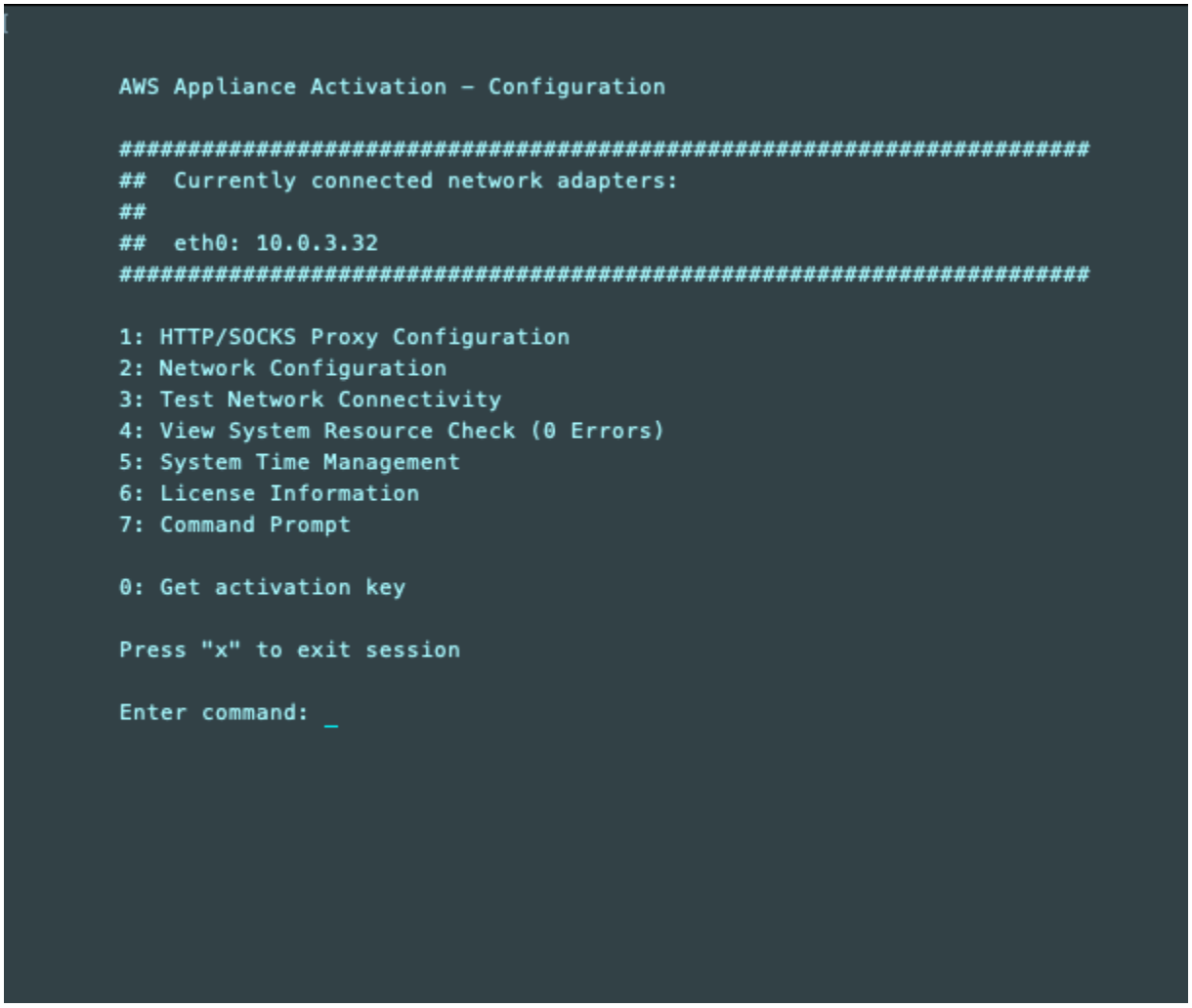
Sie können verfügbare VMs nach `Id` auswählen.

2. Verwenden Sie den folgenden Befehl, um auf die lokale Konsole zuzugreifen.

```
# virsh console VM_Id
```



3. Standardanmeldeinformationen für die Anmeldung bei der lokalen Konsole finden Sie unter Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen.
4. Nachdem Sie sich angemeldet haben, können Sie Ihr Gateway aktivieren und konfigurieren.

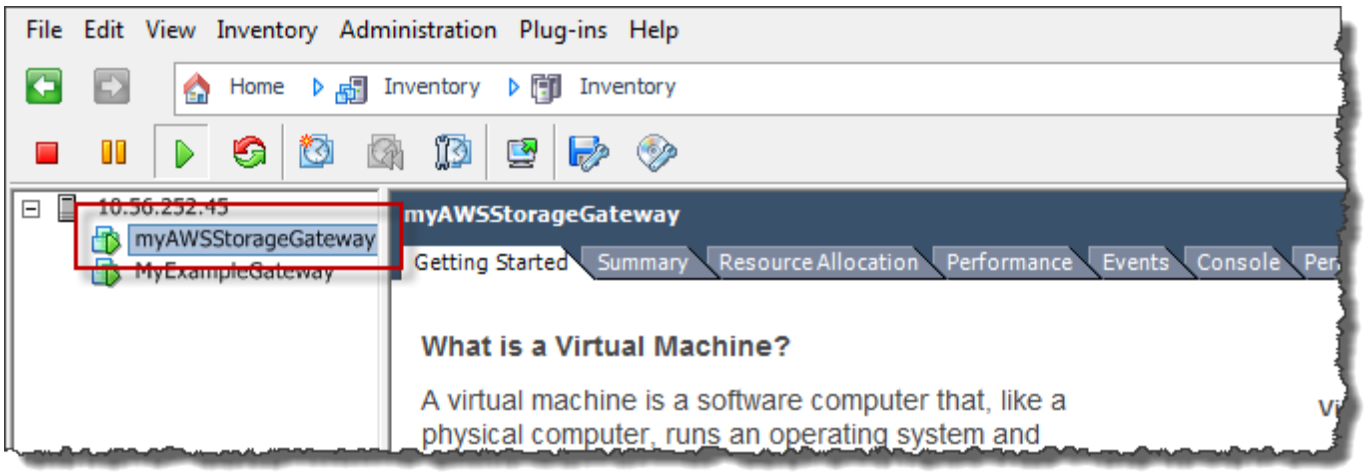


Zugreifen auf die lokale Konsole mit VMware ESXi

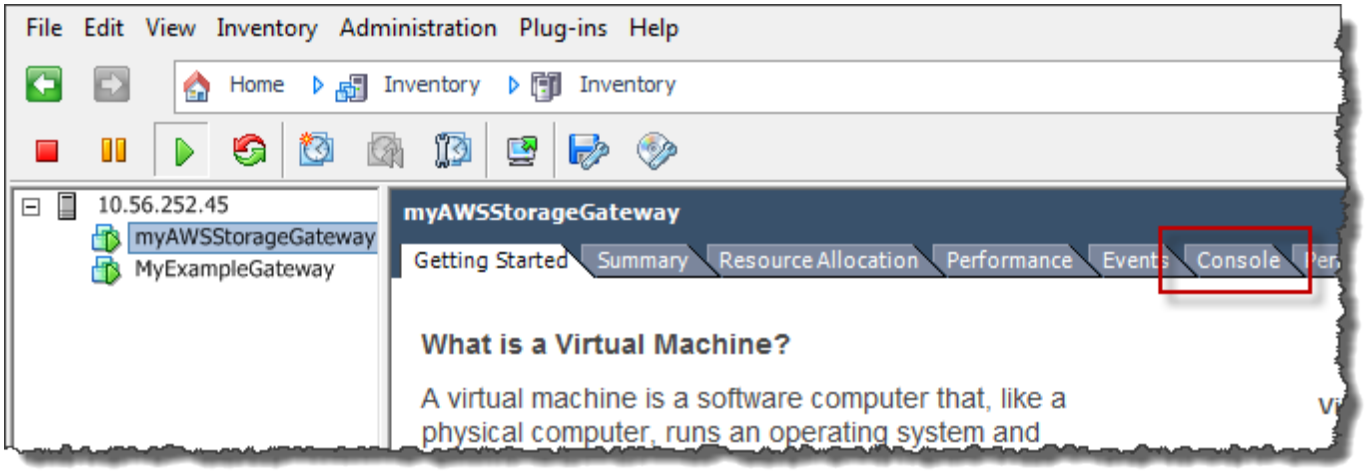
So greifen Sie mithilfe von VMware ESXi auf die lokale Konsole des Gateways zu

1. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM.
2. Stellen Sie sicher, dass das Gateway aktiviert ist.

> **Note**
>
> Wenn Ihre Gateway-VM aktiviert ist, erscheint wie im folgenden Screenshot dargestellt ein grünes Pfeilsymbol mit dem VM-Symbol. Wenn Ihre Gateway-VM nicht aktiviert ist, wählen Sie das Symbol Power On (Energie ein) im Menü Toolbar (Symbolleiste), um sie zu aktivieren.

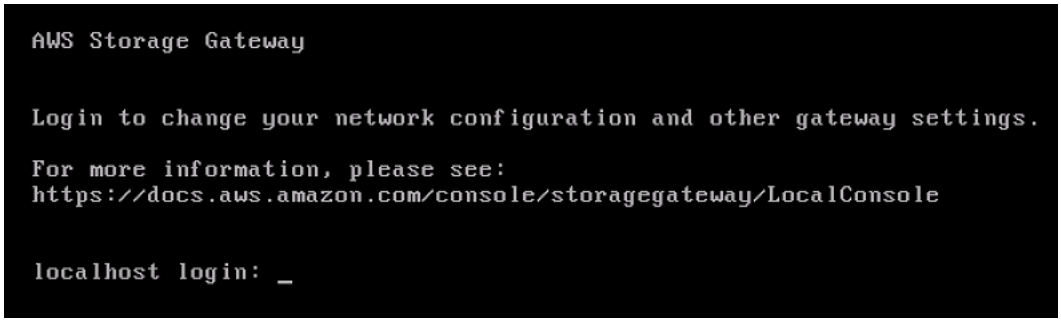


3. Wählen Sie die Registerkarte Console (Konsole).



Nach einem kurzen Augenblick können Sie sich an die VM anmelden.

> **Note**
>
> Drücken Sie Ctrl+Alt (Strg+Alt), um den Mauszeiger aus dem Konsolenfenster freizugeben.



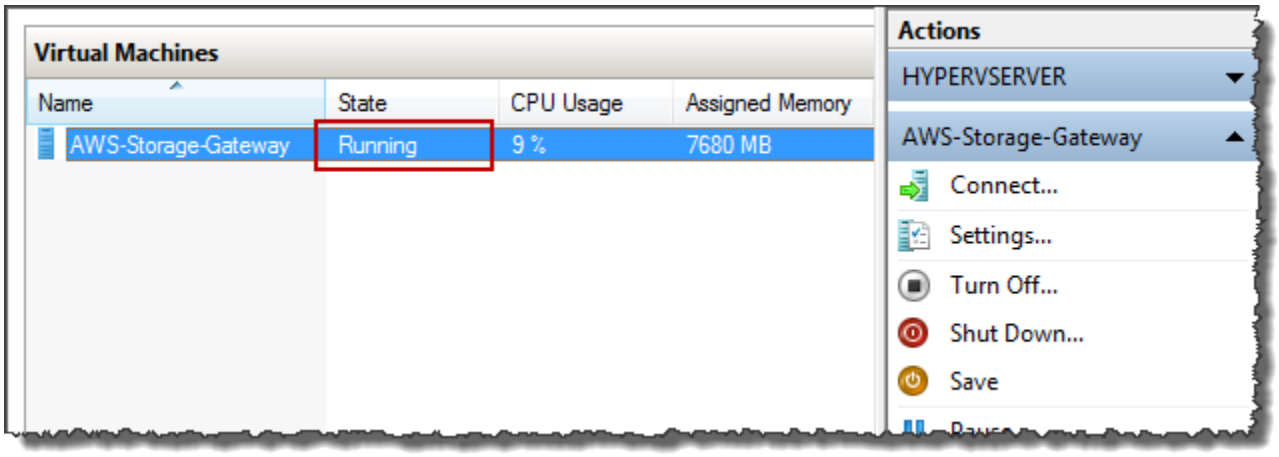
4. Um sich mit den Standard-Anmeldeinformationen anzumelden, fahren Sie mit dem Verfahren Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen fort.

Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V

Zugreifen auf die lokale Gateway-Konsole (Microsoft Hyper-V)

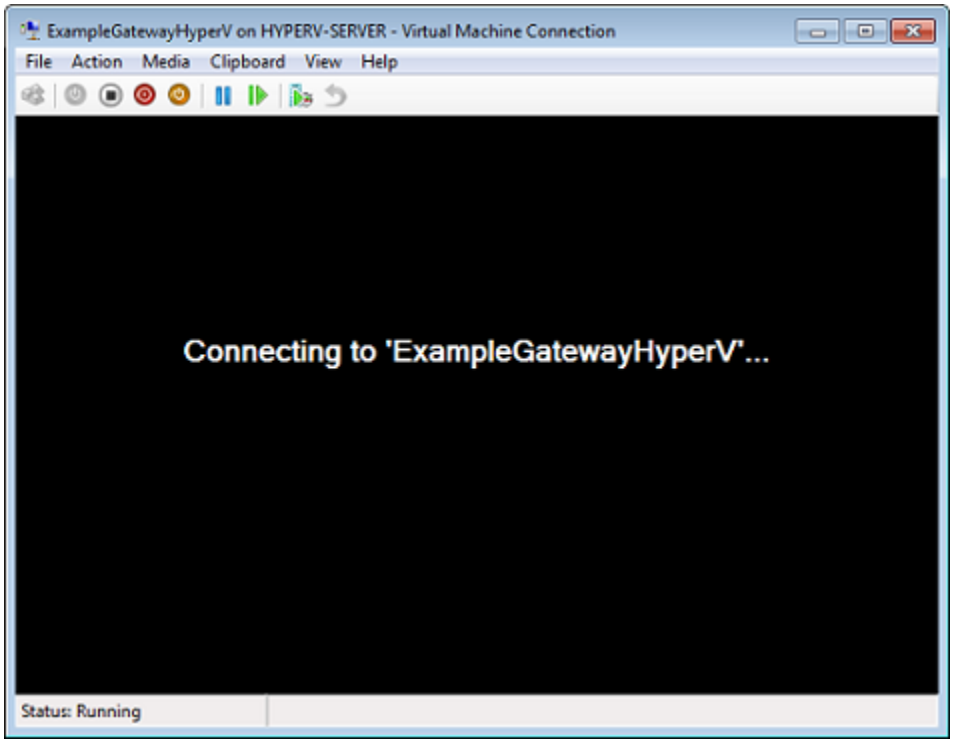
1. Wählen Sie in der Liste Virtual Machines (Virtuelle Maschinen) im Microsoft Hyper-V Manager Ihre Gateway-VM aus.
2. Stellen Sie sicher, dass das Gateway aktiviert ist.

> **Note**
>
> Wenn Ihre Gateway-VM aktiviert ist, wird `Running` als State (Status) der VM angezeigt, wie im folgenden Screenshot dargestellt. Wenn Ihre Gateway-VM nicht aktiviert ist, wählen Sie Start im Fenster Actions (Aktionen), um sie zu aktivieren.

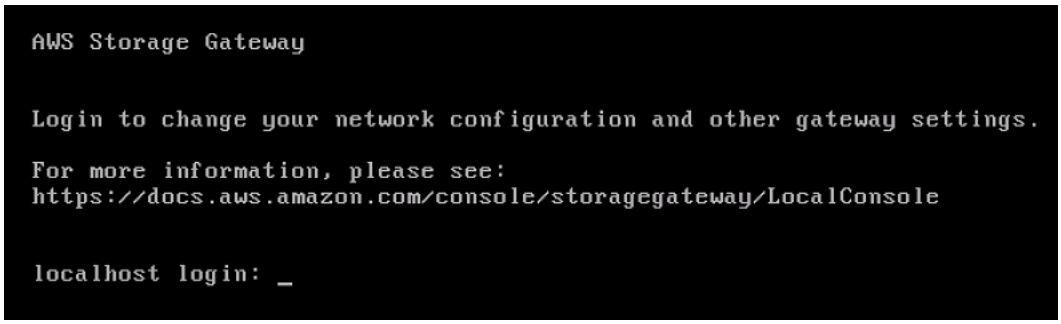


3. Wählen Sie im Fenster Actions (Aktionen) die Option Connect (Verbinden).

   Das Fenster Virtual Machine Connection (Verbindung der virtuellen Maschine) wird angezeigt. Wenn ein Authentifizierungsfenster angezeigt wird, geben Sie die Anmeldeinformationen ein, die Sie vom Hypervisor-Administrator erhalten haben.



   Nach einem kurzen Augenblick können Sie sich an die VM anmelden.



4. Um sich mit den Standard-Anmeldeinformationen anzumelden, fahren Sie mit dem Verfahren Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen fort.

Konfigurieren von Networkadaptern für Ihr Gateway

In diesem Abschnitt finden Sie Informationen zum Konfigurieren von mehreren Netzwerkadaptern für Ihr Gateway.

Themen

Konfigurieren des Gateways für mehrere NICs in einem VMware-ESXi-Host

Das folgende Verfahren setzt voraus, dass für Ihre Gateway-VM bereits ein Netzwerkadapter definiert wurde und beschreibt, wie Sie einen Adapter unter VMware ESXi hinzufügen.

So konfigurieren Sie das Gateway für einen zusätzlichen Netzwerkadapter im VMware-ESXi-Host

1. Fahren Sie das Gateway herunter.
2. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM.

   Die VM kann für die Dauer dieses Verfahrens aktiviert bleiben.
3. Öffnen Sie im Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM, und wählen Sie Edit Settings (Einstellungen bearbeiten).
4. Wählen Sie auf der Registerkarte Hardware im Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) die Option Add (Hinzufügen), um ein Gerät hinzuzufügen.
5. Befolgen Sie die Anweisungen des Hardware-Assistenten zum Hinzufügen eines Netzwerkadapters.

   a. Wählen Sie im Fenster Device Type (Gerätetyp) die Option Ethernet Adapter, um einen Adapter hinzuzufügen, und wählen Sie dann Next (Weiter).

   b. Stellen Sie sicher, dass im Fenster Network Type (Netzwerktyp) die Option Connect at power on (Verbindung bei Einschalten der Energie herstellen) für Type (Typ) ausgewählt ist, und wählen Sie dann Next (Weiter).

      Wir empfehlen, dass Sie den VMXNET3-Netzwerkadapter mit Storage Gateway verwenden. Weitere Informationen zu den Adaptertypen, die ggf. in der Adapter-Liste aufgeführt

werden, finden Sie unter den Netzwerkadapter-Typen in der ESXi und vCenter Server-Dokumentation.

c. Prüfen Sie im Fenster Ready to Complete (Bereit zum Abschließen) die Informationen und wählen Sie Finish (Fertigstellen).

6. Wählen Sie die Registerkarte 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.

Weitere Informationen zu Aufgaben für die lokale Konsole, die für VMware-, Hyper-V- und KVM-Hosts typisch sind, finden Sie unter Ausführen von Aufgaben in der lokalen VM-Konsole von .

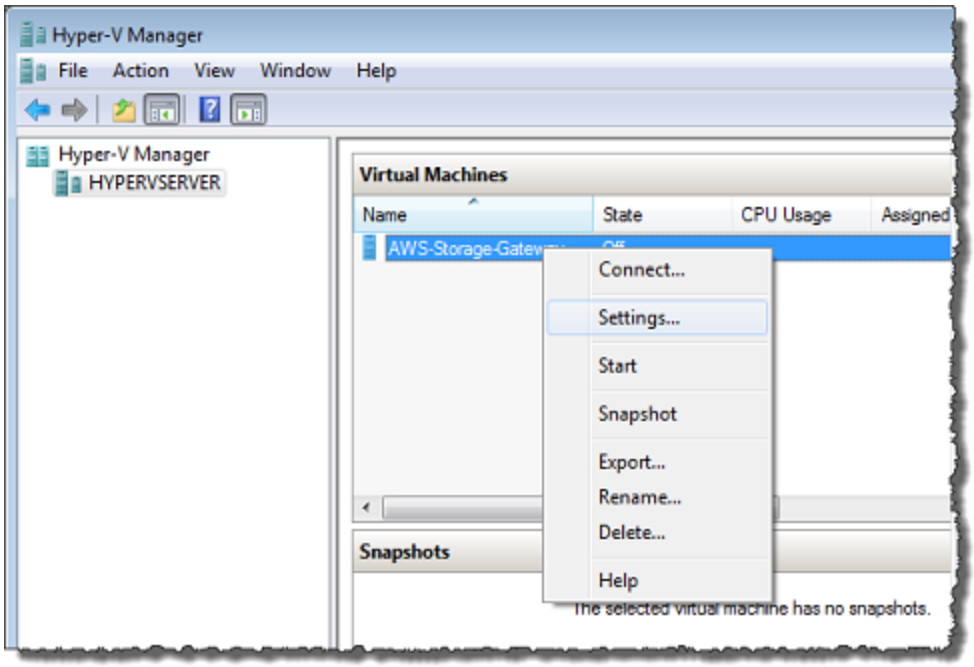
Konfigurieren des Gateways für mehrere NICs in einem Microsoft-Hyper-V-Host

Im folgenden Verfahren wird davon ausgegangen, dass für Ihre Gateway-VM bereits ein Netzwerkadapter definiert wurde und Sie einen zweiten Adapter hinzufügen. In diesem Verfahren wird zeigt, wie Sie einen Adapter für einen Microsoft Hyper-V-Host hinzufügen.

So konfigurieren Sie Ihr Gateway für einen zusätzlichen Netzwerkadapter in einem Microsoft Hyper-V-Host

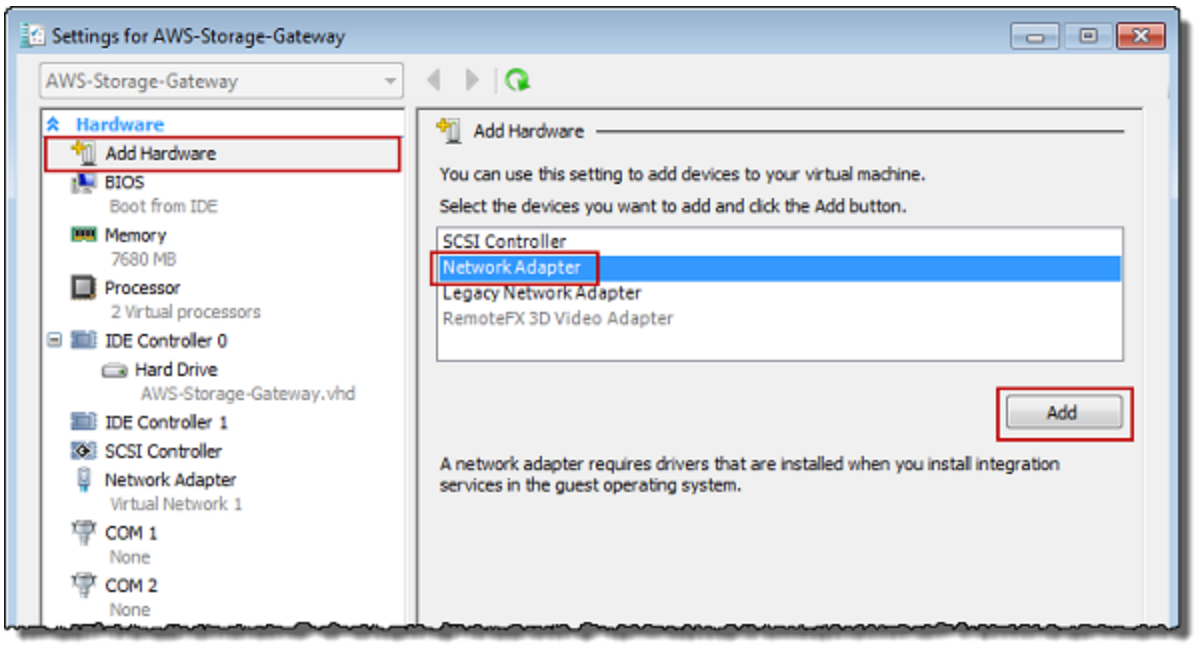
1. Schalten Sie in der Storage-Gateway-Konsole das Gateway aus. Anweisungen finden Sie unter So beenden Sie ein Tape Gateway.
2. Wählen Sie im Microsoft Hyper-V ManagerIhre Gateway-VM.
3. Wenn die VM nicht bereits deaktiviert ist, öffnen Sie das Kontextmenü (rechte Maustaste) für Ihr Gateway und wählen Sie Turn Off (Deaktivieren).

4. Öffnen Sie im Client das Kontextmenü für Ihre Gateway-VM und wählen Sie Settings (Einstellungen).



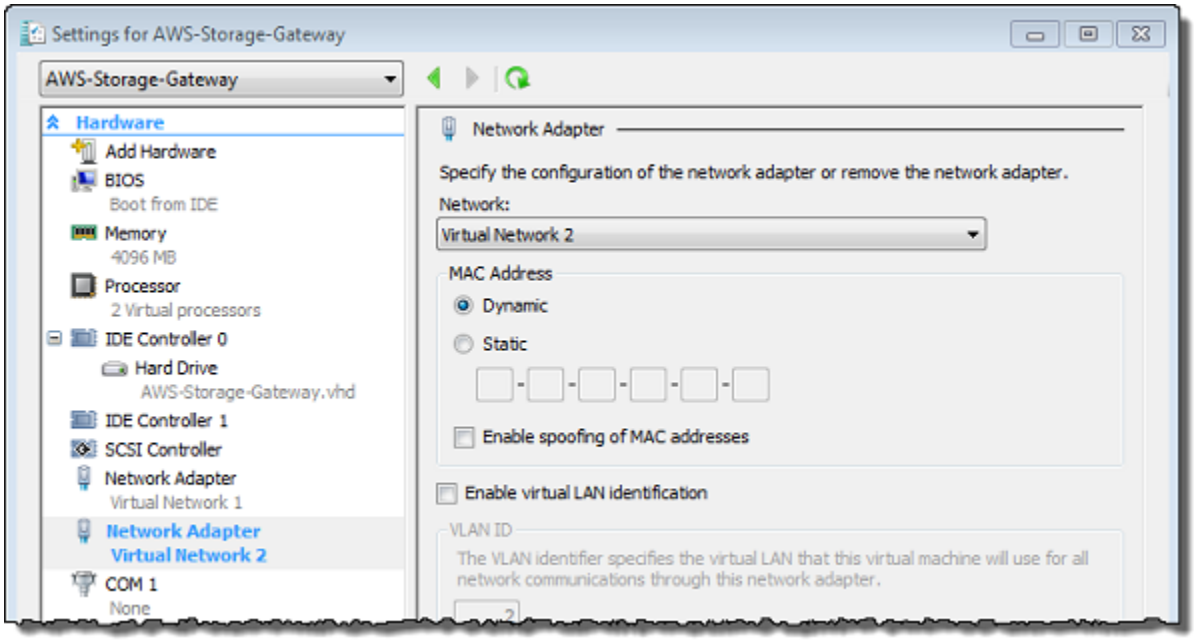
5. Wählen Sie im Dialogfeld Settings (Einstellungen) der VM für Hardware die Option Add Hardware (Hardware hinzufügen).

6. Wählen Sie im Fenster Add Hardware (Hardware hinzufügen) die Option Network Adapter (Netzwerkadapter) und anschließend Add (Hinzufügen), um ein Gerät hinzuzufügen.



7. Konfigurieren Sie den Netzwerkadapter, und wählen Sie dann Apply (Anwenden), um die Einstellungen anzuwenden.

   Im folgenden Beispiel wird Virtual Network 2 (Virtuelles Netzwerk 2) für den neuen Adapter gewählt.



8. Vergewissern Sie sich, dass im Dialogfeld Settings (Einstellungen) für Hardware der zweite Adapter hinzugefügt wurde, und wählen Sie dann OK.
9. Schalten Sie in der Storage-Gateway-Konsole das Gateway ein. Anweisungen finden Sie unter So starten Sie ein Tape Gateway.
10. Wählen Sie im Fenster Navigation die Option Gateways und anschließend das Gateway, dem Sie den Adapter hinzugefügt haben. Vergewissern Sie sich, dass die zweite IP-Adresse in der Registerkarte Details aufgeführt wird.

> **Note**
>
> Die Beispiel-Mountingbefehle auf der Informationsseite für eine Dateifreigabe in der Storage-Gateway-Konsole enthalten immer die IP-Adresse des Netzwerkadapters, der zuletzt zum zugehörigen Gateway der Dateifreigabe hinzugefügt wurde.

Weitere Informationen zu Aufgaben für die lokale Konsole, die für VMware-, Hyper-V- und KVM-Hosts typisch sind, finden Sie unter Ausführen von Aufgaben in der lokalen VM-Konsole von .

Löschen des Gateways über die AWS Storage Gateway -Konsole und Bereinigen zugehöriger Ressourcen

Wenn Sie ein Gateway nicht weiter verwenden möchten, können Sie dieses zusammen mit den zugehörigen Ressourcen löschen. Durch das Entfernen von Ressourcen wird verhindert, dass Gebühren für Ressourcen entstehen, die Sie voraussichtlich nicht weiter verwenden werden, und Ihre monatliche Rechnung wird gesenkt.

Wenn Sie ein Gateway löschen, wird es nicht mehr in der - AWS Storage Gateway Managementkonsole angezeigt und seine iSCSI-Verbindung zum Initiator wird geschlossen. Die Schritte zum Löschen eines Gateways sind für alle Gateway-Typen gleich. Abhängig von dem Typ des Gateways, das Sie löschen möchten, und dem Host, auf dem es bereitgestellt ist, führen Sie jedoch spezifische Anweisungen zum Entfernen zugehöriger Ressourcen aus.

> **Note**
>
> Wenn Sie ein Tape Gateway löschen, werden alle Bänder, die sich derzeit im `AVAILABLE` Status befinden, ebenfalls gelöscht, und alle Daten auf diesen Bändern gehen verloren. Wenn Sie Daten von Bändern behalten möchten, die von einem Gateway verwendet werden, das Sie löschen möchten, müssen Sie die Bänder archivieren, bevor Sie das Gateway löschen. Weitere Informationen finden Sie unter Archivierung virtueller Bänder.

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..

Themen

- Löschen eines Gateways mithilfe der Storage-Gateway-Konsole
- Entfernen von Ressourcen von einem lokal bereitgestellten Gateway
- Entfernen von Ressourcen von einem auf einer Amazon-EC2-Instance bereitgestellten Gateway

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 ist, müssen

Sie jedoch möglicherweise zusätzliche Aufgaben zum Entfernen von dem Gateway zugeordneten Ressourcen ausführen. Durch das Entfernen dieser Ressourcen wird verhindert, dass Sie für Ressourcen zahlen, die Sie voraussichtlich nicht mehr verwenden werden.

> **Note**
>
> Bei Gateways, die auf einer Amazon-EC2-Instance bereitgestellt werden, existiert die Instance weiterhin, bis Sie sie löschen.
> Bei Gateways, die auf einer virtuellen Maschine (VM) bereitgestellt sind, ist die Gateway-VM nach dem Löschen des Gateways weiterhin in der Virtualisierungsumgebung vorhanden. Zum Entfernen der Vm verwenden Sie den VMware vSphere-Client, Microsoft Hyper-V Manager oder Linux Kernel-basierte virtuelle Maschine (KVM)-Client, um eine Verbindung mit dem Host herzustellen und die VM zu entfernen. Beachten Sie, dass Sie die gelöschte Gateway-VM nicht erneut verwenden können, um ein neues Gateway zu aktivieren.

So löschen Sie ein Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie Gateways und anschließend ein oder mehrere Gateways zum Löschen aus.
3. Wählen Sie für Aktionen die Option Gateway löschen aus. Das Bestätigungsdialogfeld wird angezeigt.

   > **Warning**
   >
   > Bevor Sie diesen Schritt ausführen, stellen Sie sicher, dass derzeit keine Anwendungen in die Gateway-Volumes schreiben. Wenn Sie das Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten. Wenn ein Gateway gelöscht wird, gibt es keine Möglichkeit, es wiederherzustellen.

4. Vergewissern Sie sich, dass Sie die angegebenen Gateways löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen aus.
5. (Optional) Wenn Sie Feedback zu Ihrem gelöschten Gateway geben möchten, füllen Sie das Feedback-Dialogfeld aus und wählen Sie dann Absenden. Wählen Sie andernfalls Überspringen aus.

> **Important**
>
> Sie bezahlen nach dem Löschen eines Gateways keine Gebühren mehr für die Software, jedoch bleiben Ressourcen wie virtuelle Bänder, Amazon Elastic Block Store (Amazon EBS)-Snapshots und Amazon-EC2-Instances bestehen. Diese Ressourcen werden Ihnen weiterhin berechnet. Sie können Amazon-EC2-Instances und Amazon EBS-Snapshots entfernen, indem Sie Ihr Amazon-EC2-Abonnement kündigen. Wenn Sie Ihr Amazon-EC2-Abonnement behalten möchten, können Sie Ihre Amazon-EC2-Snapshots mithilfe der Amazon-EC2-Konsole löschen.

Entfernen von Ressourcen von einem lokal bereitgestellten Gateway

Anhand der folgenden Anweisungen können Sie Ressourcen von einem Gateway entfernen, das lokal bereitgestellt ist.

Entfernen von Ressourcen von einem auf einer VM bereitgestellten Tape Gateway

Beim Löschen einer Gateway-Virtual Tape Library (Gateway-VTL) führen Sie vor und nach dem Löschen des Gateways zusätzliche Schritte zur Bereinigung aus. Diese zusätzlichen Schritte helfen Ihnen beim Entfernen von Ressourcen, die Sie nicht benötigen, damit Sie nicht weiter für diese bezahlen.

Wenn das Tape Gateway, das Sie löschen möchten, auf einer virtuellen Maschine (VM) bereitgestellt ist, sollten Sie die folgenden Aktionen ausführen, um die Ressourcen zu bereinigen.

> **Important**
>
> Vor dem Löschen eines Tape Gateways müssen Sie alle Bandabrufvorgänge abbrechen und alle abgerufenen Bänder auswerfen.
> Nachdem Sie das Tape Gateway gelöscht haben, müssen Sie alle zu diesem Tape Gateway gehörigen Ressourcen entfernen, die Sie nicht benötigen, um unnötige Kosten zu vermeiden.

Beim Löschen eines Tape Gateways kann eines von zwei Szenarien auftreten.

- Das Tape Gateway ist mit verbunden AWS – Wenn das Tape Gateway mit verbunden ist AWS und Sie das Gateway löschen, sind die dem Gateway zugeordneten iSCSI-Ziele (d. h. die virtuellen Bandlaufwerke und der Medienwechsler) nicht mehr verfügbar.
- Das Tape Gateway ist nicht verbunden mit AWS – Wenn das Tape Gateway nicht mit verbunden ist AWS, z. B. wenn die zugrunde liegende VM ausgeschaltet ist oder Ihr Netzwerk ausgefallen ist, können Sie das Gateway nicht löschen. Wenn Sie versuchen, es zu löschen, haben Sie nach der erneuten Inbetriebnahme der Umgebung möglicherweise ein On-Premises ausgeführtes Tape Gateway mit verfügbaren iSCSI-Zielen. Es werden jedoch keine Tape Gateway-Daten in hochgeladen oder von dort heruntergeladen AWS.

Wenn das zu löschende Tape nicht funktioniert, müssen Sie es zuerst deaktivieren, bevor Sie es löschen. Gehen Sie dazu wie folgt vor:

- Um Bänder mit dem Status "RETRIEVED" aus der Bibliothek zu löschen, werfen Sie das Band mithilfe Ihrer Sicherungssoftware aus. Anweisungen finden Sie unter Archivieren des Bandes.

Nach der Deaktivierung des Tape Gateways und dem Löschen der Bänder können Sie das Tape Gateway löschen. Anweisungen zum Löschen eines Gateways finden Sie unter Löschen eines Gateways mithilfe der Storage-Gateway-Konsole.

Wenn Sie Bänder archiviert haben, bleiben diese Bänder erhalten und Sie zahlen weiterhin für Speicher, bis Sie sie löschen. Informationen zum Löschen von Bändern aus einem Archiv finden Sie unter Löschen von Bändern.

> **Important**
>
> Sie zahlen für virtuelle Bänder in einem Archiv für mindestens 90 Tage Speicher. Wenn Sie ein virtuelles Band abrufen, das weniger als 90 Tage im Archiv gespeichert war, werden Ihnen trotzdem 90 Tage Speicher berechnet.

Entfernen von Ressourcen von einem auf einer Amazon-EC2-Instance bereitgestellten Gateway

Wenn Sie ein Gateway löschen möchten, das Sie auf einer Amazon EC2-Instance bereitgestellt haben, empfehlen wir Ihnen, die AWS Ressourcen zu bereinigen, die mit dem Gateway verwendet wurden, insbesondere die Amazon EC2-Instance, alle Amazon-EBS-Volumes und Bänder, wenn Sie

ein Tape Gateway bereitgestellt haben. Auf diese Weise können Sie unerwartete nutzungsabhängige Gebühren vermeiden.

Entfernen von Ressourcen von einem auf Amazon EC2 bereitgestellten Tape Gateway

Wenn Sie ein Tape bereitgestellt haben, schlagen wir vor, dass Sie die folgenden Schritte ausführen, um das Gateway zu löschen und seine Ressourcen zu bereinigen:

1. Löschen Sie alle virtuellen Bänder, die Sie auf das Tape Gateway abgerufen haben. Weitere Informationen finden Sie unter Löschen von Bändern.
2. Löschen Sie alle virtuellen Bänder aus der Bandbibliothek. Weitere Informationen finden Sie unter Löschen von Bändern.
3. Löschen Sie das Tape Gateway. Weitere Informationen finden Sie unter Löschen eines Gateways mithilfe der Storage-Gateway-Konsole.
4. Beenden Sie alle Amazon-EC2-Instances und löschen Sie alle Amazon-EBS-Volumes. Weitere Informationen finden Sie unter Bereinigungen von Instances und Volumes im Amazon-EC2-Benutzerhandbuch für Linux-Instances.
5. Löschen Sie alle archivierten virtuellen Bänder. Weitere Informationen finden Sie unter Löschen von Bändern.

> **Important**
>
> Sie zahlen für virtuelle Bänder im Archiv für mindestens 90 Tage Speicher. Wenn Sie ein virtuelles Band abrufen, das weniger als 90 Tage im Archiv gespeichert war, werden Ihnen trotzdem 90 Tage Speicher berechnet.

Leistung

In diesem Abschnitt wird die Leistung von Storage Gateway beschrieben.

Themen

Leistungsleitfaden für Tape Gateway

In diesem Abschnitt finden Sie eine Konfigurationsanleitung für die Bereitstellung von Hardware für Ihre Tape Gateway-VM. Die Amazon-EC2-Instance-Größen und -Typen, die in der Tabelle aufgeführt sind, sind Beispiele und werden als Referenz bereitgestellt.

Konfiguration	Schreibdurchsatz in Gbit/s	Lesedurchsatz aus Cache in Gbit/s	Lesen Sie „Amazon Web Services Cloud-Durchsatz in Gbit/s“
Host-Plattform: Amazon-EC2-Instance − c5.4xlarge CPU: 16 vCPU | RAM: 32 GB Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPs Cache-Festplatte: Striped-RAID (2 x 500 GB, io1 EBS SSD, 25.000 IOPs) Upload-Pufferdatenträger: 450 GB, io1 SSD, 2000 IOPs	2.3	4,0	2.2

Konfiguration	Schreibdurchsatz in Gbit/s	Lesedurchsatz aus Cache in Gbit/s	Lesen Sie „Amazon Web Services Cloud-Durchsatz in Gbit/s“
Netzwerkbandbreite zur Cloud: 10 Gbit/s			
Host-Plattform: Storage Gateway-Hardware Appliance Cache-Datenträger: 2,5 TB Upload-Pufferdatenträger: 2 TB Netzwerkbandbreite zur Cloud: 10 Gbit/s	2.3	8.8	3.8
Host-Plattform: Amazon-EC2-Instance − c5d.9xlarge CPU: 36 vCPU | RAM: 72 GB Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPs Cache-Datenträger: 900 GB NVMe-Disk Upload-Pufferdatenträger: 900 GB NVMe-Disk Netzwerkbandbreite zur Cloud: 10 Gbit/s	5.2	11.6	5.2

Konfiguration	Schreibdurchsatz in Gbit/s	Lesedurchsatz aus Cache in Gbit/s	Lesen Sie „Amazon Web Services Cloud-Durchsatz in Gbit/s“
Host-Plattform: Amazon-EC2-Instance − c5d.metal CPU: 96 vCPU | RAM: 192 GB Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPs Cache-Festplatte: Striped-RAID (2 x 900-GB-NVMe-Festplatte) Upload-Pufferdatenträger: 900 GB NVMe-Disk Netzwerkbandbreite zur Cloud: 10 Gbit/s	5.2	11.6	7.2

Note

Diese Leistung wurde unter der Verwendung einer Blockgröße von 1 MB und zehn Bandlaufwerken gleichzeitig erzielt.
Die EC2-Konfigurationen in der obigen Tabelle sollen nur repräsentativ für die Leistung sein, die Sie auf Ihren eigenen physischen Servern mit ähnlichen Ressourcen erzielen könnten. Die EC2-Konfigurationen mit Striped-RAID wurden beispielsweise über einen speziellen Mechanismus vorgenommen, der von unserem Gateway auf EC2 im Allgemeinen nicht unterstützt wird. Um eine ähnliche Leistung zu erzielen, sollten Sie stattdessen einen Hardware-RAID-Controller verwenden, der an den On-Premises-Server angeschlossen ist, auf dem Ihr Gateway läuft.
Die Leistung hängt von der Konfiguration Ihrer Hostplattform und der Netzwerkbandbreite ab.

Informationen zur Verbesserung der Schreib- und Lese-Durchsatzleistung Ihres Tape Gateways finden Sie unter Optimieren von iSCSI-Einstellungen, Verwenden Sie eine größere Blockgröße für Bandlaufwerke und Optimieren der Leistung von virtuellen Bandlaufwerken in der Sicherungssoftware.

Optimieren der Gateway-Leistung

Empfohlene Gateway-Serverkonfiguration

Um die beste Leistung aus Ihrem Gateway herauszuholen, wird von Storage Gateway die folgende Gateway-Konfiguration für den Host-Server Ihres Gateways empfohlen:

- Mindestens 64 dedizierte physische CPU-Kerne
- Für ein Tape Gateway sollte Ihre Hardware die folgenden Mengen an RAM reservieren:
  - Mindestens 16 GiB reservierter RAM für Gateways mit einer Cache-Größe von bis zu 16 TiB
  - Mindestens 32 GiB reservierter RAM für Gateways mit einer Cache-Größe von 16 TiB bis 32 TiB
  - Mindestens 48 GiB reservierter RAM für Gateways mit einer Cache-Größe von 32 TiB bis 64 TiB

  > **Note**
  >
  > Für eine optimale Gateway-Leistung müssen Sie mindestens 32 GiB RAM bereitstellen.

- Festplatte 1, die wie folgt als Gateway-Cache verwendet werden soll:
  - Striped-RAID (redundantes Array unabhängiger Festplatten), bestehend aus NVMe-SSDs.
- Festplatte 2, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
  - Striped-RAID, bestehend aus NVMe-SSDs.
- Festplatte 3, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
  - Striped-RAID aus NVMe-SSDs.
- Netzwerkadapter 1 auf VM Netzwerk 1 konfiguriert:
  - Verwenden Sie VM-Netzwerk 1 und fügen Sie VMXnet3 (10 Gbit/s) zur Verwendung der Aufnahme hinzu.
- Netzwerkadapter 2 auf VM Netzwerk 2 konfiguriert:
  - Verwenden Sie VM-Netzwerk 2 und fügen Sie VMXnet3 (10 Gbit/s) hinzu, um eine Verbindung zu AWS herzustellen.

Hinzufügen von Ressourcen zu Ihrem Gateway

Die folgenden Engpässe können die Leistung Ihres Tape Gateway sunter den theoretischen maximalen anhaltenden Durchsatz (Ihre Bandbreite zur AWS Cloud) reduzieren:

- Anzahl CPU-Kerne
- Durchsatz der Cache-/Upload-Puffer-Festplatte
- RAM-Gesamtgröße
- Netzwerkbandbreite zu AWS
- Netzwerkbandbreite vom Initiator zum Gateway

In diesem Abschnitt werden Schritte beschreiben, mit denen Sie die Leistung Ihres Gateways optimieren können. Die Anleitungen basiert auf dem Hinzufügen von Ressourcen zu Ihrem Gateway oder Ihrem Anwendungsserver.

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

Verwenden von Hochleistungs-Festplatten

Der Durchsatz von Cache- und Upload-Puffer-Festplatten kann die Upload- und Download-Leistung Ihres Gateways beeinträchtigen. Wenn die Leistung Ihres Gateways deutlich unter den Erwartungen liegt, sollten Sie in Erwägung ziehen, den Durchsatz der Cache- und Upload-Puffer-Festplatten wie folgt zu verbessern:

- Verwenden Sie Striped-RAID wie RAID 10, um den Festplattendurchsatz zu verbessern, idealerweise mit einem Hardware-RAID-Controller.

> **Note**
>
> Bei RAID (Redundant Array of Independent Disks) bzw. speziell Disk-Striped-RAID-Konfigurationen wie RAID 10 wird ein Datenbestand in Blöcke aufgeteilt und die Datenblöcke werden auf mehrere Speichergeräte verteilt. Das von Ihnen verwendete RAID-Level wirkt sich auf die genaue Geschwindigkeit und Fehlertoleranz aus, die Sie erreichen können. Durch die Verteilung der I/O-Workloads auf mehrere Festplatten ist der Gesamtdurchsatz des RAID-Geräts viel höher als der einer einzelnen Member-Festplatte.

- Verwendung direkt angeschlossener Hochleistungsfestplatten

  Zum Optimieren der Leistung Ihres Gateways können Sie Hochleistungsdatenträger hinzufügen, wie z. B. Solid-State Drives (SSDs) und einen NVMe-Controller. Sie können auch virtuelle Festplatten direkt von einem Storage Area Network (SAN) anstelle des Microsoft Hyper-V NTFS, zu Ihrer VM hinzufügen. Verbesserte Festplattenleistung führt in der Regel zu höherem Durchsatz und zu mehr Ein- und Ausgabe-Operationen pro Sekunde (IOPS).

  Um den Durchsatz zu messen, verwenden Sie die `WriteBytes` Metriken `ReadBytes` und 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. Weitere Informationen zu Gateway-Metriken, finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

  > **Note**
  >
  > CloudWatch -Metriken sind nicht für alle Gateways verfügbar. Weitere Informationen, zu Gateway Metriken, finden Sie unter Überwachen von Storage Gateway.

Hinzufügen von weiteren Upload-Puffer-Festplatten

Um einen höheren Schreibdurchsatz zu erreichen, fügen Sie mindestens zwei Upload-Puffer-Festplatten hinzu. Werden Daten auf das Gateway geschrieben, werden sie lokal auf die Upload-Puffer-Festplatten geschrieben und dort gespeichert. Danach werden die gespeicherten lokalen Daten asynchron von den Festplatten gelesen, um sie zu verarbeiten und in AWS hochzuladen. Wenn weitere Upload-Puffer-Festplatten hinzugefügt werden, kann dies die Anzahl der gleichzeitigen I/O-Vorgänge auf den einzelnen Festplatten verringern. Dies kann zu einem erhöhten Schreibdurchsatz für das Gateway führen.

Sichern von virtuellen Gateway-Festplatten mit getrennten physischen Datenträgern

Bei der Bereitstellung von Gateway-Datenträgern wird dringend empfohlen, keine lokalen Festplatten für den Upload-Puffer und Cache-Speicher bereitzustellen, die die gleiche zugrunde liegende physische Speicherressource verwenden. Zum Beispiel, für VMware ESXi, die Zugrunde liegenden physische Speicherressourcen werden als Datenspeicher dargestellt. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-Dateien.

Wenn Sie eine virtuelle Festplatte bereitstellen (z. B. als Upload-Puffer), können Sie die virtuelle Festplatte im gleichen Datenspeicher wie die VM oder in einem anderen Datenspeicher speichern.

Wenn Sie über mehr als einen Datenspeicher verfügen, sollten Sie unbedingt einen Datenspeicher für jeden Typ von lokalem Speicher wählen, den sie erstellen. Ein Datenspeicher, der nur durch einen einzigen zugrunde liegenden physischen Datenträger gestützt wird, kann zu einer schlechten Leistung führen. Beispielsweise wenn Sie solch einen Datenträger sowohl zum Stützen des Cache-Speichers als auch des Upload-Puffers in einer Gateway-Konfiguration verwenden. Dementsprechend kann auch ein Datenspeicher, der durch eine leistungsschwächere RAID-Konfiguration gestützt wird, wie z. B. RAID 1 oder RAID 6, eine schlechte Leistung zur Folge haben.

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 virtuellen Prozessoren, die der Gateway-VM zugeordnet sind, jeweils von einem dedizierten CPU-Kern gestützt werden. Stellen Sie zudem sicher, dass Sie die CPUs des Host-Servers nicht überzeichnen.

Wenn Sie Ihrem Gateway-Host-Server weitere CPUs hinzufügen, erhöhen Sie die Verarbeitungskapazität des Gateways. Dadurch ermöglichen Sie Ihrem Gateway, gleichzeitig sowohl Daten aus Ihrer Anwendung in Ihrem lokalen Speicher zu sichern als auch diese Daten in Amazon S3 hochzuladen. Zusätzliche CPUs helfen auch sicherzustellen, dass Ihr Gateway genug CPU-Ressourcen erhält, wenn der Host mit anderen VMs geteilt wird. Über genügend CPU-Ressourcen zu verfügen hat den allgemeinen Effekt der Verbesserung des Durchsatzes.

Erhöhen der Bandbreite zwischen Ihrem Gateway und der AWS Cloud

Eine Erhöhung Ihrer Bandbreite zu und von AWS erhöht die maximale Dateneingangsrate für Ihr Gateway und den Ausgang in die AWS Cloud. Dies kann die Leistung Ihres Gateways verbessern, wenn die Netzwerkgeschwindigkeit der begrenzende Faktor in Ihrer Gateway-Konfiguration ist und nicht andere Faktoren wie langsame Festplatten oder eine mangelhafte Bandbreite der Verbindung zwischen Gateway und Initiator.

Die Netzwerkbandbreite zu und von AWS definiert die theoretische maximale durchschnittliche Leistung Ihres Tape Gateways bei anhaltenden Workloads.

- Die durchschnittliche Geschwindigkeit, mit der Sie über lange Zeiträume Daten auf Ihr Tape Gateway schreiben können, wird Ihre Upload-Bandbreite zu AWS nicht überschreiten.
- Die durchschnittliche Rate, mit der Sie Daten aus Ihrem Tape Gateway über lange Intervalle lesen können, wird Ihre Download-Bandbreite zu nicht überschreiten AWS.

> **Note**
>
> Die beobachtete Gateway-Leistung wird wahrscheinlich geringer sein als die Netzwerkbandbreite. Dies ist auf andere hier aufgeführte einschränkende Faktoren zurückzuführen, wie z. B. den Durchsatz der Cache/Upload-Puffer-Festplatte, die Anzahl der CPU-Kerne, die RAM-Gesamtgröße oder die Bandbreite zwischen Ihrem Initiator und dem Gateway. Darüber hinaus umfasst der normale Betrieb Ihres Gateways viele Maßnahmen zum Schutz Ihrer Daten, was dazu führen kann, dass die beobachtete Leistung geringer als die Netzwerkbandbreite ist.

Optimieren von iSCSI-Einstellungen

Sie können die iSCSI-Einstellungen auf Ihrem iSCSI-Initiator optimieren, um eine höhere E/A-Leistung zu erzielen. Wir empfehlen die Auswahl von 256 KiB für `MaxReceiveDataSegmentLength` und `FirstBurstLength` sowie von 1 MiB für `MaxBurstLength`. Weitere Hinweise zum Konfigurieren von iSCSI-Einstellungen finden Sie unter Anpassen von iSCSI-Einstellungen.

> **Note**
>
> Diese empfohlenen Einstellungen können eine insgesamt bessere Leistung ermöglichen. Die spezifischen iSCSI-Einstellungen, die zur Leistungsoptimierung erforderlich sind, variieren jedoch je nach verwendeter Backup-Software. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Backup-Software.

Verwenden Sie eine größere Blockgröße für Bandlaufwerke

Bei einem Tape Gateway beträgt die Standardblockgröße für ein Bandlaufwerk 64 KB. Sie können jedoch die Blockgröße auf bis zu 1 MB erhöhen, um die E/A-Leistung zu verbessern.

Die von Ihnen gewählte Blockgröße hängt von der maximalen Blockgröße ab, die Ihre Sicherungssoftware unterstützt. Es wird empfohlen, in Ihrer Sicherungssoftware die größtmögliche Blockgröße für Bandlaufwerke festzulegen. Allerdings darf diese Blockgröße nicht größer sein der Höchstwert von 1 MB, den das Gateway unterstützt.

Tape Gateways handeln die Blockgröße für virtuelle Bandlaufwerke so aus, dass sie automatisch mit der Einstellung in der Sicherungssoftware übereinstimmen. Wenn Sie die Blockgröße in der Sicherungssoftware erhöhen, wird empfohlen, bei den Einstellungen zu überprüfen, ob der Host-Initiator die neue Blockgröße unterstützt. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Sicherungssoftware. Weitere Informationen zu spezifischen Anleitungen für die Gateway-Leistung finden Sie unter Leistung.

Optimieren der Leistung von virtuellen Bandlaufwerken in der Sicherungssoftware

Ihre Sicherungssoftware kann auf bis zu 10 virtuellen Bandlaufwerken in einem Tape Gateway gleichzeitig Daten sichern. Wir empfehlen, dass Sie Sicherungsaufträge in Ihrer Sicherungssoftware konfigurieren, bei denen mindestens vier (4) virtuelle Bandlaufwerke gleichzeitig im Tape Gateway verwendet werden. Es lässt sich ein besserer Schreibdurchsatz erreichen, wenn die Sicherungssoftware die Daten auf mehreren virtuellen Bändern gleichzeitig sichert.

In der Regel können Sie einen höheren maximalen Durchsatz erreichen, wenn Sie mit mehr virtuellen Bändern gleichzeitig arbeiten (lesen oder schreiben). Wenn Sie mehr Bandlaufwerke verwenden, kann Ihr Gateway mehr Anforderungen gleichzeitig bearbeiten, wodurch möglicherweise die Leistung verbessert wird.

Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung

Erhöhen der Bandbreite zwischen Ihrem Anwendungsserver und Ihrem Gateway

Die Verbindung zwischen Ihrem iSCSI-Initiator und dem Gateway kann die Upload- und Download-Leistung einschränken. Wenn Ihr Gateway eine deutlich schlechtere Leistung als erwartet aufweist und Sie die Anzahl der CPU-Kerne und den Festplattendurchsatz bereits verbessert haben, sollten Sie Folgendes in Betracht ziehen:

- Rüsten Sie Ihre Netzwerkkabel auf, um eine höhere Bandbreite zwischen Ihrem Initiator und dem Gateway zu erreichen.
- Verwenden Sie so viele Bandlaufwerke wie möglich gleichzeitig. iSCSI unterstützt keine Warteschlangenbildung für mehrere Anforderungen für dasselbe Ziel. Daher gilt, je mehr Bandlaufwerke Sie verwenden, desto mehr Anforderungen kann Ihr Gateway gleichzeitig bedienen. Auf diese Weise können Sie die Bandbreite zwischen Ihrem Gateway und dem Initiator besser nutzen und den scheinbaren Durchsatz Ihres Gateways erhöhen.

Zum Optimieren der Gateway-Leistung, stellen Sie sicher, dass die Netzwerkbandbreite zwischen Ihrer Anwendung und dem Gateway, Ihre Anwendungsansprüche unterstützen kann. Sie können die Metriken `ReadBytes` und `WriteBytes` des Gateways verwenden, um den gesamten Datendurchsatz zu messen. Weitere Informationen zu diesen Metriken finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

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

Hinzufügen von CPU-Ressourcen zu Ihrer Anwendungsumgebung

Kann Ihre Anwendung zusätzliche CPU-Ressourcen verwenden, kann das Hinzufügen weiterer CPUs dazu beitragen, dass Ihre Anwendung die E/A-Last skaliert.

Verwenden von VMware vSphere High Availability mit Storage Gateway

Storage Gateway bietet durch eine Reihe von Zustandsprüfungen auf Anwendungsebene, die in VMware vSphere High Availability (VMware HA) integriert sind, Hochverfügbarkeit für VMware. 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.

vSphere HA arbeitet, indem virtuelle Maschinen und die Hosts, auf denen sie sich befinden, aus Redundanzgründen in einem Cluster zusammengefasst werden. Hosts im Cluster werden überwacht und im Falle eines Ausfalls werden die virtuellen Maschinen auf einem ausgefallenen Host auf alternativen Hosts neu gestartet. Im Allgemeinen erfolgt diese Wiederherstellung schnell und ohne Datenverlust. Weitere Informationen zu vSphere HA finden Sie unter Funktionsweise von vSphere HA in der VMware-Dokumentation.

> **Note**
>
> Die Zeit, die für den Neustart einer ausgefallenen virtuellen Maschine und die Wiederherstellung der iSCSI-Verbindung auf einem neuen Host benötigt wird, hängt

von vielen Faktoren ab, z. B. der Hostbetriebssystem- und Ressourcenlast, der Festplattengeschwindigkeit, der Netzwerkverbindung und der SAN/Speicherinfrastruktur. Um Failover-Ausfallzeiten zu minimieren, implementieren Sie die Empfehlungen unter Optimieren der Gateway-Leistung.

Führen Sie die folgenden Schritte aus, um VMware HA mit Storage Gateway zu verwenden.

Themen

Konfigurieren Ihres vSphere VMware HA-Clusters

Erstellen Sie zunächst einen VMware-Cluster, wenn Sie dies noch nicht getan haben. Informationen zum Erstellen eines VMware-Clusters finden Sie unter Erstellen eines vSphere HA-Clusters in der VMware-Dokumentation.

Konfigurieren Sie anschließend Ihren VMware-Cluster für die Arbeit mit Storage Gateway.

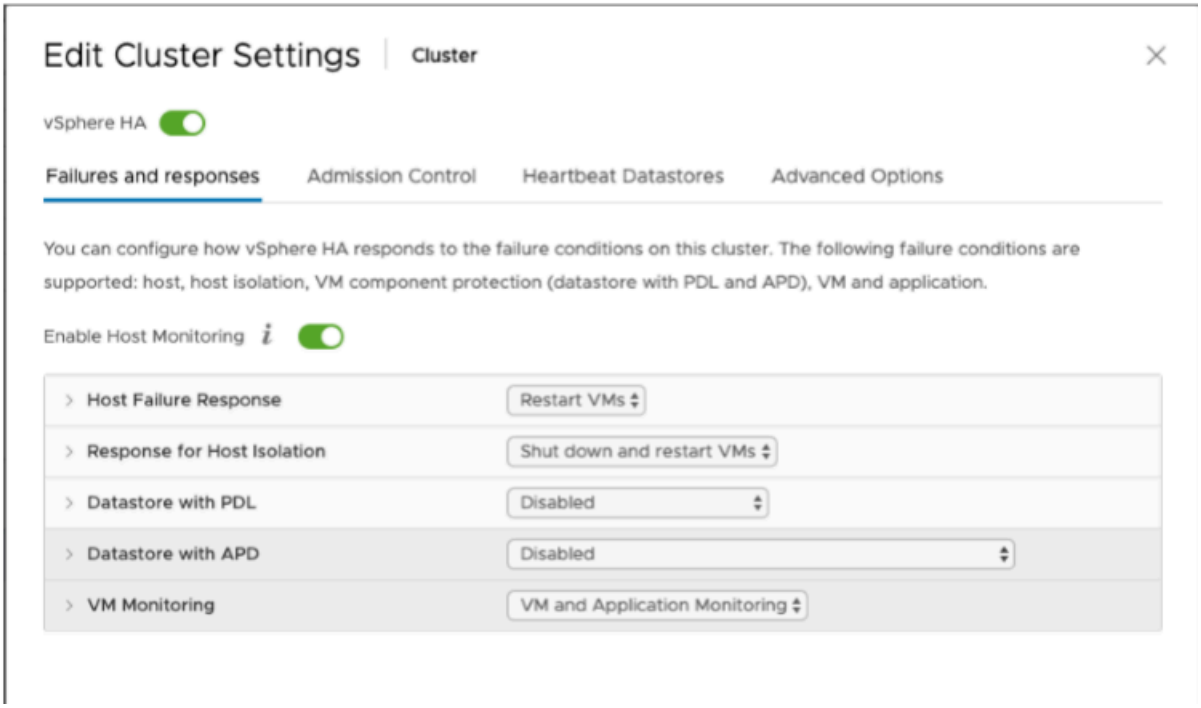
So konfigurieren Sie Ihren VMware-Cluster

1. Stellen Sie auf der Seite Clustereinstellungen bearbeiten in VMware vSphere sicher, dass die VM-Überwachung für die VM- und Anwendungsüberwachung konfiguriert ist. Legen Sie hierzu die folgenden Optionen wie aufgeführt fest:

   - Host Failure Response (Host-Fehlerantwort): Restart VMs (VMs neu starten)
   - Response for Host Isolation (Antwort für Host-Isolation): Shut down and restart VMs (VMs herunterfahren und neu starten)
   - 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)

Im folgenden Screenshot sehen Sie ein Beispiel.



2. Optimieren Sie die Empfindlichkeit des Clusters, indem Sie die folgenden Werte anpassen:

   - Fehlerintervall: Nach diesem Intervall wird die VM neu gestartet, wenn kein VM-Heartbeat empfangen wird.
   - 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 auf dem Cluster andere VMs ausgeführt werden, können Sie diese Werte speziell für Ihre VM festlegen. Dies ist erst möglich, wenn Sie die VM über das OVA-Image bereitstellen. Weitere Hinweise zum Festlegen dieser Werte finden Sie unter (Optional) Hinzufügen von Überschreibungsoptionen für andere VMs auf Ihrem Cluster.

Herunterladen des OVA-Image von der Storage-Gateway-Konsole

So laden Sie das OVA-Image für Ihren Gateway-Typ herunter

- Wählen Sie auf der Seite Gateway einrichten in der Storage-Gateway-Konsole Ihren Gateway-Typ und Ihre Host-Plattform aus und verwenden Sie dann den Link in der Konsole, um die OVA-Datei herunterzuladen, wie unter Einrichten von Tape Gateway beschrieben.

Bereitstellen des Gateways

Stellen Sie das OVA-Image in Ihrem konfigurierten Cluster auf einem der Cluster-Hosts bereit.

So stellen Sie das OVA-Image des Gateways bereit

1. Stellen Sie das OVA-Image auf einem der Hosts im Cluster bereit.
2. Stellen Sie sicher, dass die Datenspeicher, die Sie für den Stamm-Datenträger und den Cache wählen, für alle Hosts im Cluster verfügbar sind. Bei der Bereitstellung der OVA-Datei für Storage Gateway in einer VMware- oder On-Premises-Umgebung werden die Festplatten als paravirtualisierte SCSI-Festplatten beschrieben. Paravirtualisierung ist ein Modus, in dem die Gateway-VM mit dem Host-Betriebssystem arbeitet, damit die Konsole die der VM hinzugefügten virtuellen Festplatten identifizieren kann.

   So konfigurieren Sie die VM für die Verwendung von paravirtualisierten Controllern

   1. Öffnen Sie im VMware vSphere-Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM und wählen Sie dann Edit Settings (Einstellungen bearbeiten).
   2. Wählen Sie im Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) die Registerkarte Hardware, wählen Sie SCSI controller 0 (SCSI-Controller 0) und wählen Sie dann Change Type (Typ ändern).

3. Wählen Sie im Dialogfeld Change SCSI Controller Type (SCSI-Controllertyp ändern) den SCSI-Controllertyp VMware Paravirtual und wählen Sie dann OK.

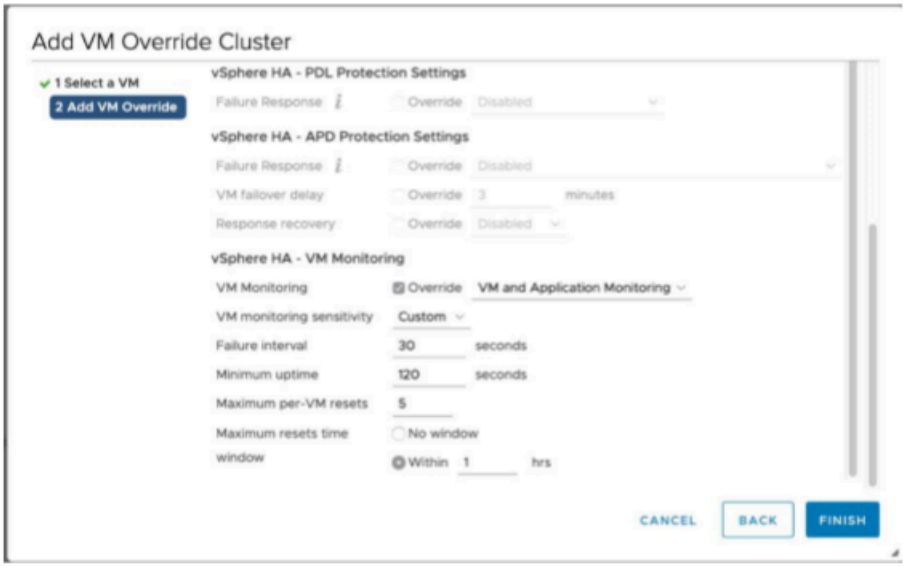
(Optional) Hinzufügen von Überschreibungsoptionen für andere VMs auf Ihrem Cluster

Wenn auf Ihrem Cluster andere VMs ausgeführt werden, können Sie die Clusterwerte speziell für jede einzelne VM festlegen.

So fügen Sie Überschreibungsoptionen für andere VMs in Ihrem Cluster hinzu

1. Wählen Sie Ihren Cluster auf der Seite Summary (Zusammenfassung), um die Clusterseite zu öffnen, und wählen Sie dann Configure (Konfigurieren).
2. Wählen Sie die Registerkarte Configuration (Konfiguration) und dann VM Overrides (VM-Überschreibungen)aus.
3. Fügen Sie eine neue VM-Überschreibungsoption hinzu, um die einzelnen Werte zu ändern.

   Im folgenden Screenshot sehen Sie Überschreibungsoptionen.



Aktivieren des Gateways

Nachdem das OVA-Image für Ihr Gateway bereitgestellt wurde, aktivieren Sie Ihr Gateway. Die entsprechenden Anweisungen unterscheiden sich je nach Gateway-Typ.

So aktivieren Sie das Gateway

- Befolgen Sie die in den folgenden Themen beschriebenen Verfahren:

  a. Verbinden Sie Ihr Tape Gateway mit AWS

  b. Überprüfen der Einstellungen und Aktivieren von Tape Gateway

  c. Konfigurieren von Tape Gateway

Testen der Konfiguration von VMware High Availability

Testen Sie Ihre Konfiguration, nachdem Sie Ihr Gateway aktiviert haben.

So testen Sie Ihre Konfiguration für VMware HA

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und anschließend das Gateway aus, das Sie auf VMware HA testen möchten.
3. Wählen Sie unter Actions (Aktionen) die Option Verify VMware HA (Überprüfen von VMware HA) aus.
4. Wählen Sie im Feld Verify VMware High Availability Configuration (Überprüfen der Konfiguration von VMware High Availability), das jetzt angezeigt wird, die Option OK.

   > **Note**
   >
   > Wenn Sie die Konfiguration für VMware HA testen, wird Ihre Gateway-VM neu gestartet und die Verbindung zu Ihrem Gateway unterbrochen. Der Test kann einige Minuten in Anspruch nehmen.

   Wenn der Test erfolgreich abgeschlossen wurde, wird der Status Verified (Überprüft) auf der Registerkarte „Details“ des Gateways in der Konsole angezeigt.
5. Wählen Sie Exit (Beenden) aus.

Informationen zu VMware HA-Ereignissen finden Sie in den Amazon- CloudWatch Protokollgruppen. Weitere Informationen finden Sie unter Abrufen von Tape-Gateway-Zustandsprotokollen mit CloudWatch Protokollgruppen, die .

Sicherheit in AWS Storage Gateway

Cloud-Sicherheit bei AWS hat höchste Priorität. Als - AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die entwickelt wurde, um die Anforderungen der sicherheitssensibelsten Organisationen zu erfüllen.

Sicherheit ist eine geteilte Verantwortung zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS Services in der Amazon Web Services Cloud ausführt. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Externe Prüfer testen und überprüfen im Rahmen der AWS Compliance-Programme regelmäßig die Wirksamkeit unserer Sicherheit. Informationen zu den Compliance-Programmen, die für AWS Storage Gateway gelten, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -ServicesIm.
- Sicherheit in der Cloud – Ihre Verantwortung wird durch den - AWS Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Storage Gateway angewendet werden kann. Die folgenden Themen veranschaulichen, wie Sie Storage Gateway konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere - AWS Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer Storage Gateway-Ressourcen unterstützen.

Themen

Datenschutz in AWS Storage Gateway

Das AWS Modell der geteilten VerantwortungModell gilt für den Datenschutz in AWS Storage Gateway . Wie in diesem Modell beschrieben, AWS ist für den Schutz der globalen Infrastruktur verantwortlich, die alle ausführt 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 Ihnen, -Anmeldeinformationen zu schützen AWS-Konto und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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).
- Verwenden Sie SSL/TLS für die Kommunikation mit - AWS Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API- und Benutzeraktivitätsprotokollierung mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder eine API FIPS-140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, 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 AWS-Services über die Konsole, API AWS CLI oder AWS SDKs arbeiten. 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

Storage Gateway verwendet SSL/TLS (Secure Socket Layers/Transport Layer Security), um Daten zu verschlüsseln, die zwischen Ihrer Gateway-Appliance und Ihrem AWS Speicher übertragen werden. Storage Gateway verwendet standardmäßig von Amazon S3 verwaltete Verschlüsselungsschlüssel (SSE-S3), um alle in Amazon S3 gespeicherten Daten serverseitig zu verschlüsseln. Sie haben die Möglichkeit, die Storage Gateway-API zu verwenden, um Ihr Gateway so zu konfigurieren, dass in der Cloud gespeicherte Daten mit serverseitiger Verschlüsselung mit AWS Key Management Service (SSE-KMS)-Schlüsseln verschlüsselt werden.

> **Important**
>
> Wenn Sie einen - AWS KMS Schlüssel für die serverseitige Verschlüsselung verwenden, müssen Sie einen symmetrischen Schlüssel auswählen. 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.

Verschlüsseln einer Dateifreigabe

Bei einer Dateifreigabe können Sie Ihr Gateway so konfigurieren, dass Ihre Objekte mithilfe von SSE-KMS mit Schlüsseln verschlüsselt werden, die von AWS KMS verwaltet werden. Informationen zur Verwendung der Storage Gateway-API zum Verschlüsseln von Daten, die in eine Dateifreigabe geschrieben wurden, finden Sie unter CreateNFSFileShare in der AWS Storage Gateway API-Referenz zu .

Verschlüsseln eines Volumes

Für zwischengespeicherte und gespeicherte Volumes können Sie Ihr Gateway so konfigurieren, dass in der Cloud gespeicherte Volume-Daten mit von AWS KMS verwalteten Schlüsseln verschlüsselt werden, indem Sie die Storage Gateway-API verwenden. Sie können einen der verwalteten Schlüssel als KMS-Schlüssel angeben. Der von Ihnen für die Verschlüsselung Ihres Volumes verwendete Schlüssel kann nach dem Erstellen des Volumes nicht geändert werden. Informationen zur Verwendung der Storage Gateway-API zum Verschlüsseln von Daten, die auf ein zwischengespeichertes oder gespeichertes Volume geschrieben wurden, finden Sie unter CreateCachediSCSIVolume oder CreateStorediSCSIVolume in der AWS Storage Gateway API-Referenz zu .

Verschlüsseln eines Bands

Für ein virtuelles Band können Sie Ihr Gateway so konfigurieren, dass in der Cloud gespeicherte Banddaten mit von AWS KMS verwalteten Schlüsseln verschlüsselt werden, indem Sie die Storage Gateway-API verwenden. Sie können einen der verwalteten Schlüssel als KMS-Schlüssel angeben. Der von Ihnen für die Verschlüsselung Ihrer Banddaten verwendete Schlüssel kann nach dem Erstellen des Bands nicht geändert werden. Informationen zur Verwendung der Storage Gateway-API zum Verschlüsseln von Daten, die auf ein virtuelles Band geschrieben wurden, finden Sie unter CreateTapes in der AWS Storage Gateway API-Referenz zu .

Beachten Sie AWS KMS bei der Verschlüsselung Ihrer Daten Folgendes:

- Ihre Daten werden im Ruhezustand in der Cloud verschlüsselt. Das bedeutet, dass die Daten in Amazon S3 verschlüsselt werden.
- IAM-Benutzer müssen über die erforderlichen Berechtigungen verfügen, um die AWS KMS -API-Operationen aufzurufen. Weitere Informationen finden Sie unter Verwenden von IAM-Richtlinien mit AWS KMS im Entwicklerhandbuch zu AWS Key Management Service .
- Wenn Sie Ihren AWS AWS KMS Schlüssel löschen oder deaktivieren oder das Erteilungs-Token widerrufen, können Sie nicht auf die Daten auf dem Volume oder Band zugreifen. Weitere Informationen finden Sie unter Löschen von KMS-Schlüsseln im Entwicklerhandbuch zu AWS Key Management Service .
- Wenn Sie einen Snapshot von einem Volume erstellen, das KMS-verschlüsselt ist, wird der Snapshot verschlüsselt. Der Snapshot erbt den KMS-Schlüssel des Volumes.
- Wenn Sie ein neues Volume aus einem KMS-verschlüsselten Snapshot erstellen, wird der Snapshot verschlüsselt. Sie können einen anderen KMS-Schlüssel für das neue Volume angeben.

> **Note**
>
> Storage Gateway unterstützt derzeit nicht das Erstellen eines unverschlüsselten Volumes von einem Wiederherstellungspunkt eines KMS-verschlüsselten Volumes oder eines KMS-verschlüsselten Snapshots.

Weitere Informationen zu AWS KMS finden Sie unter Was ist AWS Key Management Service?

Identity and Access Management für AWS Storage Gateway

AWS Identity and Access Management (IAM) ist ein AWS-Service , mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer für die Nutzung von AWS SGW-Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service , den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in AWS SGW.

Service-Benutzer – Wenn Sie den AWS SGW-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere AWS SGW-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung für AWS Storage Gateway-Identität und -Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS SGW haben.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für AWS SGW-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf AWS SGW. Ihre Aufgabe besteht darin, zu bestimmen, auf welche AWS SGW-Funktionen und -Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit AWS SGW verwenden kann, finden Sie unter Funktionsweise von AWS Storage Gateway mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS SGW verfassen können. Beispiele

für identitätsbasierte AWS SGW-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Storage Gateway.

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten bei anmelden. Sie müssen als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (bei angemeldet AWS) sein.

Sie können sich bei AWS als Verbundidentität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt werden. AWS IAM Identity Center (IAM Identity Center)-Benutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie AWS über einen Verbund auf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, um welchen Benutzertyp es sich handelt, können Sie sich bei der AWS Management Console oder im - AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung bei AWS finden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung - Benutzerhandbuch.

Wenn Sie AWS programmgesteuert auf zugreifen, AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (Command Line Interface, CLI) bereit, um Ihre Anforderungen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenständigen Signieren von Anforderungen finden Sie unter Signieren von AWS API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. empfiehlt beispielsweise, AWS Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto

Root-Benutzer bezeichnet und Sie melden sich mit der E-Mail-Adresse und dem Passwort an, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Fordern Sie als bewährte Methode menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, auf, den Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen auf zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, die AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit AWS-Services Anmeldeinformationen auf zugreift, die über eine Identitätsquelle bereitgestellt werden. Wenn Verbundidentitäten auf zugreifen AWS-Konten, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen oder eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie für alle Ihre AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche

Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI - oder AWS -API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können AWS-Services Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden

Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anfragen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder -Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, 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.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff in , AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anfügen. Eine Richtlinie ist ein Objekt in , AWS das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus der AWS Management Console, der AWS CLI oder der AWS -API abrufen.

Identitätsbasierte Richtlinien

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 Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die

Sie mehreren Benutzern, Gruppen und Rollen in Ihrem anfügen können AWS-Konto. Verwaltete Richtlinien umfassen - AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

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

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services AWS WAF, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter Zugriffssteuerungsliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze

für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service-Kontrollrichtlinien (SCPs)– SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik zur Richtlinienbewertung im IAM-Benutzerhandbuch.

Funktionsweise von AWS Storage Gateway mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf AWS SGW zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit AWS SGW verwenden können.

IAM-Funktionen, die Sie mit AWS Storage Gateway verwenden können

IAM-Feature	AWS SGW-Unterstützung
Identitätsbasierte Richtlinien	Ja
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 Überblick über das Zusammenwirken von AWS SGW und anderen - AWS Services mit den meisten IAM-Funktionen finden Sie unter -AWS Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für AWS SGW

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 Erstellen von IAM-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. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. 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 AWS SGW

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

Ressourcenbasierte Richtlinien in AWS SGW

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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen 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. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen befinden AWS-Konten, muss ein IAM-Administrator im vertrauenswürdigen Konto der Prinzipal-Entität (Benutzer oder Rolle) auch die Berechtigung für den Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal

in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS SGW

Unterstützt Richtlinienaktionen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben in der Regel denselben Namen wie die zugehörige AWS API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS SGW-Aktionen finden Sie unter Von AWS Storage Gateway definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in AWS SGW verwenden das folgende Präfix vor der Aktion:

```
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 AWS Storage Gateway.

Richtlinienressourcen für AWS SGW

Unterstützt Richtlinienressourcen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS SGW-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Storage Gateway definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen 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 AWS Storage Gateway.

Richtlinienbedingungsschlüssel für AWS SGW

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. 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.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der AWS SGW-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Storage Gateway in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen 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 AWS Storage Gateway.

ACLs in AWS SGW

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS SGW

Unterstützt ABAC (Tags in Richtlinien)	Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und viele AWS Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

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 Was ist ABAC? 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 AWS SGW

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der , die mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich AWS Management Console mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn

Sie beispielsweise AWS über den SSO-Link (Single Sign-On) Ihres Unternehmens auf zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell mit der AWS CLI oder der AWS API erstellen. Sie können diese temporären Anmeldeinformationen dann verwenden, um auf zuzugreifen AWS. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Weiterleiten von Zugriffssitzungen für AWS SGW

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS SGW

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**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die AWS SGW-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn AWS SGW dazu Anleitungen gibt.

Serviceverknüpfte Rollen für AWS SGW

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. 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 AWS Storage Gateway

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von AWS SGW-Ressourcen. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von AWS SGW definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Storage Gateway in der Service-Autorisierungs-Referenz.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS SGW-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden 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. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die -AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle 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 für Ihre Anwendungsfälle spezifisch sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen 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 Service-Aktionen zu gewähren, wenn sie über eine bestimmte verwendet werden AWS-Service, z. B. AWS CloudFormation. 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 zum 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 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 Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der AWS SGW-Konsole

Um auf die AWS Storage Gateway-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS SGW-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. 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.

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen für die Konsole erteilen. 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 weiterhin die AWS SGW-Konsole verwenden können, fügen Sie den Entitäten auch die von 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 enthält Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder AWS API.

```
{
```

```
    "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 für AWS Storage Gateway-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit AWS SGW und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in AWS SGW auszuführen
- Ich bin nicht autorisiert, iam durchzuführen:PassRole

- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine AWS SGW-Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in AWS SGW auszuführen

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 autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS SGW übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder serviceverknüpfte 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.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine AWS SGW-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob AWS SGW diese Funktionen unterstützt, finden Sie unter Funktionsweise von AWS Storage Gateway mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen in Ihrem Besitz finden AWS-Konten Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten im IAM-Benutzerhandbuch.
- 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 So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Protokollierung und Überwachung in AWS Storage Gateway

Storage Gateway ist in integriert AWS CloudTrail. Dieser Service zeichnet die Aktionen eines Benutzers, einer Rolle oder eines AWS -Services in Storage Gateway auf. CloudTrail erfasst alle API-Aufrufe für Storage Gateway als Ereignisse. Die erfassten Aufrufe enthalten Aufrufe von der Storage-Gateway-Konsole und Code-Aufrufe der Storage-Gateway-API-Operationen. Wenn Sie

einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Storage Gateway . Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an Storage Gateway gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

Storage Gateway-Informationen in CloudTrail

CloudTrail wird beim Erstellen des Kontos in Ihrem Amazon Web Services-Konto aktiviert. Wenn eine Aktivität in Storage Gateway auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen - AWS Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihrem Amazon Web Services-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem Amazon-Web-Services-Konto, einschließlich Ereignissen für Storage Gateway, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon 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 Services konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle Storage-Gateway-Aktionen werden protokolliert und im Thema Aktionen dokumentiert. Aufrufe der `ShutdownGateway` Aktionen `ActivateGateway`, `ListGateways`und erzeugen beispielsweise 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 Anforderung mit Root- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung von einem anderen - AWS Service gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Informationen zu Storage-Gateway-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die Aktion demonstriert.

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
```

```
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                    "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
             }]
}
```

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die 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"
              }]
}
```

Compliance-Validierung für AWS Storage Gateway

Externe Prüfer bewerten im Rahmen verschiedener AWS -Compliance-Programme die Sicherheit und Compliance von AWS Storage Gateway. Dazu gehören SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR und HITRUST CSF.

Eine Liste der - AWS Services, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie unter AWS -Services im Geltungsbereich nach Compliance-Programm Allgemeine Informationen finden Sie unter AWS Compliance-Programme

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten unter AWS Artifact .

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:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte für die Bereitstellung von Sicherheits- und Compliance-orientierten Basisumgebungen in beschrieben AWS.
- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe AWS von HIPAA-konforme Anwendungen erstellen können.
- AWS Compliance-Ressourcen – Diese Sammlung von Arbeitsmappen und Leitfäden könnte für Ihre Branche und Ihren Standort gelten.
- Bewertung von Ressourcen mit Regeln im -AWS Config Entwicklerhandbuch – Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- AWS Security Hub – Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS , mit dem Sie Ihre Compliance mit den Sicherheitsstandards und bewährten Methoden der Branche überprüfen können.

Ausfallsicherheit in AWS Storage Gateway

Die AWS globale -Infrastruktur ist um - AWS Regionen und Availability Zones herum aufgebaut. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit hoch redundanten Netzwerken mit niedriger Latenz und hohem Durchsatz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen -Infrastruktur stellt Storage Gateway verschiedene Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden:

- Verwenden Sie VMware vSphere High Availability (VMware HA), um Speicher-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen zu schützen. Weitere Informationen finden Sie unter Verwenden von VMware vSphere High Availability mit Storage Gateway.
- Archivieren Sie virtuelle Bänder in S3 Glacier Flexible Retrieval. Weitere Informationen finden Sie unter Archivierung virtueller Bänder.

Infrastruktursicherheit in AWS Storage Gateway

Als verwalteter Service ist AWS Storage Gateway durch die AWS globalen Verfahren zur Gewährleistung der Netzwerksicherheit von geschützt, die im Whitepaper Amazon Web Services: Übersicht über die Sicherheitsprozesse beschrieben sind.

Sie verwenden durch 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.

AWS Bewährte Methoden für die Sicherheit

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.

Fehlerbehebung bei Ihrem Gateway

In den folgenden Abschnitten erhalten Sie Informationen zur Fehlerbehebung bei Problemen im Zusammenhang mit Gateways, Dateifreigaben, Volumes, virtuellen Bändern und Snapshots. Die lokalen Gateway Informationen zur Fehlerbehebung decken Gateways ab, die sowohl auf der VMware ESXi als auch auf den Microsoft Hyper-V Clients bereitgestellt sind. Die Informationen zur Fehlerbehebung für Dateifreigaben gelten für den File-Gateway-Typ. Die Informationen zur Fehlerbehebung für Volumes gelten für den Volume-Gateway-Typ. Die Informationen zur Fehlerbehebung für Bänder gelten für den Tape-Gateway-Typ. Die Informationen zur Fehlerbehebung bei Gateway-Problemen gelten für die Verwendung von - CloudWatch Metriken. Die Informationen zur Fehlerbehebung für Probleme im Zusammenhang mit hoher Verfügbarkeit beziehen sich auf Gateways, die auf der VMware vSphere High Availability(HA)-Plattform ausgeführt werden.

Themen

Fehlerbehebung bei lokalen Gateway-Problemen

Im Folgenden finden Sie Informationen zu typischen Problemen, die bei der Arbeit mit Ihren On-Premises-Gateways auftreten können, und wie Sie aktivieren können, AWS Support um die Fehlerbehebung für Ihr Gateway 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. • Für die VMware ESXi kann die IP-Adresse der VM im vSphere-Client auf der Registerkarte Übersicht gefunden werden. • Für Microsoft Hyper-V, kann die IP-Adresse der VM's gefunden werden, indem man sich auf der lokalen Konsole anmeldet. Wenn Sie immer noch Probleme haben die Gateway-IP-Adresse zu ermitteln: • Stellen Sie sicher, dass der VM aktiviert ist. Nur wenn die VM aktiviert ist, wird dem Gateway eine IP-Adresse zugewiesen. • Warten Sie bis die VM den Startup abgeschlossen hat. Wenn Sie Ihre VM gerade erst aktiviert haben, kann es einige Minuten dauern, bis die Gateways mit der Boot-Sequenz abschließen.
Sie haben Netzwerk- oder Firewall-Probleme.	• Erteilen Sie dem Gateway die Zugriffserlaubnis für die entsprechenden Ports. • Die Überprüfung von SSL-Zertifikaten sollte nicht aktiviert sein. Storage Gateway verwendet eine gegenseitige TLS-Authentifizierung, die fehlschlägt, wenn eine Drittanbieteranwendung versucht, eines der Zertifikate abzufangen/zu signieren. • 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,	• Überprüfen Sie, dass auf die Gateway-VM zugegriffen werden kann, indem Sie die VM Ihres Clients anpingen.

Problem	Maßnahme
wenn Sie in der Storage-Gateway-Managementk onsole auf die Schaltflä che Weiter zur Aktivierung klicken.	• Stellen Sie sicher, dass Ihre VM eine Netzwerkverbindung zum Internet hat. Andernfalls müssen Sie die Konfiguration eines SOCKS-Proxy vornehmen. Weitere Informationen zur Verfahren sweise finden Sie unter Weiterleiten Ihres lokalen Gateways über einen Proxy. • Stellen Sie sicher, dass die Uhrzeit des Hosts richtig eingestellt ist, dass der Host so konfiguriert ist, dass er die Uhrzeit automatis ch mit einem Network Time Protocol (NTP) Server synchroni siert und dass die Gateway-VM auf die richtige Uhrzeit eingestel lt ist. Weitere Informationen zum Synchronisieren der Uhrzeit des Hypervisor-Hosts und der VMs finden Sie unter Synchronisieren der Gateway-VM-Zeit. • 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. • Die Überprüfung von SSL-Zertifikaten sollte nicht aktiviert sein. Storage Gateway verwendet eine gegenseitige TLS-Authentifizier ung, die fehlschlägt, wenn eine Drittanbieteranwendung versucht, eines der Zertifikate abzufangen/zu signieren. • Stellen Sie sicher, dass Ihre VM über mindestens 7,5 GB RAM verfügen. Die Gateway-Zuweisung schlägt fehl, wenn es weniger als 7,5 GB RAM zur Verfügung stehen. Weitere Informationen finden Sie unter Voraussetzungen.

Problem	Maßnahme
Entfernen Sie eine als Upload-Pufferspeicher zugewiesene Festplatte. Beispielsweise möchten Sie die Anzahl der Upload-Pufferspeicher für ein Gateway reduzieren oder eine Festplatte ersetzen, die als fehlgeschlagener Puffer verwendet wurde.	Anweisungen zum Entfernen eines Datenträgers, der als Upload-Pufferspeicherplatz zugewiesen ist, finden Sie unter Entfernen von Datenträgern aus dem Gateway.
Sie müssen die Bandbreite zwischen Ihrem Gateway und AWS verbessern.	Sie können die Bandbreite von Ihrem Gateway zu verbessern, AWS indem Sie Ihre Internetverbindung zu AWS auf einem Netzwerkadapter (NIC) einrichten, der getrennt von der ist, die Ihre Anwendungen und die Gateway-VM verbindet. Dieser Ansatz ist nützlich, wenn Sie eine Verbindung mit hoher Bandbreite zu haben AWS und Bandbreitenkonflikte vermeiden möchten, insbesondere während einer Snapshot-Wiederherstellung. Für Workloads mit hohem Durchsatz können Sie AWS Direct Connect verwenden, um eine dedizierte Netzwerkverbindung zwischen dem lokalen Gateway und AWS herzustellen. Um die Bandbreite der Verbindung von Ihrem Gateway zu zu messen AWS, verwenden Sie die `CloudBytesUploaded` Metriken `CloudBytesDownloaded` und des Gateways. Weitere Informationen zu diesem Thema finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS. 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 sicher, dass auf der Registerkarte Gateway der Storage-Gateway-Konsole die IP-Adressen für Ihre Gateway-VM identisch mit Ihrer Hypervisor-Clientsoftware sind (VMware vSphere-Client oder Microsoft Hyper-V-Manager). Wenn Sie eine Nichtübereinstimmung finden, starten Sie das Gateway über die Storage-Gateway-Konsole neu, wie unter Herunterfahren der Gateway-VM 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.
	  • Für die VMware ESXi kann die IP-Adresse der VM im vSphere-Client auf der Registerkarte Übersicht gefunden werden.
	  • 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 zu , AWS wie unter beschriebenTesten der Gateway-Internetverbindung.
	• Prüfen Sie die Netzwerkadapterkonfiguration des Gateways und stellen Sie sicher, dass alle Schnittstellen, die Sie für das Gateway aktivieren möchten, aktiviert sind. Um die Netzwerka dapter Konfiguration Ihres Gateways anzuzeigen, befolgen Sie die Anweisungen in Konfigurieren Ihres Gateway-Netzwerks und wählen Sie die Option die die Netzwerkkonfiguration Ihres Gateway anzeigt.
	
	Sie können den Durchsatz zu und von Ihrem Gateway über die Amazon- CloudWatch Konsole anzeigen. Weitere Informationen zur Messung des Durchsatzes zu und von Ihrem Gateway und finden Sie AWS unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

Problem	Maßnahme
Sie haben Schwierig keiten mit dem Importieren (Bereitstellen) von Storage Gateway auf Microsoft Hyper-V.	Weitere Informationen finden Sie unter Fehlerbehebung bei der Einrichtung von Microsoft Hyper-V, 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 AWS Support.

Erlauben AWS Support von zur Fehlerbehebung Ihres lokal gehosteten Gateways

Storage Gateway bietet eine lokale Konsole, mit der Sie mehrere Wartungsaufgaben ausführen können, einschließlich der Aktivierung von AWS Support für den Zugriff auf Ihr Gateway, um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Standardmäßig ist der AWS Support Zugriff auf Ihr Gateway deaktiviert. Dieser Zugriff wird über die lokale Host-Konsole gewährt. Um AWS 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.

So erlauben Sie AWS Support den Zugriff auf Ihr Gateway

1. Melden Sie sich bei der lokalen Konsole Ihres Hosts an.
   - VMware ESXi: Weitere Informationen finden Sie unter Zugreifen auf die lokale 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:

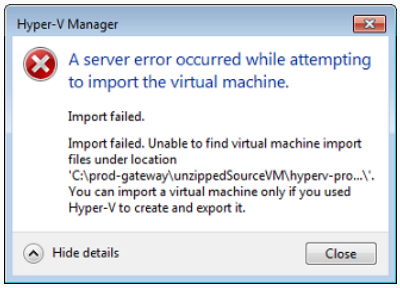
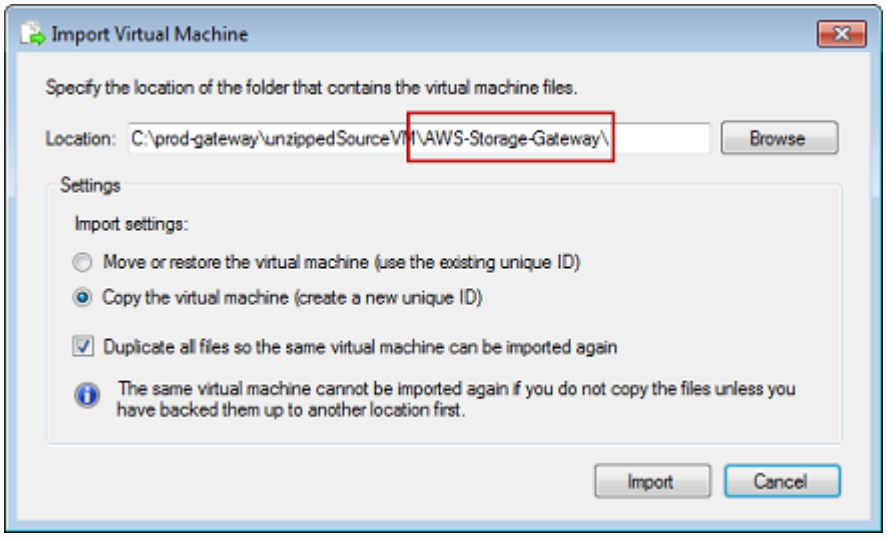
   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, geben Sie im Fenster VERFÜGBARE BEFEHLE **`open-support-channel`** ein, um eine Verbindung zum Storage-Gateway-Kundensupport herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. Wenn Sie eine Verbindung 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.

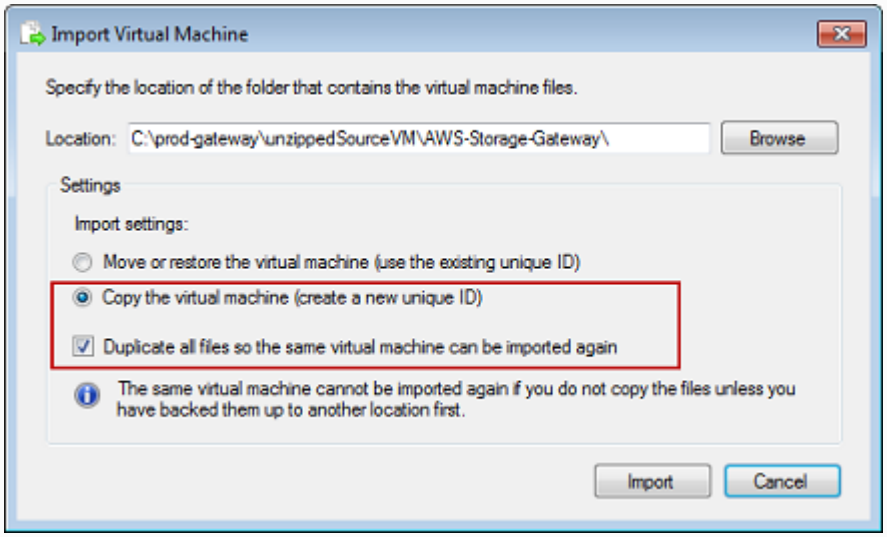
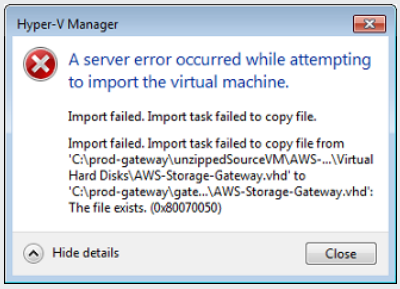
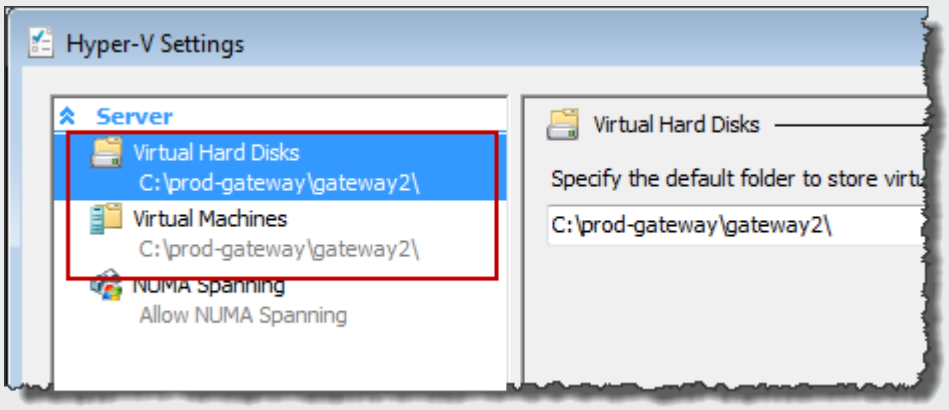
   > **Note**
   >
   > Die Kanalnummer ist keine Transmission Control Protocol/User Datagram Protocol (TCP/UDP) Portnummer. Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP 22)-Verbindung zu den Storage-Gateway-Servern her und stellt den Support-Kanal für die Verbindung bereit.

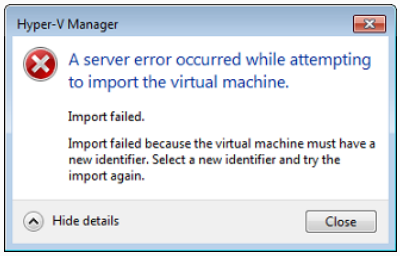
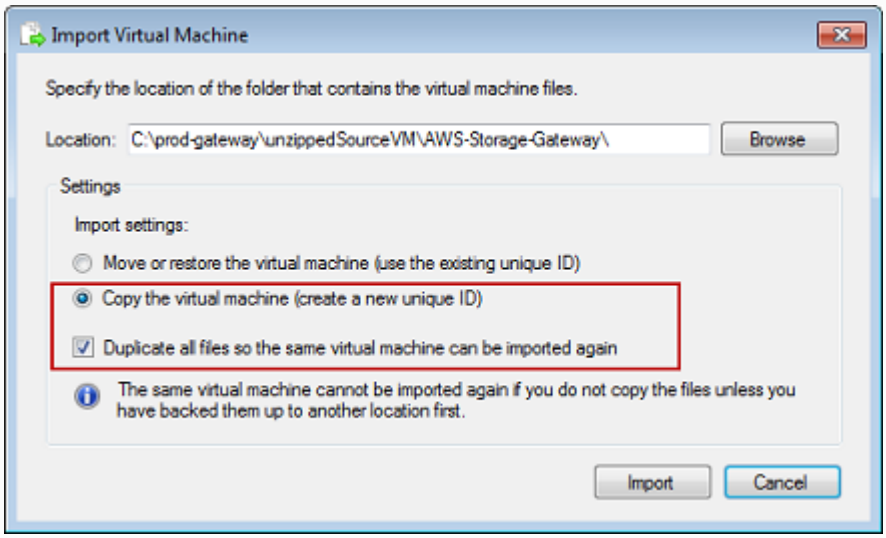
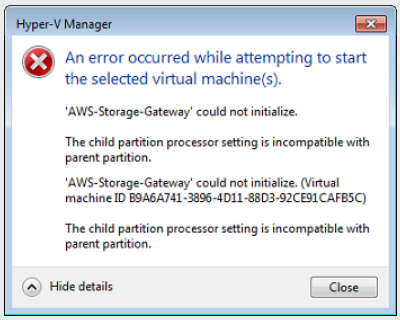
5. Nachdem der Support-Kanal eingerichtet wurde, geben Sie Ihre Support-Servicenummer an, AWS Support damit Unterstützung bei der Fehlerbehebung bieten AWS Support kann.
6. Wenn die Supportsitzung beendet ist, geben Sie **`q`** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn Sie vom Amazon Web Services Support darüber informiert werden, dass die Support-Sitzung abgeschlossen ist.
7. Geben Sie **`exit`** ein, um sich von der Gateway-Konsole abzumelden.
8. Folgen Sie den Eingabeaufforderungen, um die lokale Konsole zu beenden.

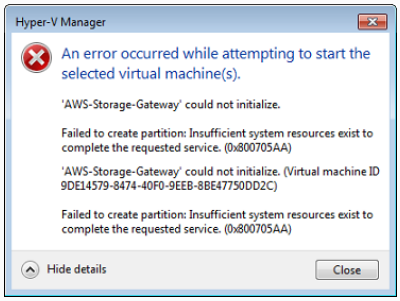
Fehlerbehebung bei der Einrichtung von Microsoft Hyper-V

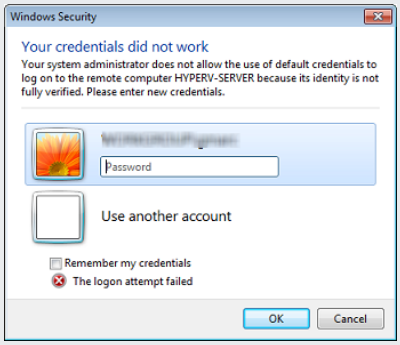
In der folgenden Tabelle sind typische Probleme aufgeführt, die beim Bereitstellen von Storage Gateway auf der Microsoft Hyper-V-Plattform auftreten können.

Problem	Maßnahme
Sie versuchen, ein Gateway zu importieren und erhalten die Fehlermeldung: „Import ist fehlgeschlagen. Die Import-Datei der Virtuellen Maschine wird unter Standort nicht gefunden...“. 	Dieser Fehler kann aus folgenden Gründen auftreten: • Wenn Sie nicht auf das Stammverzeichnis der entpackten Gateway-Quell-Dateien zeigen. Der letzte Teil des angegebenen Speicherorts im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) sollte `AWS-Storage-Gateway` lauten, wie im folgenden Beispiel dargestellt:  • Wenn Sie bereits ein Gateway bereitgestellt haben, die Option Copy the virtual machine (virtuelle Maschine kopieren) nicht ausgewählt ist und Sie die Option Duplicate all files (Alle Dateien duplizieren) im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) markiert haben, dann wurde die VM an dem Speicherort erstellt, an dem Sie die Dateien entpackt haben, und Sie können nicht erneut von dort importieren. Zur Behebung dieses Problems, erwerben Sie eine neue Kopie der entpackten Gateway Quell-Dateien und kopieren Sie diese an einen neuen Speicherort. Verwenden Sie den neuen Speicherort als Importquelle. Das folgende Beispiel zeigt die Optionen, die Sie überprüfe

Problem	Maßnahme
	n müssen, wenn Sie aus einem entpackten Quelldateien-Speic herort mehrere Gateways erstellen möchten. 
Sie versuchen, ein Gateway zu importieren und erhalten die Fehlermel dung: „Import ist fehlgesch lagen. Import Aufgabe zur Kopie der Datei fehlgesch lagen. 	Wenn Sie bereits ein Gateway bereitgestellt haben und Sie versuchen den Standard-Ordner wiederzuverwenden, der die virtuelle Festplatten Dateien und die virtuelle Maschinen-Konfigur ationsdateien speichert, wird dieser Fehler auftreten. Zur Behebung dieses Problems geben Sie neue Speicherorte im Dialogfeld Hyper-V Settings (Hyper-V-Einstellungen) an. 

Problem	Maßnahme
Sie versuchen, ein Gateway zu importieren und erhalten die Fehlermeldung: „Import fehlgeschlagen. Der Import ist fehlgeschlagen, da die virtuelle Maschine über eine neue ID verfügen muss. Wählen Sie eine ID und versuchen Sie erneut zu importieren.“ 	Wenn Sie das Gateway importieren, stellen Sie sicher, dass Sie die Option Copy the virtual maschine (Virtuelle Maschine kopieren) und die Option Duplicate all files (Alle Dateien duplizieren) im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) auswählen , um eine neue eindeutige ID für die VM zu erstellen. Das folgende Beispiel zeigt die Optionen im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren), die Sie verwenden sollten. 
Sie versuchen, eine Gateway-VM zu starten und erhalten die Fehlermeldung erhalten: „Die untergeordnete Partitions-Prozessor-Einstellung ist nicht kompatibel mit der übergeordneten Partition.“ 	Dieser Fehler wird wahrscheinlich durch eine CPU-Abweichungen zwischen den erforderlichen CPUs für das Gateway und den verfügbaren CPUs auf dem Host verursacht. Stellen Sie sicher, dass die VM-CPU-Inventur von der zugrunde liegenden Hypervisor unterstützt wird. Weitere Informationen zu den Anforderungen für Storage Gateway finden Sie unter Voraussetzungen.

Problem	Maßnahme
Sie versuchen, eine Gateway-VM zu starten und erhalten die Fehlermeldung: "Fehler beim Erstellen der Partition: Nicht genügend Ressourcen vorhanden, um den angeforderten Dienst auszuführen." 	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 Voraussetzungen.
Ihre Snapshots und Gateway-Software-Aktualisierungen treten zu geringfügig anderen Zeiten als erwartet auf.	Die Uhr der Gateway-VM, weicht möglicherweise von der tatsächlichen Uhrzeit ab, dies wird als Ganggenauigkeit bezeichnet. Überprüfen und korrigieren Sie die Uhrzeit der VM, indem Sie die Option Synchronisierung der lokalen Gateway-Konsole verwenden. Weitere Informationen finden Sie unter Synchronisieren der Gateway-VM-Zeit.
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 Hypervisor herstellen. 	Fügen Sie Ihre Benutzer-Anmeldeinformationen als lokaler Administrator für den Hypervisor-Host mithilfe des Sconfig.cmd Tool hinzu.
Möglicherweise stellen Sie eine schlechte Netzwerkleistung fest, wenn Sie die Virtual Machine Queue (VMQ) auf einem Hyper-V-Host aktivieren, der einen Broadcom-Netzwerkadapter verwendet.	Informationen zu einer Problemumgehung finden Sie in der Microsoft-Dokumentation zum Thema Schlechte Netzwerkleistung auf virtuellen Maschinen auf einem Windows Server 2012 Hyper-V-Host, wenn VMQ aktiviert ist.

Fehlerbehebung bei Problemen mit Amazon-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 Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Tape Gateway.

Themen

- Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.
- EC2-Gateway-Instance in der Instance-Liste nicht gefunden

- Sie haben ein Amazon-EBS-Volume erstellt, können es aber nicht an die EC2-Gateway-Instance anfügen
- Beim Hinzufügen von Speicher-Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind
- Sie möchten einen als Upload-Pufferspeicher zugewiesenen Datenträger entfernen, um die Größe des Upload-Pufferspeichers zu reduzieren
- Durchsatz zum oder vom EC2-Gateway sinkt auf Null
- Sie möchten AWS Support bei der Fehlerbehebung Ihres EC2-Gateways helfen
- Sie möchten sich mit Ihrer Gateway-Instance über die serielle Amazon-EC2-Konsole verbinden

Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.

Prüfen Sie in der Amazon-EC2-Konsole Folgendes:

- Port 80 ist in der Sicherheitsgruppe aktiviert, die Sie mit der Instance verknüpft haben. Weitere Informationen über das Hinzufügen von Sicherheitsgruppenregeln finden Sie unter Hinzufügen von Sicherheitsgruppenregeln im Amazon-EC2-Benutzerhandbuch für Linux-Instances.
- 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 haben ein Amazon-EBS-Volume erstellt, können es aber nicht an die EC2-Gateway-Instance anfügen

Stellen Sie sicher, dass sich dieses Amazon-EBS-Volume in derselben Availability Zone wie die Gateway-Instance befindet. Falls eine Abweichung in den Availability Zones besteht, erstellen Sie ein neues Amazon-EBS-Volume, das sich in derselben Availability Zone wie die Instance befindet.

Beim Hinzufügen von Speicher-Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind

Für ein neu aktiviertes Gateway ist kein Volume-Speicher definiert. Bevor Sie Volume-Speicher definieren können, müssen Sie die lokale Festplatten zum Gateway zuweisen, die Sie als Upload-Puffer und Cache-Speicher verwenden. Für ein Gateway, das auf Amazon EC2 bereitgestellt ist, entsprechen die lokalen Datenträger Amazon-EBS-Volumes, die an die Instance angefügt sind. Dieser Fehler tritt wahrscheinlich auf, weil keine Amazon-EBS-Volumes für die Instance definiert sind.

Prüfen Sie Block-Geräte, die für die Instance definiert sind, die das Gateway ausführt. Wenn es nur zwei Block-Geräte (Geräte mit der Standard-AMI) gibt, dann sollten Sie Speicher hinzufügen. Weitere Informationen zur Verfahrensweise finden Sie unter Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Tape Gateway. Nachdem Sie zwei oder mehr Amazon-EBS-Volumes angefügt haben, versuchen Sie, den Volume-Speicher im Gateway zu erstellen.

Sie möchten einen als Upload-Pufferspeicher zugewiesenen Datenträger entfernen, um die Größe des Upload-Pufferspeichers zu reduzieren

Führen Sie die Schritte unter Bestimmen der Größe des zuzuordnenden Upload-Puffers aus.

Durchsatz zum oder vom EC2-Gateway sinkt auf Null

Verifizieren Sie, dass die Gateway-Instance ausgeführt wird. Wenn die Instance gestartet wird, z. B. durch einen Neustart, warten Sie, bis die Instance neu gestartet ist.

Verifizieren Sie außerdem, dass sich die Gateway-IP-Adresse nicht geändert hat. Wenn die Instance beendet wurde und anschließend neu gestartet wurde, hat sich die IP-Adresse der Instance möglicherweise geändert. In diesem Fall müssen Sie ein neues Gateway aktivieren.

Sie können den Durchsatz zu und von Ihrem Gateway über die Amazon- CloudWatch Konsole anzeigen. Weitere Informationen zur Messung des Durchsatzes zu und von Ihrem Gateway und finden Sie AWS unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

Sie möchten AWS Support bei der Fehlerbehebung Ihres EC2-Gateways helfen

Storage Gateway bietet eine lokale Konsole, mit der Sie mehrere Wartungsaufgaben ausführen können, einschließlich der Aktivierung von AWS Support für den Zugriff auf Ihr Gateway, um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Standardmäßig ist der AWS Support Zugriff auf Ihr Gateway deaktiviert. Sie aktivieren diesen Zugriff über die lokale Amazon-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 AWS Support Verbindung zu Ihrem Gateway herstellen zu können, melden Sie sich zunächst bei der lokalen Konsole für die Amazon EC2-Instance an, navigieren zur Konsole des Storage Gateways und geben dann den Zugriff an.

So aktivieren Sie den AWS Support Zugriff auf ein Gateway, das auf einer Amazon EC2-Instance bereitgestellt wird

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**
>
> Der *PRIVATE KEY* ist die `.pem`-Datei, die das private Zertifikat des EC2-Schlüsselpaars besitzt, das Sie zum Starten der Amazon–EC2-Instance verwendet haben. Weitere Informationen finden Sie unter Abrufen des öffentlichen Schlüssels für Ihr Schlüsselpaar im Amazon-EC2-Benutzerhandbuch.
> *INSTANCE-PUBLIC-DNS-NAME* ist der öffentliche DNS-Name (Domain Name System) Ihrer Amazon-EC2-Instance, auf der Ihr Gateway ausgeführt wird. 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 AWS 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 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) Portnummer. 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, AWS Support damit Unterstützung bei der Fehlerbehebung bieten AWS Support kann.
6. Wenn die Supportsitzung beendet ist, geben Sie **q** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn Sie AWS Support benachrichtigt, 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.

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.

Fehlerbehebung bei Hardware-Appliance-Problemen

In den folgenden Themen werden Probleme, die im Zusammenhang mit der Hardware-Appliance für Storage Gateway auftreten können, sowie Lösungsvorschläge beschrieben.

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 die Appliance auf die Werkseinstellungen zurücksetzen müssen, wenden Sie sich an das Hardware-Appliance-Team für Storage Gateway, um wie im folgenden Support-Abschnitt beschrieben Unterstützung zu erhalten.

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 iDRAC9 Virtual Power Bol: Remotely Power cycle Dell EMC PowerEdge Servers auf der Dell Technologies- InfoHub Website.

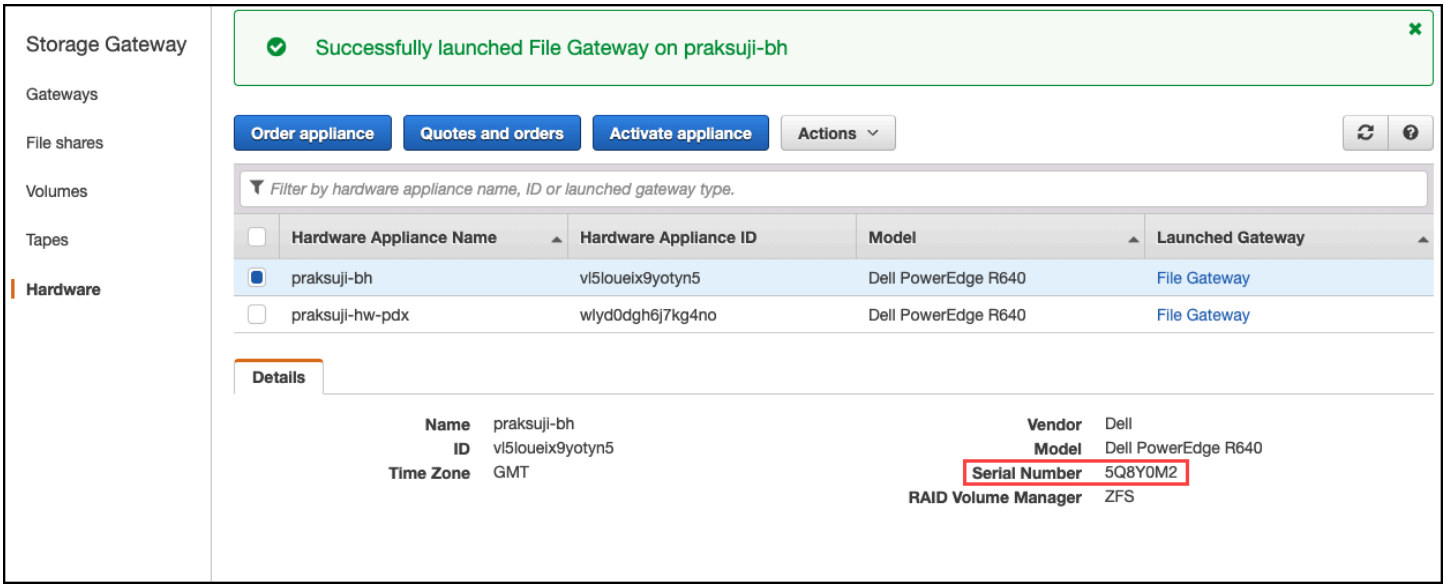
Wo erhalten Sie Dell iDRAC-Support?

Der Dell PowerEdge R640-Server verfügt über die Dell iDRAC-Verwaltungsschnittstelle. Wir empfehlen Folgendes:

- Wenn Sie die iDRAC-Verwaltungsschnittstelle verwenden, sollten Sie das Standardkennwort ändern. Weitere Informationen zu den iDRAC PowerEdge -Anmeldeinformationen finden Sie unter Dell – Was sind die Standardanmeldeinformationen für iDRAC?.
- Stellen Sie sicher, dass die Firmware Sicherheitsverstöße 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

Um die Seriennummer der Hardware-Appliance zu finden, rufen Sie die Seite Hardware-Appliance-Übersicht wie im Folgenden beschrieben in der Storage-Gateway-Konsole auf.
Hardware-Registerkarte der Storage-Gateway-Konsole mit ausgewählter Appliance und angezeigten Details.



Hardware-Registerkarte der Storage-Gateway-Konsole mit ausgewählter Appliance und angezeigten Details.

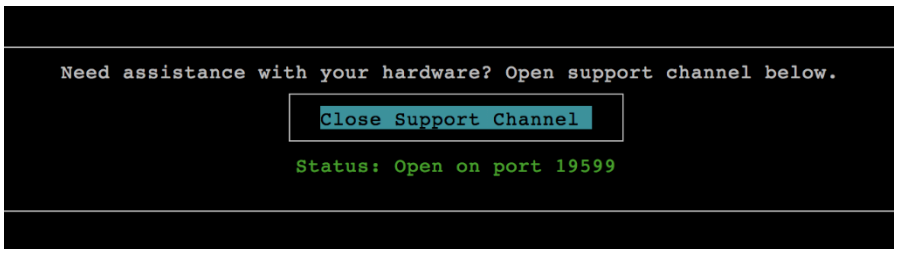
Wo Sie Hardware-Appliance-Support erhalten?

Informationen zur Kontaktaufnahme mit dem Hardware-Appliance-Support für Storage Gateway finden Sie unter AWS Support.

Das AWS Support Team bittet Sie möglicherweise, den Support-Kanal zu aktivieren, um Ihre Gateway-Probleme remote zu beheben. Dieser Port muss für den normalen Betrieb des Gateways nicht offen sein, für die Fehlerbehebung ist dies jedoch erforderlich. Sie können den Support-Kanal über die Hardware-Konsole aktivieren, wie im folgenden Verfahren dargestellt.

So öffnen Sie einen Support-Kanal für AWS

1. Öffnen Sie die Hardwarekonsole.
2. Wählen Sie Open Support Channel (Support-Kanal öffnen), wie im Folgenden dargestellt. Hardware-Appliance-Konsole, auf der der Status des Support-Kanals angezeigt wird



Hardware-Appliance-Konsole, auf der der Status des Support-Kanals angezeigt wird

Die zugewiesene Portnummer sollte innerhalb von 30 Sekunden angezeigt werden, sofern keine Probleme mit der Netzwerkverbindung oder der Firewall bestehen.

3. Notieren Sie sich die Portnummer und stellen Sie sie bereit AWS Support.

Beheben von Problemen mit virtuellen Bändern

Informationen über die Aktionen die Sie vornehmen können, wenn Sie unerwartete Probleme mit Ihren virtuellen Bändern haben.

Themen

Wiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway

Obwohl ist es selten vorkommt, könnte in Ihrem Tape Gateway ein schwerwiegender Fehler auftreten. Solche Fehler können in Ihrer Hypervisor-Host, dem Gateway selbst oder in der Cache-Festplatte auftreten. Wenn ein Fehler auftritt, können Sie Ihre Bänder wiederherstellen. Befolgen Sie hierzu die Anweisungen zur Fehlerbehebung in diesem Abschnitt.

Themen

Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen.

Wenn bei Ihrem Tape Gateway oder dem Hypervisor-Host ein nicht behebbarer Fehler auftritt, können Sie alle Daten wiederherstellen, die bereits AWS auf ein anderes Tape Gateway hochgeladen wurden.

Beachten Sie, dass die Daten die auf ein Band geschrieben wurden nicht vollständig hochgeladen sein müssen bis dieses Band erfolgreich in VTS archiviert wurde. Die Daten auf den Bändern, die

auf einem anderen Gateway wiederhergestellt worden können unvollständig oder leer sein. Wir empfehlen, einen Bestand für alle wiederhergestellten Bänder vorzunehmen, um sicherzustellen, dass diese die erwarteten Inhalte enthalten.

So stellen Sie ein Band auf einem anderen Tape Gateway wieder her

1. Identifizieren Sie ein vorhandenes funktionierendes Tape Gateway, das als Wiederherstellungs-Ziel-Gateway dient. Wenn Sie über kein Tape Gateway verfügen, auf dem Sie ihre Bänder wiederherstellen können, erstellen Sie ein neues Tape Gateway. Weitere Informationen zum Erstellen eines Gateways finden Sie unter Erstellen eines Gateways.
2. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
3. Wählen Sie im Navigationsbereich erst Gateways und dann dasTape Gateway aus, von dem Sie Ihre Bänder wiederherstellen möchten.
4. Wählen Sie die Registerkarte Details. Eine Nachricht über das wiederhergestellte Band wird in der Registerkarte angezeigt.
5. Wählen Sie Wiederherstellungsbänder erstellen aus, um das Gateway zu deaktivieren.
6. Wählen Sie im angezeigten Dialogfeld Disable gateway (Gateway deaktivieren).

   Damit wird der Betrieb des Tape Gateway dauerhaft angehalten und alle verfügbaren Wiederherstellungspunkte werden bereitgestellt. Anweisungen finden Sie unter Deaktivierung Ihres Tape Gateways.
7. Wählen Sie aus den Bändern, die das deaktivierte Gateway anzeigt, das virtuelle Band und den Wiederherstellungspunkt aus, den Sie wiederherstellen möchten. Eine virtuelles Band kann mehrere Wiederherstellungspunkte haben.
8. Um mit dem Wiederherstellen von Bändern zu beginnen, müssen Sie zum Ziel-Tape-Gateway wechseln und Wiederherstellungsband erstellen wählen.
9. Überprüfen Sie im Dialogfeld Create recovery tape (Wiederherstellungsband erstellen) den Barcode des virtuellen Bands, das wiederhergestellt werden soll.
10. wählen Sie für Gateway das Tape Gateway aus, auf dem Sie das virtuelle Band wiederherstellen möchten.
11. Wählen Sie Create recovery tape (Wiederherstellungsband erstellen).
12. Löschen Sie das fehlerhafte Tape Gateway, damit es Ihnen nicht in Rechnung gestellt wird. Anweisungen finden Sie unter Löschen des Gateways über die AWS Storage Gateway -Konsole und Bereinigen zugehöriger Ressourcen.

Storage Gateway verschiebt das Band vom ausgefallenen Tape Gateway auf das von Ihnen angegebene Tape Gateway. Tape Gateway markiert das Band mit dem Status RECOVERED.

Sie müssen ein virtuelles Band aus einer fehlerhaften Cache-Festplatte wiederherstellen

Wenn in Ihrer Cache-Festplatte ein Fehler auftritt, verhindert das Gateway Lese- und Schreiboptionen auf dem virtuellen Band im Gateway. Beispielsweise kann ein Fehler auftreten, wenn eine Festplatte vom Gateway beschädigt oder entfernt wurde. Die Storage-Gateway-Konsole zeigt eine Meldung über den Fehler an.

In der Fehlermeldung fordert Sie Storage Gateway auf, eine von zwei Aktionen zur Wiederherstellung Ihrer Bänder auszuführen:

- Herunterfahren und erneutes Hinzufügen von Festplatten: Verwenden Sie diesen Ansatz, wenn die Festplatte intakte Daten enthält und entfernt wurde. Wenn der Fehler z. B aufgetreten ist, da der Datenträger versehentlich von Ihrem Host entfernt wurde aber die Festplatte und die Daten intakt sind, können Sie den Datenträger erneut hinzufügen. Um dies durchzuführen, siehe Vorgang zu einem späteren Zeitpunkt in diesem Thema.
- Zurücksetzen der Cache-Festplatte: Wählen Sie diesen Ansatz, wenn die Cache-Festplatte beschädigt oder nicht verfügbar ist. Wenn der Datenträger Fehler bewirkt, dass das Cache nicht verfügbar, beschädigt oder unbenutzbar ist, können Sie die Datenträger zurücksetzen. Wenn Sie die Cache-Festplatte zurücksetzen, werden Bänder, die bereinigte Daten aufweisen (das sind Bänder, für die Daten auf der Cache-Festplatte und in Amazon S3 synchronisiert werden), weiterhin für Sie verfügbar sein. Jedoch werden Bänder, deren Daten nicht mit Amazon S3 synchronisiert werden, automatisch wiederhergestellt. Der Status dieser Bänder ist auf WIEDERBESCHAFFT gesetzt, doch die Bänder sind schreibgeschützt. Weitere Informationen zum Entfernen einer Festplatte aus dem Host finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.

> **Important**
>
> Wenn die Cache-Festplatte, die sie zurücksetzen, Daten enthält, die Sie noch nicht in Amazon S3 hochgeladen haben, können diese Daten verloren gehen. Nachdem Sie den Cache-Datenträger neu gesetzt haben, werden keine konfigurierten Cache-Datenträger im Gateway sein, Sie müssen mindestens einen neuen Cache-Datenträger für Ihr Gateway konfigurieren, damit es richtig funktioniert.

Um den Cache-Datenträger neu zu setzen sehen Sie den Vorgang, der später in diesem Thema auftaucht.

Herunterfahren und das erneute hinzufügen einer Festplatte

1. Fahren Sie das Gateway herunter. Weitere Informationen, wie Sie ein Gateway herunterfahren, finden Sie unter Herunterfahren der Gateway-VM.
2. Fügen Sie die Festplatte an Ihren Host zurück, und stellen Sie sicher, dass die Datenträger Knotennummer des Datenträgers nicht verändert wurde. Weitere Informationen zum Hinzufügen eines Datenträgers finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.
3. Starten Sie Ihr Gateway neu. Weitere Informationen wie Sie ein Gateway neu starten finden Sie unter Herunterfahren der Gateway-VM.

Nachdem das Gateway neu gestartet wurde, können Sie den Status der Cache-Festplatten überprüfen. Der Status eines Datenträgers kann einer der folgenden sein:

- vorhanden - Der Datenträger ist verfügbar.
- fehlend – Der Datenträger ist nicht mehr mit dem Gateway verbunden.
- stimmen nicht überein . Der Datenträger-Knoten ist von einem Datenträger belegt, der falsche Metadaten besitzt oder die Inhalte des Datenträgers sind beschädigt.

Einen Cache-Datenträger neu setzen und neu konfigurieren

1. Wählen Sie in der oben abgebildeten Fehlermeldung A disk error has occurred (Ein Festplattenfehler ist aufgetreten) die Option Reset Cache Disk (Cache-Festplatte zurücksetzen).
2. Konfigurieren Sie auf der Seite Gateway konfigurieren die Festplatte als Cache-Speicher. Informationen zur Vorgehensweise finden Sie unter Konfigurieren von Tape Gateway.
3. Nachdem Sie die Cache-Speicherung konfiguriert haben, fahren Sie das Gateway herunter und starten Sie es erneut, wie im Vorgang oben beschrieben.

Das Gateway sollte nach dem Neustart wiederhergestellt sein. Sie können dann den Status der Cache-Festplatte überprüfen.

So prüfen Sie den Status einer Cache-Festplatte

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Gateways und wählen Sie dann Ihr Gateway.
3. Wählen Sie für Actions (Aktionen) die Option Configure Local Storage (Lokalen Speicher konfigurieren) aus, um das Dialogfeld Configure Local Storage (Lokalen Speicher konfigurieren) anzuzeigen. In diesem Dialogfeld werden alle lokalen Festplatten in der Gateway angezeigt.

Der Cache-Festplatten-Knoten-Status wird neben der Festplatte angezeigt.

> **Note**
>
> Wenn Sie den Wiederherstellungsprozess nicht abschließen, zeigt das Gateway einen Banner an, der Sie auffordert lokalen Speicher zu konfigurieren.

Fehlerbehebung bei nicht wiederherstellbaren Bändern

Wenn Ihr virtuelles Band unerwartet ausfällt, setzt Storage Gateway den Status des fehlgeschlagen Bands zu IRRECOVERABLE. Die Aktion, die Sie durchführen hängt von den Umständen ab. Sie können Informationen zu einigen Themen finden und wie Sie diese möglicherweise beheben können.

Wiederherstellen von Daten von einem Band mit dem Status IRRECOVERABLE

Wenn Sie ein virtuelles Band mit dem Status IRRECOVERABLE haben und mit diesem arbeiten, versuchen Sie einen der folgenden Schritte:

- Aktivieren Sie ein neues Tape Gateway, sofern Sie noch keines aktiviert haben. Weitere Informationen finden Sie unter Erstellen eines Gateways.
- Deaktivieren Sie das Tape Gateway mit dem nicht wiederherstellbaren Band und stellen Sie das Band von einem Wiederherstellungspunkt auf dem neuen Tape Gateway wieder her. Weitere Informationen finden Sie unter Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen..

> **Note**
>
> Sie müssen Ihren iSCSI-Initiator und Ihre Sicherungsanwendung neu konfigurieren, um das neue Tape Gateway verwenden zu können. Weitere Informationen finden Sie unter Verbinden von VTL-Geräten.

Sie nicht benötigen kein IRRECOVERABLE Band das nicht archiviert ist

Wenn Sie ein virtuelles Band mit dem Status IRRECOVERABLE besitzen, brauchen Sie es nicht und das Band war noch nie archiviert, so sollten Sie es löschen. Weitere Informationen finden Sie unter Löschen von Bändern.

In einer Cache-Festplatte in Ihrem Gateway tritt ein Fehler auf

Wenn bei einem oder mehreren Cache-Datenträgern in Ihrem Gateway ein Fehler auftritt, verhindert das Gateway Lese- und Schreiboptionen auf dem virtuellen Band im Gateway. Um die normale Funktionalität wiederherzustellen, konfigurieren Sie Ihr Gateway wie folgt neu:

- Wenn die Cache-Festplatte nicht zugänglich oder nicht verwendbar ist, löschen Sie den Datenträger aus Ihrer Gateway-Konfiguration.
- Wenn die Cache-Festplatte weiterhin zugänglich und nutzbar ist, verbinden Sie sie erneut mit Ihrem Gateway.

> **Note**
>
> Wenn Sie eine Cache-Festplatte löschen, sind Bänder oder Volumes mit sauberen Daten (d. h., deren Daten auf der Cache-Festplatte und in Amazon S3 synchronisiert sind) weiterhin verfügbar, wenn das Gateway wieder normal funktioniert. Wenn Ihr Gateway beispielsweise über drei Cache-Festplatten verfügt und Sie zwei löschen, haben Bänder oder Volumes, die unbeschrieben und fehlerfrei sind, den Status AVAILABLE. Andere Bänder und Volumes erhalten dann den Status IRRECOVERABLE.
>
> Wenn Sie kurzlebige Datenträger als Cache-Festplatten für Ihr Gateway verwenden oder Ihre Cache-Festplatten auf einem kurzlebigen Datenträger bereitstellen, gehen Ihre Cache-Festplatten verloren, wenn Sie das Gateway herunterfahren. Wenn Ihre Cache-Festplatte und Amazon S3 nicht synchronisiert werden, kann das Herunterfahren des Gateways zu

Datenverlust führen. Aus diesem Grund raten wir von der Verwendung von kurzlebigen Laufwerken oder Datenträgern ab.

High Availability-Zustandsbenachrichtigungen

Wenn Sie Ihr Gateway auf der VMware vSphere High Availability(HA)-Plattform ausführen, erhalten Sie möglicherweise Zustandsbenachrichtigungen. Weitere Informationen zu Zustandsbenachrichtigungen finden Sie unter Beheben von Problemen mit Hochverfügbarkeit.

Beheben von Problemen mit 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, erzeugen alle Gateways die folgenden Zustandsbenachrichtigungen für Ihre konfigurierte Amazon- CloudWatch 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 Zurücksetzen durch vSphere High Availability Application Monitoring dieses Ereignis auslösen.

Maßnahme

Wenn Ihr Gateway in einer solchen Umgebung ausgeführt wird, überprüfen Sie, ob die Benachrichtigung `HealthCheckFailure` vorhanden ist, und konsultieren Sie das VMware-Ereignisprotokoll für die VM.

Benachrichtigung: HealthCheckFailure

Für ein Gateway auf VMware vSphere HA können Sie die Benachrichtigung `HealthCheckFailure` erhalten, wenn eine Zustandsprüfung fehlschlägt und ein Neustart der VM angefordert wird. Dieses Ereignis tritt auch während eines Tests zum Überwachen der Verfügbarkeit auf, der durch die Benachrichtigung `AvailabilityMonitorTest` angezeigt wird. In diesem Fall wird die Benachrichtigung `HealthCheckFailure` erwartet.

> **Note**
>
> Diese Benachrichtigung gilt nur für VMware-Gateways.

Maßnahme

Wenn dieses Ereignis wiederholt ohne die Benachrichtigung `AvailabilityMonitorTest` auftritt, überprüfen Sie die VM-Infrastruktur auf Probleme (Speicher, Arbeitsspeicher usw.). Wenn Sie zusätzliche Unterstützung benötigen, wenden Sie sich an AWS Support.

Benachrichtigung: AvailabilityMonitorTest

Für ein Gateway auf VMware vSphere HA können Sie eine `AvailabilityMonitorTest`-Benachrichtigung während der Testausführung des Systems zur Verfügbarkeits- und Anwendungsüberwachung in VMware erhalten.

Metriken

Die Metrik `AvailabilityNotifications` ist auf allen Gateways verfügbar. Diese Metrik ist eine Zählung der Anzahl an Zustandsbenachrichtigungen im Zusammenhang mit der Verfügbarkeit, die vom Gateway generiert werden. Verwenden Sie die Statistik `Sum`, um zu beobachten, ob Ereignisse im Zusammenhang mit der Verfügbarkeit im Gateway auftreten. Weitere Informationen zu den Ereignissen finden Sie in Ihrer konfigurierten CloudWatch Protokollgruppe.

Bewährte Methoden zum Wiederherstellen 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.

Themen

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 Gateway-Internetverbindung.
- Wenn Ihr Gateway in Konfigurationen mit Bändern erreichbar ist, werden Ihre Bänder in den BOOTSTRAPPING-Status versetzt. Diese Funktion stellt sicher, dass Ihre lokal gespeicherten Daten weiterhin mit synchronisiert werden AWS. Weitere Informationen, zu diesem Status, finden Sie unter Grundlegendes zum Bandstatus.
- Wenn Ihre Gateway fehlerhaft ist und Probleme mit Ihren Volumes oder Bändern auftreten und das im Zusammenhang mit einem unerwarteten Herunterfahren steht, dann können Sie Daten wiederherstellen. Weitere Informationen dazu, wie Sie Ihre Daten wiederherstellen, finden Sie in den folgenden Abschnitten, die auf Ihren Fall passen.

Wiederherstellen Ihrer Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM

Wenn in Ihrem Tape Gateway oder im Hypervisor-Host ein Dauerfehler auftritt, können Sie die folgenden Schritte befolgen, um die Bänder von einem fehlerhaften Tape Gateway auf einem anderen Tape Gateway wiederherzustellen:

1. Legen Sie fest, welches Tape Gateway als Wiederherstellungsziel verwendet werden soll, oder erstellen Sie ein neues.
2. Deaktivieren Sie das defekte Gateway.
3. Erstellen Sie Wiederherstellungsbänder für jedes Band, dass Sie wiederherstellen möchten, und geben Sie das Ziel-Tape-Gateway an.
4. Löschen Sie die nicht funktionsfähige Tape Gateway.

Detaillierte Informationen zur Wiederherstellung der Bänder von einem fehlerhaften Tape Gateway auf einem anderen Tape Gateway finden Sie unter Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen..

Wiederherstellung Ihrer Daten von einem nicht wiederherstellbaren Band

Wenn in Ihrem Band ein Fehler auftritt und der Status des Bands IRRECOVERABLE ist, empfehlen wir, dass Sie eine der folgenden Optionen zum Wiederherstellen Ihrer Daten verwenden oder lösen Sie den Fehler je nach Situation:

- Wenn Sie die Daten auf dem irreparablen Band benötigen, können Sie das Band auf einem neuen Gateway wiederherstellen.
- Wenn Sie diese Daten nicht auf dem Band benötigen und das Band noch nie archiviert wurde, können sie dieses Band einfach von Ihrem Tape Gateway löschen.

  Detaillierte Informationen, wie Sie Ihre Daten wiederherstellen oder den Fehler lösen, wenn Ihr Band IRRECOVERABLE ist, finden Sie unter Fehlerbehebung bei nicht wiederherstellbaren Bändern.

Wiederherstellen Ihrer Daten von einer fehlerhaften Cache-Festplatte

Wenn in Ihrer Cache-Festplatte ein Fehler auftritt, empfehlen wir die folgenden Schritte zum Wiederherstellen Ihrer Daten je nach Situation, zu befolgen:

- Wenn der Fehler aufgetreten ist, weil eine Cache-Festplatte aus Ihrem Host entnommen wurde, fahren Sie das Gateway herunter, fügen Sie die Festplatte wieder ein und starten Sie das Gateway.
- Wenn der Cache-Datenträger beschädigt ist oder wenn nicht auf ihn zugegriffen werden kann, setzen Sie den Cache-Datenträger, konfigurieren Sie die Festplatte für den Cache-Speicher neu und starten Sie das Gateway neu.

Weitere Informationen hierzu finden Sie unter Sie müssen ein virtuelles Band aus einer fehlerhaften Cache-Festplatte wiederherstellen.

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.

So stellen Sie Daten von einem Tape-Gateway in einem Rechenzentrum wieder her, auf das nicht zugegriffen werden kann

1. Erstellen und aktivieren Sie ein neues Tape Gateway auf einem Amazon-EC2-Host. Weitere Informationen finden Sie unter Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Tape Gateway.
2. Stellen Sie die Bänder vom Quell-Gateway im Rechenzentrum auf dem neuen Gateway wieder her, das Sie auf Amazon EC2 erstellt haben. Weitere Informationen finden Sie unter Wiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway.

   Ihre Bänder sollten auf dem neuen Amazon-EC2-Gateway wiederhergestellt werden.

Zusätzliche Storage-Gateway-Ressourcen

In diesem Abschnitt werden und Software, Tools und Ressourcen von AWS Drittanbietern beschrieben, mit denen Sie Ihr Gateway einrichten oder verwalten können, sowie Storage Gateway-Kontingente.

Themen

Host-Setup

Themen

Konfiguration von VMware für Storage Gateway

Stellen Sie beim Konfigurieren von VMware für Storage Gateway sicher, dass Sie die VM-Zeit mit der Host-Zeit synchronisieren, die VM für die Verwendung von paravirtualisierten Festplattencontrollern

konfigurieren, wenn Sie Speicher bereitstellen, und Schutz vor Fehlern im Infrastruktur-Layer bereitstellen, das eine Gateway-VM unterstützt.

Themen

Synchronisieren der VM-Zeit mit der Host-Zeit

Damit das Gateway erfolgreich aktiviert wird, müssen Sie sicherstellen, dass die VM-Zeit mit der Host-Zeit synchronisiert ist und dass die Host-Zeit richtig eingestellt ist. In diesem Abschnitt synchronisieren Sie zunächst die Zeit für die VM mit der Host-Zeit. Anschließend prüfen Sie die Host-Zeit. Stellen Sie dann bei Bedarf die Host-Zeit ein und konfigurieren Sie den Host so, dass die Zeit automatisch mit einem NTP-Server (Network Time Protocol) synchronisiert wird.

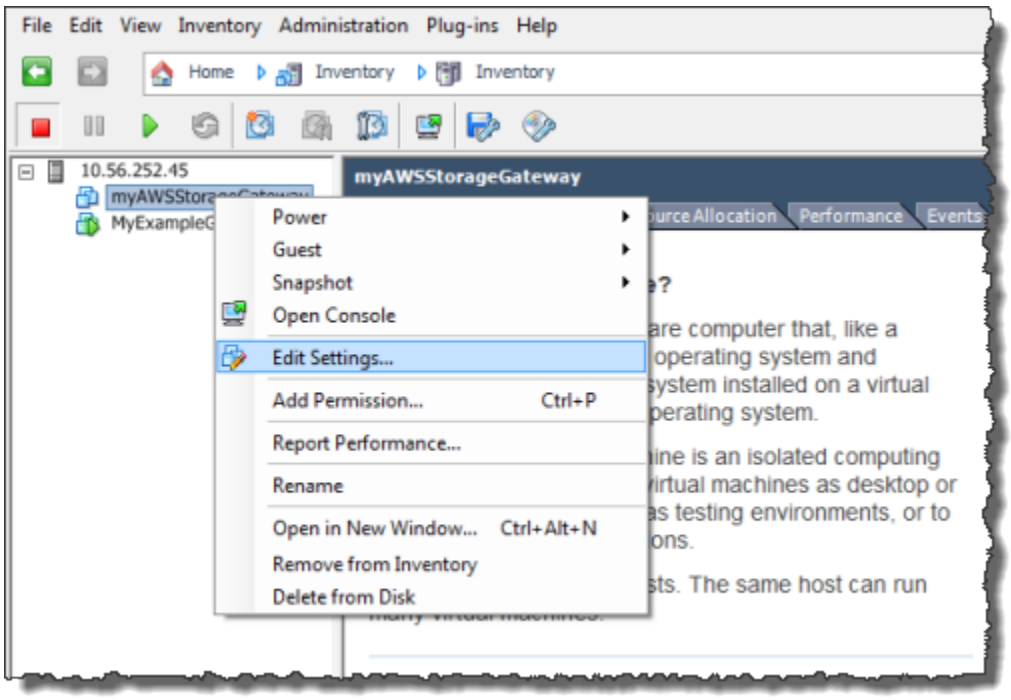
> **Important**
>
> Das Synchronisieren der VM-Zeit mit der Host-Zeit ist erforderlich, um das Gateway erfolgreich zu aktivieren.

So synchronisieren Sie die VM-Zeit mit der Host-Zeit

1. Konfigurieren Sie Ihre VM-Zeit.

   a. Öffnen Sie im vSphere-Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM und wählen Sie Edit Settings (Einstellungen bearbeiten).

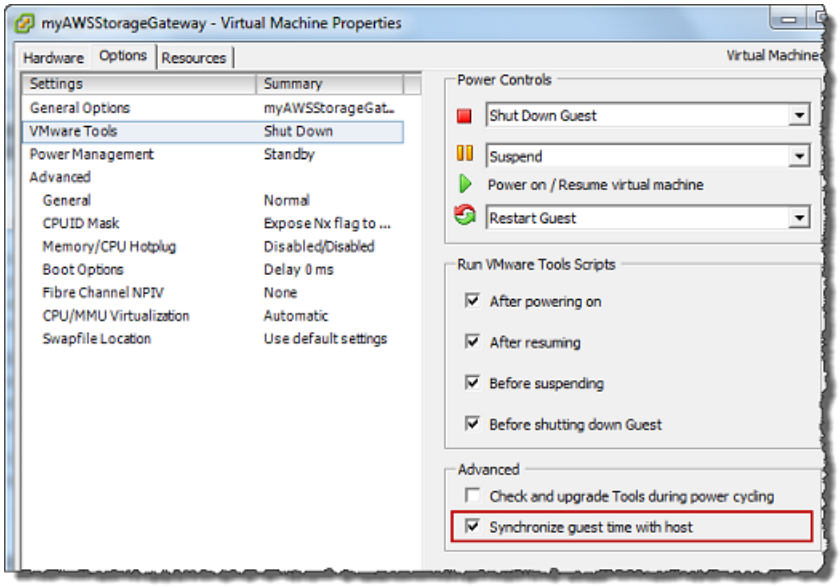
      Das Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) wird geöffnet.



b. Wählen Sie die Registerkarte Options (Optionen) und wählen Sie die Option VMware Tools (VMware-Tools) in der Optionenliste.

c. Aktivieren Sie die Option Synchronize guest time with host (Gastzeit mit Host synchronisieren) und wählen Sie dann OK.

   Die VM synchronisiert ihre Zeit mit dem Host.



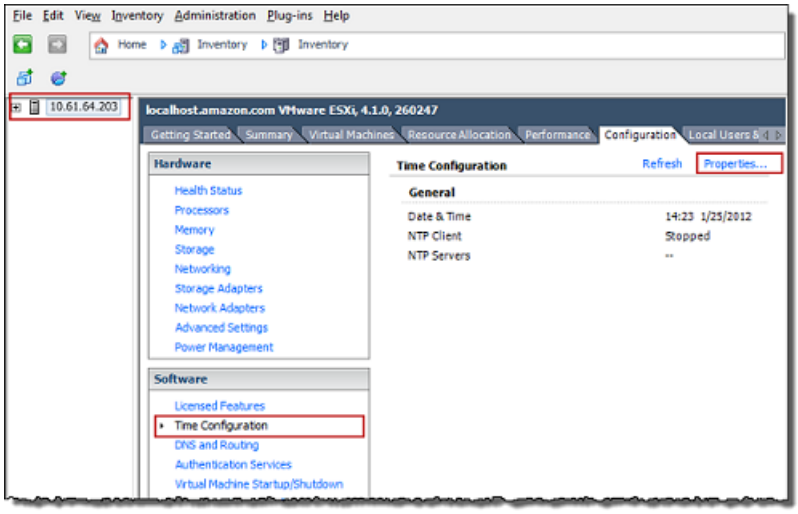
2. Konfigurieren Sie die Host-Zeit.

Es muss unbedingt sichergestellt werden, dass die Host-Uhr auf die korrekte Zeit eingestellt ist. Wenn Sie die Host-Uhr noch nicht konfiguriert haben, führen Sie die folgenden Schritte aus, um sie einzurichten und mit einem NTP-Server zu synchronisieren.

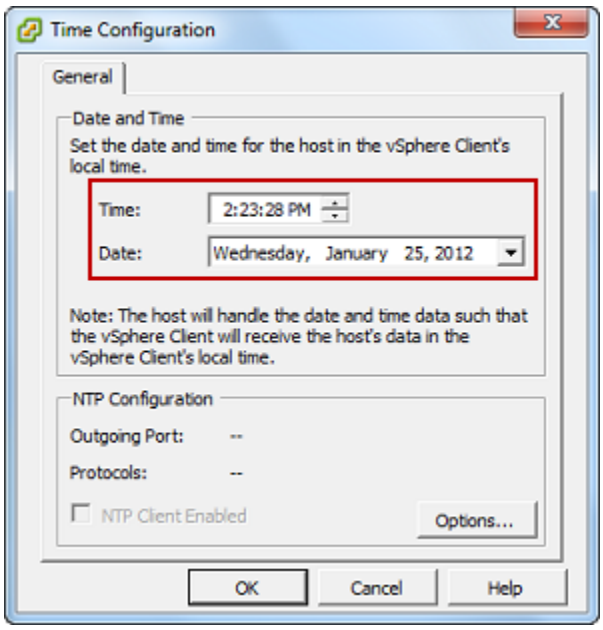
a. Wählen Sie im VMware vSphere-Client den vSphere Host-Knoten im linken Bereich und wählen Sie dann die Registerkarte Configuration (Konfiguration).

b. Wählen Sie die Option Time Configuration (Zeitkonfiguration) im Bereich Software und wählen Sie dann den Link Properties (Eigenschaften).

   Das Dialogfeld Time Configuration (Zeitkonfiguration) wird geöffnet.

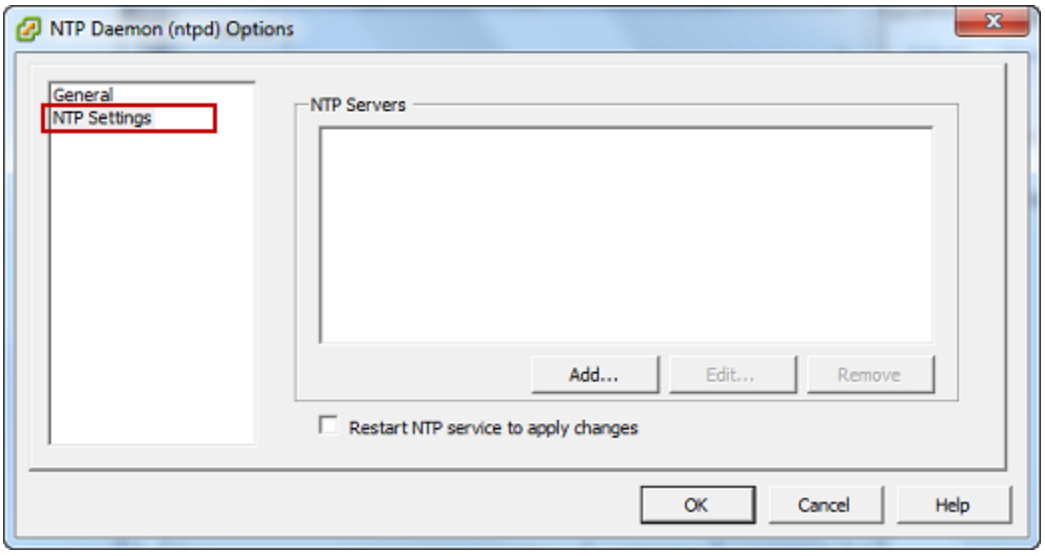


c. Legen Sie im Bereich Date and Time (Datum und Uhrzeit) das Datum und die Uhrzeit fest.



d. Konfigurieren Sie den Host so, dass seine Zeit automatisch mit einem NTP-Server synchronisiert wird.

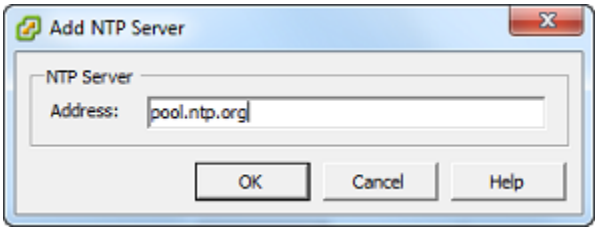
   i. Wählen Sie Options (Optionen) im Dialogfeld Time Configuration (Zeitkonfiguration) und wählen Sie dann im Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) die Option NTP Settings (NTP-Einstellungen) im linken Bereich.



   ii. Wählen Sie Add (Hinzufügen), um einen neuen NTP-Server hinzuzufügen.

   iii. Geben Sie im Dialogfeld Add NTP Server (NTP-Server hinzufügen) die IP-Adresse oder den vollqualifizierten Domänennamen eines NTP-Servers ein und wählen Sie dann OK.

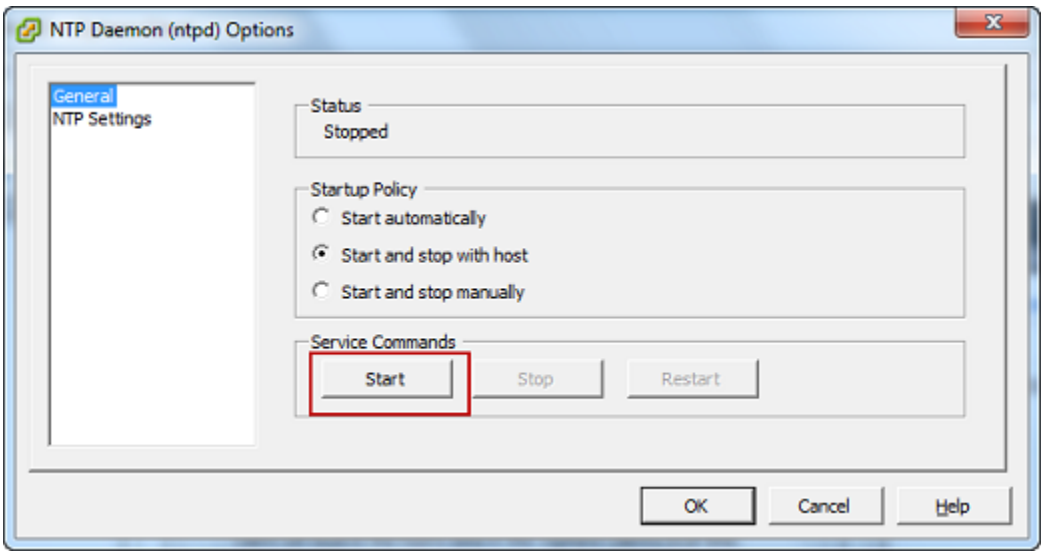
   Sie können `pool.ntp.org` verwenden, wie im folgenden Beispiel gezeigt.



iv. Wählen Sie im Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) die Option General (Allgemein) im linken Bereich.

v. Wählen Sie im Bereich Service Commands (Servicebefehle) die Option Start, um den Service zu starten.

Hinweis: Wenn Sie diese NTP-Serverreferenz ändern oder später einen anderen Server hinzufügen, müssen Sie den Service neu starten, um den neuen Server zu verwenden.



e. Wählen Sie OK, um das Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) zu schließen.

f. Wählen Sie OK, um das Dialogfeld Time Configuration (Zeitkonfiguration) zu schließen.

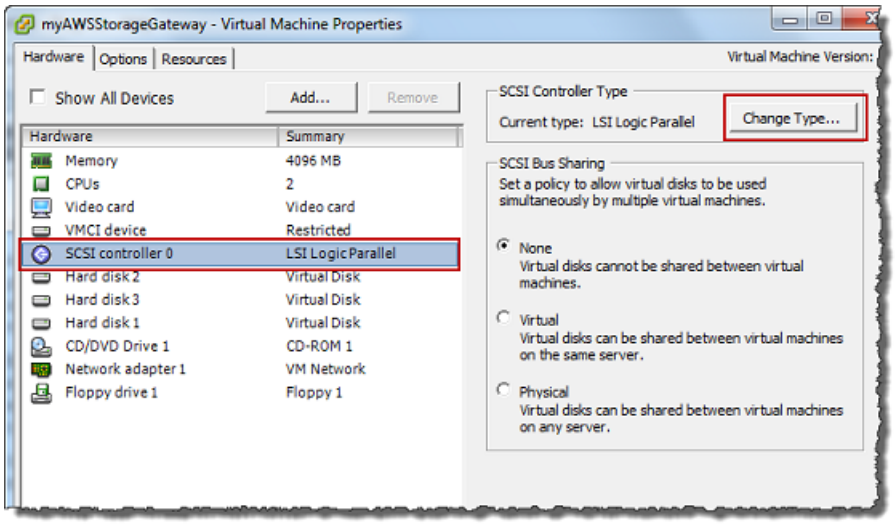
Konfigurieren der AWS Storage Gateway VM für die Verwendung paravirtualisierter Festplattencontroller

In diesem Schritt legen Sie den iSCSI-Controller so fest, dass die VM Paravirtualisierung verwendet. Paravirtualisierung ist ein Modus, in dem die Gateway-VM mit dem Host-Betriebssystem arbeitet, damit die Konsole die der VM hinzugefügten virtuellen Festplatten identifizieren kann.

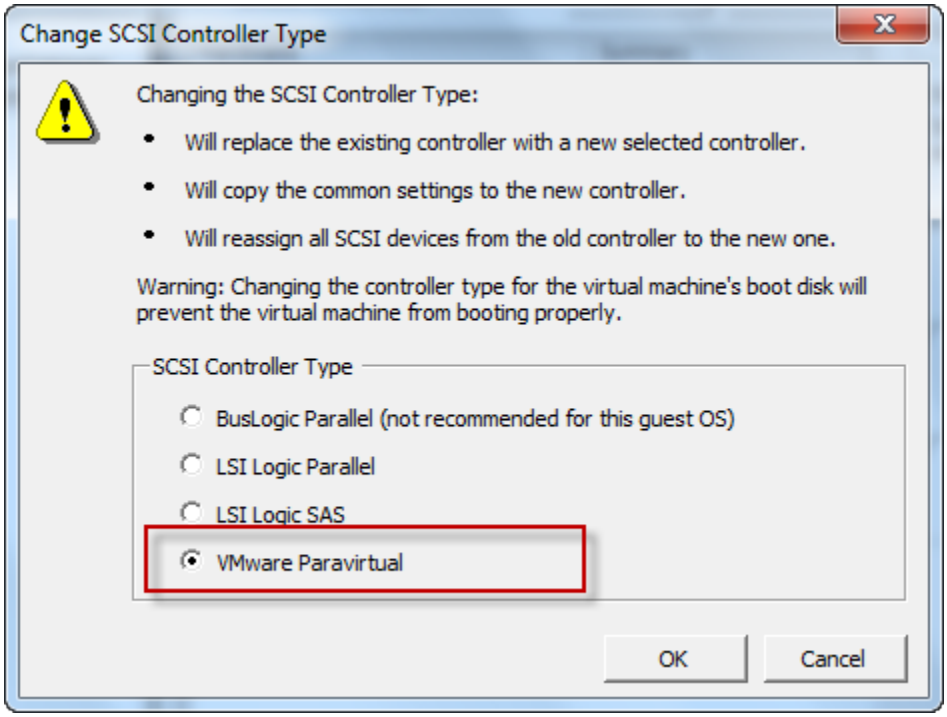
> **Note**
>
> Dieser Schritt ist erforderlich, um Probleme beim Identifizieren dieser Festplatten zu verhindern, wenn Sie sie in der Gateway-Konsole konfigurieren.

So konfigurieren Sie die VM für die Verwendung von paravirtualisierten Controllern

1. Öffnen Sie im VMware vSphere-Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM und wählen Sie dann Edit Settings (Einstellungen bearbeiten).
2. Wählen Sie im Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) die Registerkarte Hardware, wählen Sie SCSI controller 0 (SCSI-Controller 0) und wählen Sie dann Change Type (Typ ändern).



3. Wählen Sie im Dialogfeld Change SCSI Controller Type (SCSI-Controllertyp ändern) den SCSI-Controllertyp VMware Paravirtual und wählen Sie dann OK.



Verwenden von Storage Gateway mit VMware High Availability

VMware High Availability (HA) ist eine Komponente von vSphere, die Schutz vor Fehlern in der Infrastrukturebene, die eine Gateway-VM unterstützt, bieten kann. VMware HA tut dies durch die Verwendung von mehreren Hosts, die als Cluster konfiguriert sind, so dass, wenn ein Host mit einer Gateway-VM fehlschlägt, der Gateway-VM automatisch auf einem anderen Host im Cluster neu gestartet werden kann. Weitere Informationen zur VMware HA finden Sie unter VMware HA: Concepts and Best Practices auf der Website von VMware.

Um Storage Gateway mit VMware HA zu verwenden, empfehlen wir die folgenden Dinge:

- Stellen Sie das herunterladbare VMware ESX `.ova`-Paket, das die Storage Gateway-VM enthält, nur auf einem Host in einem Cluster bereit.
- Bei der Bereitstellung des `.ova` Pakets, wählen Sie einen Datenspeicher, der sich nicht auf einem lokalen Host befindet. Verwenden Sie stattdessen einen Datenspeicher, der auf alle Hosts im Cluster zugreifen kann. Wenn Sie einen Datenspeicher auswählen, der lokal zu einem Host ist und der Host ausfällt, dann kann auf die Datenquelle möglicherweise von andere Hosts im Cluster nicht mehr zugegriffen werden und andere Hosts im Cluster und Failover zu einem anderen Host sind eventuell nicht erfolgreich.

- Um zu verhindern, dass sich Ihr Initiator vom Speicher-Volumenziel während des Failovers trennt, befolgen Sie die empfohlenen iSCSI-Einstellungen für Ihr Betriebssystem. In Falle eines Failovers, kann es einige Sekunden bis zu einigen Minuten für eine Gateway-VM dauern, um einen neuen Host im Failover-Cluster zu starten. Die empfohlene iSCSI-Timeouts für Windows- und Linux-Clients sind größer als die typische Zeit die es braucht das ein Failover auftritt. Weitere Informationen zum Anpassen von Windows-Client-Timeout-Einstellungen, finden Sie unter Anpassen der Windows iSCSI-Einstellungen. Weitere Informationen zum Anpassen von Linux-Client-Timeout-Einstellungen, finden Sie unter Anpassen Ihrer Linux iSCSI-Einstellungen.
- Mit Clustering, wenn Sie bei der Bereitstellung des `.ova` Pakets zum Cluster wählen Sie den Host, wenn Sie dazu aufgefordert werden. Alternativ können Sie direkt auf einem Host in einem Cluster bereitstellen.

Synchronisieren der Gateway-VM-Zeit

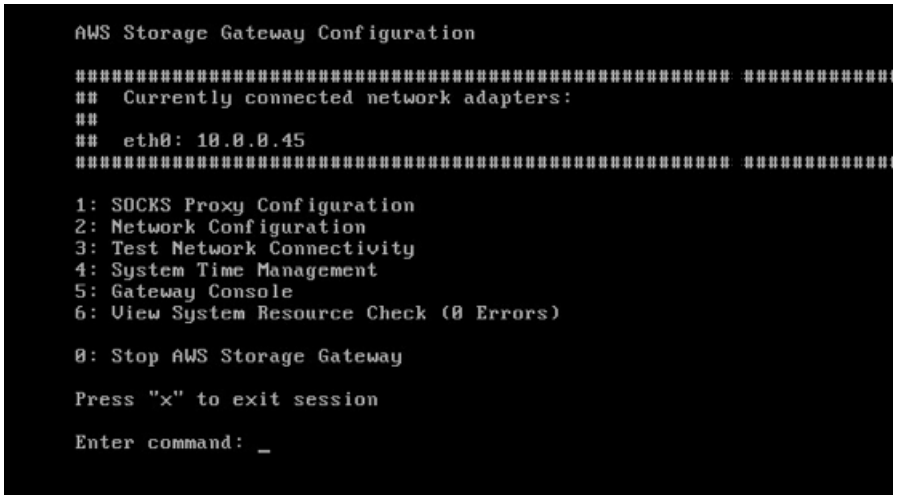
Bei einem Gateway, das auf einem VMware ESXi bereitgestellt wird, reicht es aus, die Hypervisor-Host-Zeit einzustellen und die VM-Zeit mit dem Host zu synchronisieren, um eine Abweichung zu verhindern. Weitere Informationen finden Sie unter Synchronisieren der VM-Zeit mit der Host-Zeit. Bei einem Gateway, das auf Microsoft Hyper-V bereitgestellt wird, sollten Sie die Zeit Ihrer VM regelmäßig anhand des folgenden Verfahrens prüfen.

So zeigen Sie die Zeit einer Hypervisor-Gateway-VM an und synchronisieren Sie mit der Zeit eines Network Time Protocol(NTP)-Servers

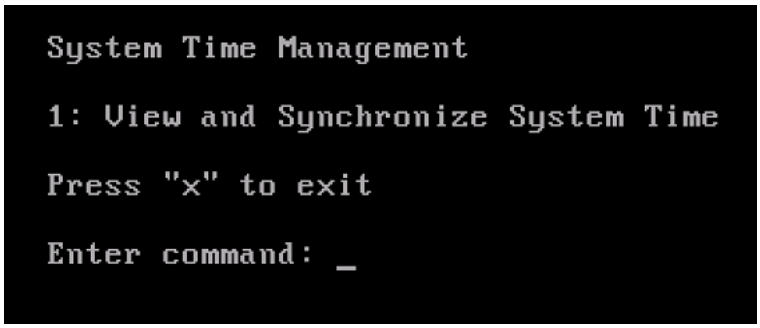
1. Melden Sie sich bei der lokalen Konsole des Gateways an:

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

2. Geben Sie im Hauptmenü Storage-Gateway-Konfiguration **4** für Systemzeitverwaltung ein.



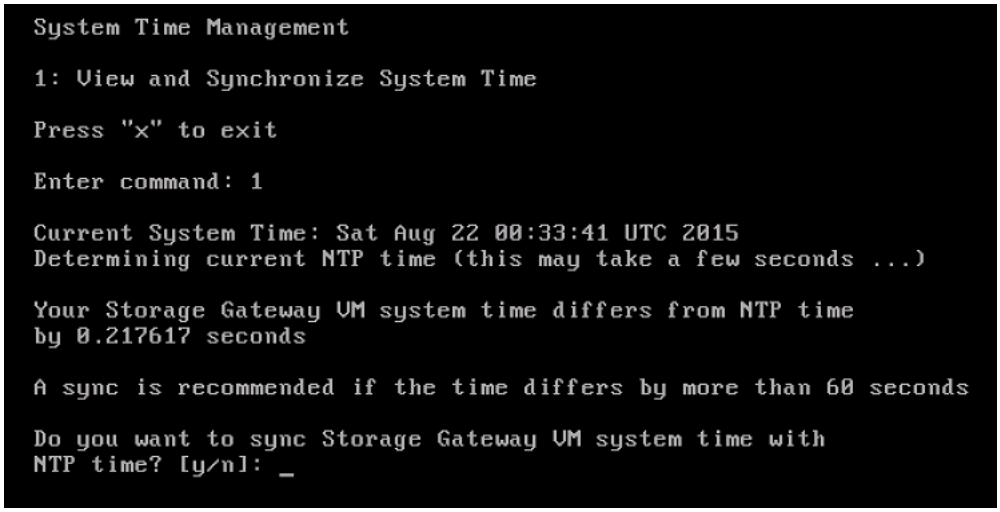
3. Geben Sie im Menü System Time Management (Systemzeit-Management) die Option **1** für View and Synchronize System Time (Systemzeit anzeigen und synchronisieren) ein.



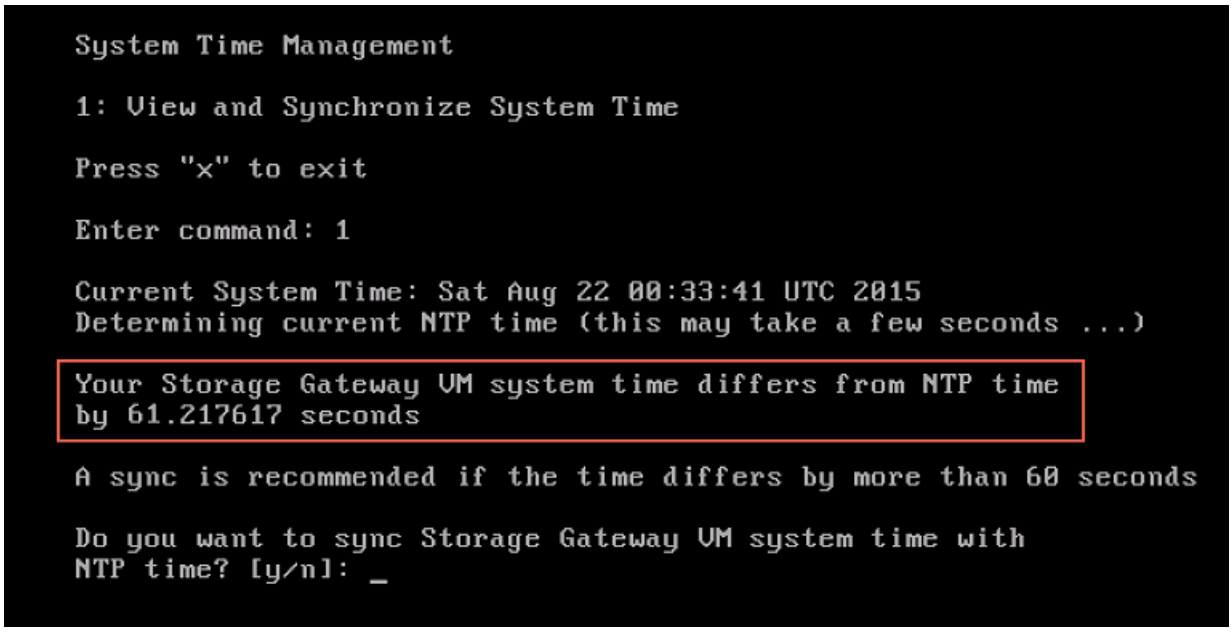
4. Wenn das Ergebnis anzeigt, dass Sie die Zeit Ihrer VM mit der Zeit des NTP synchronisieren sollten, geben Sie **y** ein. Geben Sie andernfalls **n** ein.

   Wenn Sie **y** eingeben, um zu synchronisieren, kann die Synchronisierung einige Zeit in Anspruch nehmen.

   Der folgende Screenshot zeigt eine VM, die keine Zeitsynchronisierung erfordert.



Der folgende Screenshot zeigt eine VM, die eine Zeitsynchronisierung erfordert.



Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Tape Gateway

Sie können ein Tape Gateway 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**
>
> Die AMIs der Storage Gateway-Community werden von AWS veröffentlicht und vollständig unterstützt. Sie können sehen, dass der Herausgeber ist AWS, ein verifizierter Anbieter.

So stellen Sie eine Amazon-EC2-Instance als Host für Ihr Tape Gateway bereit

1. Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter Einrichten eines Tape Gateways . Wenn Sie den Bereich Plattform-Optionen erreichen, wählen Sie Amazon EC2 als Host-Plattform aus und führen Sie dann die folgenden Schritte aus, um die Amazon-EC2-Instance zu starten, die Ihr Tape Gateway hosten wird.
2. Wählen Sie Instance starten, um die AWS Storage Gateway AMI-Vorlage in der Amazon EC2-Konsole zu öffnen, in der 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-Schnellstart finden Sie unter Schnellstart-Konfigurationsspezifikationen für Amazon EC2.
3. Geben Sie unter Name einen Namen für die Amazon-EC2-Instance ein. Nachdem die Instance bereitgestellt wurde, können Sie nach diesem Namen suchen, um Ihre Instance auf Listenseiten in der Amazon-EC2-Konsole zu finden.
4. Für Instance-Typ können Sie aus der Liste Instance-Typ die Hardware-Konfiguration für Ihre Instance auswählen. Die Hardwarekonfiguration muss bestimmte Mindestanforderungen erfüllen, um Ihr Gateway zu unterstützen. Wir empfehlen, mit dem Instance-Typ m4.xlarge zu beginnen, der die Mindestanforderungen erfüllt, damit das Gateway korrekt funktioniert. Weitere Informationen finden Sie unter Anforderungen für Amazon-EC2-Instance-Typen.

   Sie können die Größe der Instance nach dem Start bei Bedarf ändern. Weitere Informationen finden Sie unter Anpassung der Größe der Instance im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

   > **Note**
   >
   > Bestimmte Instance-Typen, insbesondere i3 EC2, verwenden NVMe-SSD-Datenträger. Dies kann zu Problemen führen, wenn Sie ein Tape Gateway starten oder beenden. Beispielsweise können Sie Daten aus dem Cache verlieren. Überwachen Sie die `CachePercentDirty` Amazon- CloudWatch Metrik und starten oder stoppen Sie Ihr

System nur, wenn dieser Parameter ist`0`. Weitere Informationen zur Überwachung von Metriken für Ihr Gateway finden Sie unter Storage Gateway-Metriken und -Dimensionen in der - CloudWatch Dokumentation.

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

> **Note**
>
> Tape Gateway setzt voraus, dass der TCP-Port 80 für eingehenden Datenverkehr und für einmaligen HTTP-Zugriff während der Gateway-Aktivierung geöffnet ist. Nach der Aktivierung können Sie diesen Port schließen.
> Darüber hinaus müssen Sie den TCP-Port 3260 für den iSCSI-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 165 GiB Kapazität für den Cache-Speicher und mindestens ein Amazon EBS-Volume mit mindestens 150 GiB Kapazität für den Upload-Puffer 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 IPv4-Adresse aus dem Abschnitt Instanzübersicht und kehren Sie dann zur Seite Gateway einrichten in der Storage-Gateway-Konsole zurück, um mit der Einrichtung Ihres Tape Gateways.

Sie können die AMI-ID ermitteln, die zum Starten eines Tape Gateway sverwendet werden soll, indem Sie die Storage 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 eines Tape Gateways . Wenn Sie den Abschnitt Plattformoptionen erreichen, wählen Sie Amazon EC2 als Host-Plattform und dann Instance starten, um die AWS Storage Gateway AMI-Vorlage in der Amazon EC2-Konsole zu öffnen.

Sie werden zur Seite EC2 Community AMI 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-API verwenden, um den öffentlichen Systems Manager-Parameter unter dem Namespace abzufragen`/aws/service/storagegateway/ami/VTL/latest`. 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/VTL/
latest
```

Dieser CLI-Befehl gibt etwa die folgende Ausgabe zurück:

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/VTL/
latest",
        "Name": "/aws/service/storagegateway/ami/VTL/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Bereitstellen von Amazon EC2 mit Standardeinstellungen

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

Sie können ein Tape Gateway auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance bereitstellen und aktivieren. Das AWS Storage Gateway-AMI (Amazon Machine Image) ist als Community-AMI verfügbar.

> **Note**
>
> Die AMIs der Storage Gateway-Community werden von AWS veröffentlicht und vollständig unterstützt. Sie können sehen, dass der Herausgeber ist AWS, ein verifizierter Anbieter.

1. Um die Amazon-EC2-Instance einzurichten, wählen Sie Amazon EC2 als Host-Plattform im Abschnitt Plattform-Optionen des Workflows aus. Anweisungen zur Konfiguration der Amazon-EC2-Instance finden Sie unter Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Tape Gateway .
2. Wählen Sie Instance starten aus, um die AWS Storage Gateway-AMI-Vorlage in der Amazon 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 Dropddown-Liste angezeigt, wenn für sie die Einstellung „Öffentliche IPv4-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 iSCSI-Ziele auf Ihrem Gateway kann nur von den Hosts aus zugegriffen werden, die sich in derselben VPC wie das Gateway befinden. Wenn auf die iSCSI-Ziele 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				
3260	TCP	iSCSI				

- Speicher konfigurieren

Standardeinstellungen	AMI-Root-Volume	Volume 2 Cache	Volume 3 Cache			
Gerätename		/dev/sdf	/dev/sdf			
Größe	80 GiB	250 GiB	250 GiB			

Standardeinstellungen	AMI-Root-Volume	Volume 2 Cache	Volume 3 Cache			
Volume-Typ	gp3	gp3	gp3			
IOPS	3000	3000	3000			
Beim Beenden löschen	Ja	Ja	Ja			
Encrypted	Nein	Nein	Nein			
Durchsatz	125	125	125			

Ändern von Amazon EC2-Instance-Metadatenoptionen

Der Instance-Metadatenservice (IMDS) ist eine On-Instance-Komponente, die sicheren Zugriff auf Amazon EC2-Metadaten bietet. Eine Instance kann so konfiguriert werden, dass eingehende Metadatenanforderungen akzeptiert werden, die IMDS Version 1 (IMDSv1) verwenden, oder dass alle Metadatenanforderungen IMDS Version 2 (IMDSv2) verwenden. IMDSv2 verwendet sitzungsorientierte Anfragen und mildert verschiedene Arten von Sicherheitsschwachstellen, über die versucht werden kann, auf das IMDS zuzugreifen. Informationen zu IMDSv2 finden Sie unter Funktionsweise von Instance-Metadatenservice Version 2 im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Wir empfehlen, dass Sie IMDSv2 für alle Amazon EC2-Instances benötigen, die Storage Gateway hosten. IMDSv2 ist standardmäßig auf allen neu gestarteten Gateway-Instances erforderlich. Wenn Sie über vorhandene Instances verfügen, die noch für die Annahme von IMDSv1-Metadatenanforderungen konfiguriert sind, finden Sie unter Erzwingen der Verwendung von IMDSv2 im Amazon Elastic Compute Cloud-Benutzerhandbuch Anweisungen zum Ändern Ihrer Instance-Metadatenoptionen, um die Verwendung von IMDSv2 zu erzwingen. Für die Anwendung dieser Änderung ist kein Neustart der Instance erforderlich.

Tape Gateway

Themen

Entfernen von Datenträgern aus dem Gateway

Obwohl wir das Entfernen der zugrunde liegenden Datenträger aus dem Gateway nicht empfehlen, möchten Sie gegebenenfalls einen Datenträger aus dem Gateway entfernen, z. B. bei einem ausgefallenen Datenträger.

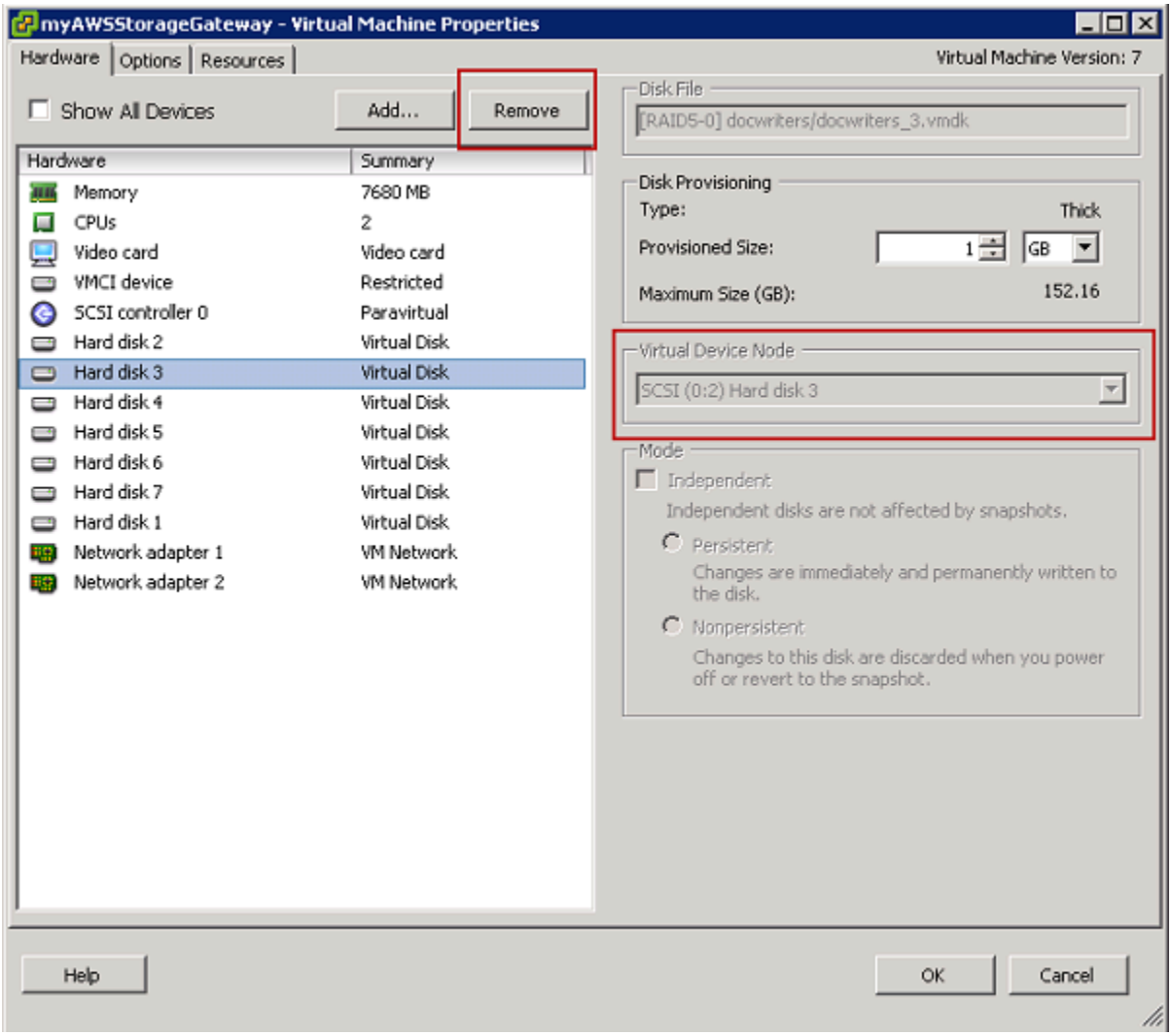
Entfernen eines Datenträgers aus einem auf VMware ESXi gehosteten Gateway

Sie können mit dem folgenden Verfahren einen Datenträger aus dem auf VMware-Hypervisor gehosteten Gateway entfernen.

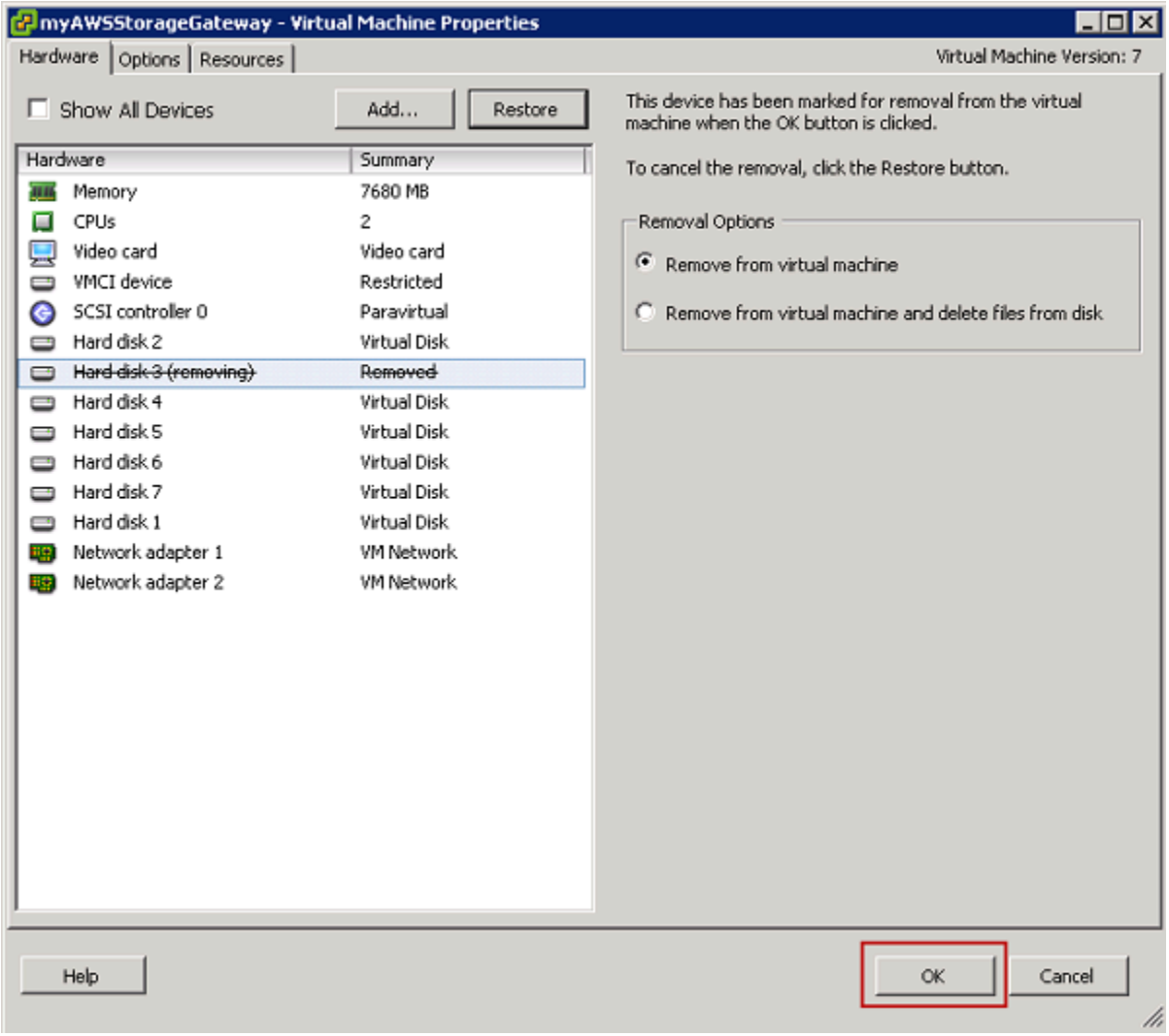
So entfernen Sie einen Datenträger für den Upload-Puffer (VMware ESXi)

1. Öffnen Sie im vSphere-Client das Kontextmenü (Klick mit der rechten Maustaste), wählen Sie den Namen der Gateway-VM und dann Einstellungen bearbeiten.
2. Klicken Sie auf der Registerkarte Hardware im Dialogfeld Eigenschaften der virtuellen Maschine auf den als Upload-Pufferspeicher zugewiesenen Datenträger und wählen Sie dann Entfernen.

   Stellen Sie sicher, dass der Wert Virtueller Geräteknoten im Dialogfeld Eigenschaften der virtuellen Maschine den gleichen Wert hat, den Sie zuvor notiert haben. Auf diese Weise stellen Sie sicher, dass Sie den richtigen Datenträger entfernen.



3. Wählen Sie eine Option im Bereich Optionen zum Entfernen und wählen Sie dann OK, um den Datenträger vollständig zu entfernen.



Entfernen eines Datenträgers aus einem auf Microsoft Hyper-V gehosteten Gateway

Sie können mit dem folgenden Verfahren einen Datenträger aus dem auf Microsoft Hyper-V gehosteten Gateway entfernen.

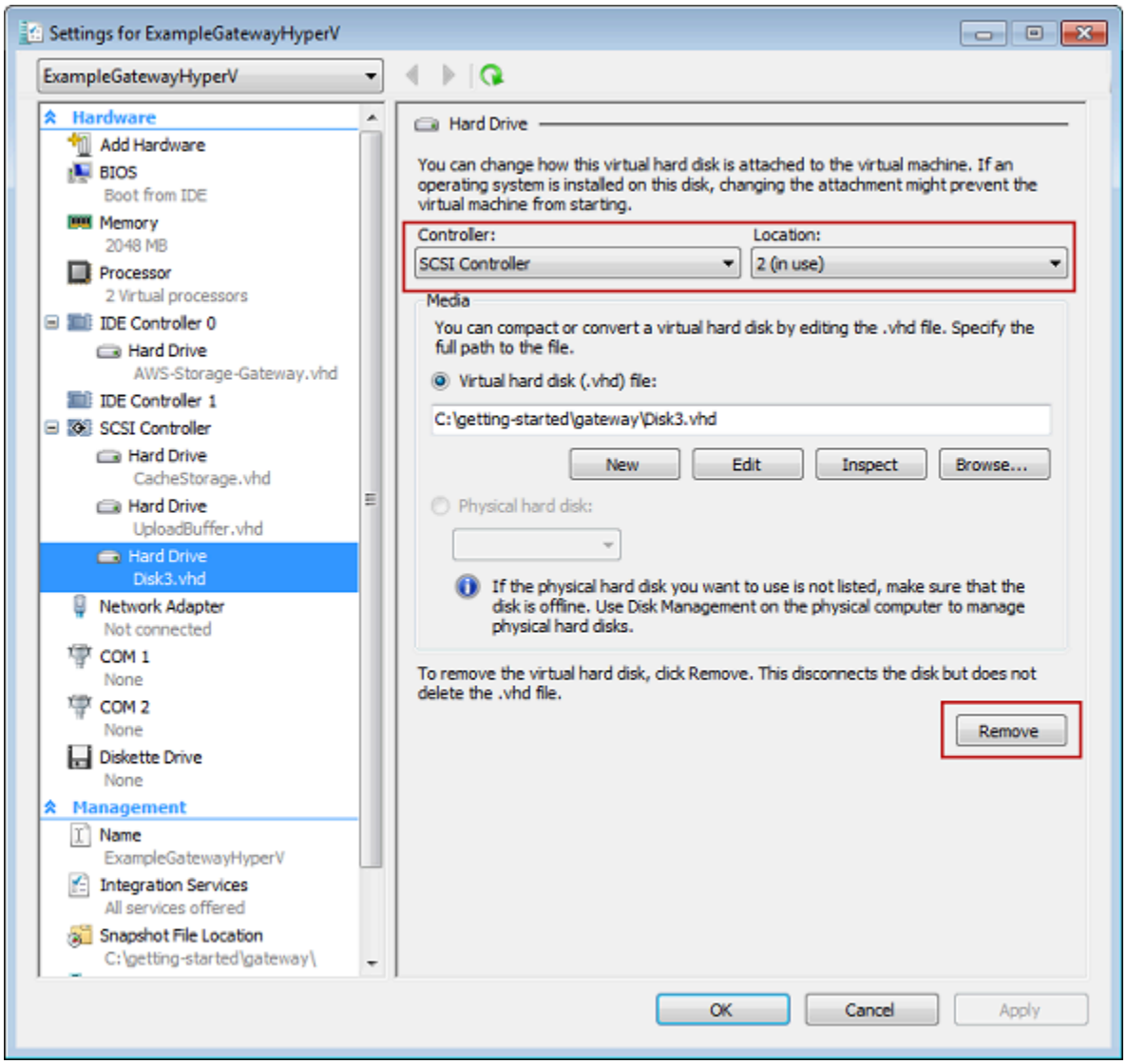
So löschen Sie einen zugrunde liegenden Datenträger für den Upload-Puffer (Microsoft Hyper-V)

1. Öffnen Sie im Microsoft Hyper-V-Manager das Kontextmenü (Klick mit der rechten Maustaste), wählen Sie den Namen der Gateway-VM und dann Einstellungen.
2. Klicken Sie in der Liste Hardware auf das Dialogfeld Einstellungen, wählen Sie den zu entfernenden Datenträger, und klicken Sie auf Entfernen.

   Die Datenträger, die Sie einem Gateway hinzufügen, werden unter dem Eintrag SCSI-Controller in der Liste Hardware angezeigt. Überprüfen Sie, ob die Werte Controller und Speicherort

denselben Wert haben, den Sie zuvor notiert haben. Auf diese Weise stellen Sie sicher, dass Sie den richtigen Datenträger entfernen.

Der erste SCSI-Controller im Microsoft Hyper-V-Manager ist Controller 0.



3. Klicken Sie auf OK, um die Änderungen anzuwenden.

Entfernen eines Datenträgers aus einem auf Linux KVM gehosteten Gateway

Um eine Festplatte von Ihrem Gateway zu trennen, das auf einem Linux KVM-Hypervisor (Kernel-basierte virtuelle Maschine) gehostet wird, können Sie einen `virsh`-Befehl verwenden, der dem folgenden ähnelt.

```
$ virsh detach-disk domain_name /device/path
```

Weitere Informationen zum Verwalten von KVM-Datenträgern finden Sie in der Dokumentation Ihrer Linux-Verteilung.

Hinzufügen und Entfernen von Amazon-EBS-Volumes für Ihr in Amazon EC2 gehostetes Gateway

Wenn Sie Ihr Gateway ursprünglich für die Ausführung als Amazon-EC2-Instance konfiguriert haben, haben Sie Amazon-EBS-Volumes zur Verwendung als Upload-Puffer und Cache-Speicher zugewiesen. Wenn im Laufe der Zeit Änderungen an Ihren Anwendungen erforderlich sind, können Sie für diesen Zweck zusätzliche Amazon-EBS-Volumes zuordnen. Sie können auch den zugewiesenen Speicher verringern, indem Sie zuvor zugewiesene Amazon-EBS-Volumes entfernen. Weitere Informationen zu Amazon EBS finden Sie unter Amazon Elastic Block Store (Amazon EBS) im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Bevor Sie zusätzlichen Speicher zum Gateway hinzufügen, sollten Sie die Größe des Upload-Puffers und des Cache-Speichers auf der Basis Ihrer Anwendungsanforderungen für ein Gateway überprüfen. Lesen Sie dazu Bestimmen der Größe des zuzuordnenden Upload-Puffers und Bestimmen der Größe des zuzuordnenden Cache-Speichers.

Es gibt Kontingente für den maximalen Speicher, den Sie als Upload-Puffer und Cache-Speicher zuordnen können. Sie können so viele Amazon-EBS-Volumes an Ihre Instance anfügen, wie Sie möchten. Sie können diese Volumes jedoch nur bis zu diesen Speicherkontingenten als Upload-Puffer und Cache-Speicher konfigurieren. Weitere Informationen finden Sie unter AWS Storage Gateway -Kontingente.

So fügen Sie ein Amazon-EBS-Volume hinzu und konfigurieren es für das Gateway

1. Erstellen Sie ein Amazon-EBS-Volume. Weitere Informationen finden Sie unter Erstellen oder Wiederherstellen eines Amazon-EBS-Volumes im Amazon-EC2-Benutzerhandbuch für Linux-Instances.
2. Fügen Sie das Amazon-EBS-Volume an Ihre Amazon-EC2-Instance an. Eine Anleitung finden Sie unter Anfügen eines Amazon-EBS-Volumes an eine Instance im Amazon-EC2-Benutzerhandbuch für Linux-Instances.
3. Konfigurieren Sie das von Ihnen hinzugefügte Amazon-EBS-Volume als Upload-Puffer oder Cache-Speicher. Anweisungen finden Sie unter Verwaltung von lokalen Festplatten für Ihr Storage Gateway.

In manchen Fällen stellen Sie möglicherweise fest, dass die Speicherkapazität, die Sie für den Upload-Puffer konfiguriert haben, nicht benötigt wird.

So entfernen Sie ein Amazon-EBS-Volume

> **Warning**
>
> Diese Schritte gelten nur für Amazon-EBS-Volumes, die als Upload-Pufferspeicher zugewiesen wurden, nicht für Volumes, die dem Cache zugewiesen sind. Wenn Sie ein Amazon EBS-Volume, das als Cache-Speicher zugeordnet ist, von einem Tape Gateway entfernen, haben die virtuellen Bänder des Gateways den Status NICHT WIEDERHERSTELLBAR und es besteht das Risiko von Datenverlust. Weitere Informationen zum Status NICHT WIEDERHERSTELLBAR finden Sie unter Grundlegendes zu Bandstatusinformationen in einer VTL.

1. Fahren Sie das Gateway mit dem im Abschnitt Herunterfahren der Gateway-VM beschriebenen Verfahren herunter.
2. Trennen Sie das Amazon-EBS-Volume von Ihrer Amazon-EC2-Instance. Eine Anleitung hierzu finden Sie unter Trennen eines Amazon-EBS-Volumes von einer Instance im Amazon-EC2-Benutzerhandbuch für Linux-Instances.
3. Löschen Sie das Amazon-EBS-Volume. Eine Anleitung hierzu finden Sie unter Löschen eines Amazon-EBS-Volumes im Amazon-EC2-Benutzerhandbuch für Linux-Instances.
4. Starten Sie das Gateway mit dem im Abschnitt Herunterfahren der Gateway-VM beschriebenen Verfahren.

Arbeiten mit VTL-Geräten

Ihre Tape-Gateway-Einrichtung bietet die folgenden SCSI-Geräte, die Sie bei der Aktivierung Ihres Gateways auswählen.

Themen

- Auswählen eines Medienwechslers nach der Gateway-Aktivierung
- Aktualisieren des Gerätetreibers für den Medienwechsler
- Anzeigen von Barcodes für Bänder in Microsoft System Center DPM

Bei Medienwechslern AWS Storage Gateway funktioniert mit Folgendem:

- AWS-Gateway-VTL: Dieses Gerät wird mit dem Gateway bereitgestellt.
- STK-L700: Diese Geräteemulation wird mit dem Gateway bereitgestellt.

  Bei der Aktivierung des Tape Gateways wählen Sie Ihre Sicherungsanwendung aus der Liste aus und das Speicher-Gateway verwendet den entsprechenden Medienwechsler. Wenn Ihre Sicherungsanwendung nicht aufgeführt ist, wählen Sie Other (Sonstiges) und dann den Medienwechsler aus, der mit der Sicherungsanwendung funktioniert.

  Welchen Typ von Medienwechsler Sie wählen, hängt von der Sicherungsanwendung ab, die Sie verwenden möchten. In der folgenden Tabelle sind Sicherungsanwendungen von Drittanbietern aufgeführt, die getestet wurden und für kompatibel mit Tape Gateways befunden wurden. Diese Tabelle enthält den für jede Sicherungsanwendung empfohlenen Medienwechslertyp.

Sicherungsanwendung	Medienwechslertyp
Arcserve Backup	`AWS-Gateway-VTL`
Bacula Enterprise V10.x	`AWS-Gateway-VTL` oder `STK-L700`
Commvault V11	`STK-L700`
Dell EMC NetWorker 19.5	`AWS-Gateway-VTL`
IBM Spectrum Protect v8.1.10	`IBM-03584L32-0402`
Micro Focus (HPE) Data Protector 9 oder 11.x	`AWS-Gateway-VTL`
Microsoft System Center 2012 R2 oder 2016 Data Protection Manager	`STK-L700`
NovaStor DataCenter/Netzwerk 6.4 oder 7.1	`STK-L700`
Bol NetVault Backup 12.4 oder 13.x	`STK-L700`
Veeam Backup & Replication 11A	`AWS-Gateway-VTL`
Veritas Backup Exec 2014 oder 15 oder 16 oder 20 oder 22.x	`AWS-Gateway-VTL`

Sicherungsanwendung	Medienwechslertyp
Veritas Backup Exec 2012 **Note** Veritas unterstützt Backup Exec 2012 nicht mehr.	`STK-L700`
Ver Bols NetBackup Version 7.x oder 8.x	`AWS-Gateway-VTL`

Important

Wir empfehlen Ihnen dringend, den Medienwechsler zu wählen, der für Ihre Sicherungsanwendung aufgeführt ist. Andere Medienwechsler funktionieren möglicherweise nicht richtig. Sie können einen anderen Medienwechslertyp auswählen nachdem das Gateway aktiviert worden ist. Weitere Informationen finden Sie unter Auswählen eines Medienwechslers nach der Gateway-Aktivierung.

Bei Bandlaufwerken funktioniert Storage Gateway mit Folgendem:

- IBM-ULT3580-TD5 – Diese Geräteemulation wird mit dem Gateway bereitgestellt.

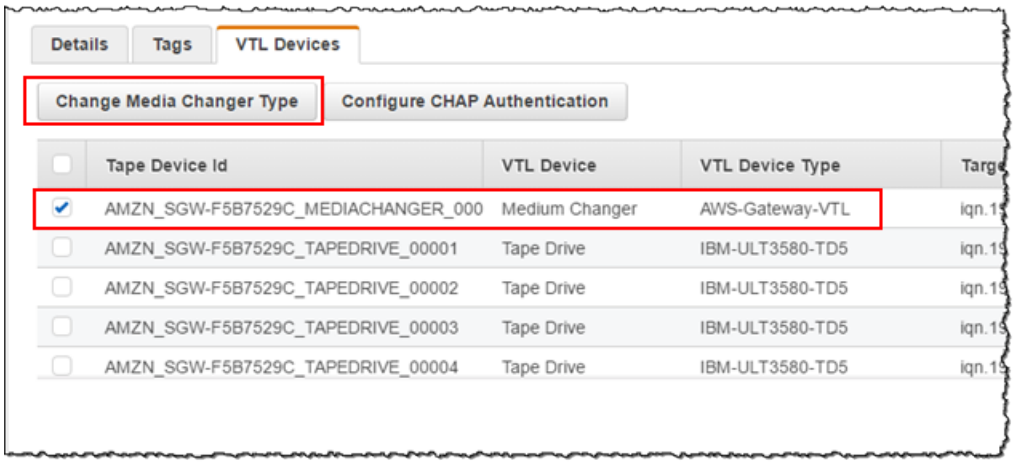
Auswählen eines Medienwechslers nach der Gateway-Aktivierung

Nach der Aktivierung des Gateways können Sie einen anderen Medienwechslertyp auswählen.

So wählen Sie einen anderen Medienwechsler nach der Gateway-Aktivierung aus

1. Stoppen Sie alle zugehörigen Aufträge, die in der Sicherungssoftware ausgeführt werden.
2. Öffnen Sie auf dem Windows-Server das Fenster mit den iSCSI-Initiator-Eigenschaften.
3. Wählen Sie die Registerkarte Targets (Ziele), um die erkannten Ziele anzuzeigen.
4. Wählen Sie im Bereich mit den erkannten Zielen den Medienwechsler, den Sie ändern möchten, wählen Sie Disconnect (Verbindung trennen) und dann OK.

5. Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Gateways und dann das Gateway aus, dessen Medienwechsler Sie ändern möchten.
6. Wählen Sie die Registerkarte VTL Devices (VTL-Geräte) aus, wählen Sie den Medienwechsler, den Sie ändern möchten, und klicken Sie dann auf die Schaltfläche Change Media Changer (Medienwechsler ändern).



7. Wählen Sie im angezeigten Dialogfeld zum Ändern des Medienwechslertyps den gewünschten Medienwechsler aus dem Dropdown-Listenfeld aus und klicken Sie dann auf Save (Speichern).

Aktualisieren des Gerätetreibers für den Medienwechsler

1. Öffnen Sie den Geräte-Manager auf dem Windows-Server und erweitern Sie die Struktur Medium Changer devices (Wechselmediengeräte) .
2. Öffnen Sie das Kontextmenü (rechte Maustaste) für Unbekannter Medienwechsler und wählen Sie Treibersoftware aktualisieren, um das Fenster Treibersoftware aktualisieren – unbekannter Medienwechsler zu öffnen.
3. Wählen Sie im Abschnitt How do you want to search for driver software? (Wie möchten Sie nach Treibersoftware suchen?) die Option Browse my computer for driver software (Auf dem Computer nach Treibersoftware suchen).
4. Wählen Sie Let me pick from a list of device drivers on my computer (Aus einer Liste von Gerätetreibern auf dem Computer auswählen).

> **Note**
>
> Wir empfehlen die Verwendung des Sony TSL-A500C-Autoloader-Treibers mit der Sicherungssoftware Veeam Backup & Replication 11A und Microsoft System Center

Data Protection Manager. Dieser Treiber von Sony wurde mit diesen Arten von Sicherungssoftware bis einschließlich Windows Server 2019 getestet.

5. Deaktivieren Sie im Bereich Select the device driver you want to install for this hardware (Wählen Sie den für diese Hardware zu installierenden Gerätetreiber.) das Kontrollkästchen Show compatible hardware (Kompatible Hardware anzeigen), wählen Sie Sony in der Liste Manufacturer (Hersteller), wählen Sie Sony TSL-A500C-Autoloader in der Liste Model (Modell) und klicken Sie dann auf Next (Weiter).
6. Ein Warnungsfeld wird angezeigt. Klicken Sie in diesem Feld auf Yes (Ja). Wenn der Treiber erfolgreich installiert wurde, schließen Sie das Fenster Update drive software (Treibersoftware aktualisieren).

Anzeigen von Barcodes für Bänder in Microsoft System Center DPM

Wenn Sie den Medienwechslertreiber für Sony TSL-A500C Autoloader verwenden, zeigt Microsoft System Center Data Protection Manager nicht automatisch Barcodes für virtuelle Bänder an, die in Storage Gateway erstellt wurden. Wenn Sie Barcodes für Ihre Bänder korrekt anzeigen möchten, ändern Sie den Treiber des Medienwechslers auf So/StorageTek Bibliothek.

Anzeigen von Barcodes

1. Stellen Sie sicher, dass alle Sicherungsaufträge abgeschlossen sind und keine Aufgaben ausstehend oder in Bearbeitung sind.
2. Werfen Sie die Bänder aus, verschieben Sie sie zum Offline-Speicher („S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep Archive“) und beenden Sie die DPM-Administratorkonsole. Weitere Informationen zum Auswerfen eines Bands in DPM finden Sie unter Archivieren eines Bands mithilfe von DPM.
3. Wählen Sie unter Administrative Tools die Option Services aus und öffnen Sie das Kontextmenü (rechte Maustaste) für DPM Service im Bereich Detail. Wählen Sie dann Properties (Eigenschaften) aus.
4. Stellen Sie auf der Registerkarte General (Allgemein) sicher, dass der Startup type (Starttyp) auf Automatic (Automatisch) festgelegt ist, und wählen Sie Stop (Stopp) aus, um den DPM-Dienst zu stoppen.
5. Rufen Sie die StorageTek Treiber aus dem Microsoft Update Catalog auf der Microsoft-Website ab.

> **Note**
>
> Beachten Sie die unterschiedlichen Treiber für die verschiedenen Größen.

Wählen Sie für Größe 18K x86-Treiber.

Wählen Sie für Größe 19K, x64-Treiber.

6. Öffnen Sie den Geräte-Manager auf Ihrem Windows-Server und erweitern Sie die Struktur Medium Changer Devices (Wechselmediengeräte).
7. Öffnen Sie das Kontextmenü (rechte Maustaste) für Unbekannter Medienwechsler und wählen Sie Treibersoftware aktualisieren, um das Fenster Treibersoftware aktualisieren – unbekannter Medienwechsler zu öffnen.
8. Navigieren Sie zum Pfad des neuen Treiberortes und installieren Sie ihn. Der Treiber wird als So/StorageTek Library angezeigt. Die Bandlaufwerke verbleiben als IBM ULT3580-TD5 SCSI-Sequenzgerät.
9. Starten Sie den DPM-Server neu.
10. Erstellen Sie in der Storage-Gateway-Konsole neue Bänder.
11. Öffnen Sie die DPM-Administratorkonsole und wählen Sie Management und dann Rescan for new tape libraries (Nach neuen Bandbibliotheken suchen) aus. Sie sollten die So/StorageTek Bibliothek sehen.
12. Wählen Sie die Bibliothek und dann Inventory (Bestand) aus.
13. Wählen Sie Add Tapes (Bänder hinzufügen) aus, um neue Bänder in DPM hinzuzufügen. Für die neuen Bänder sollte nun der Barcode angezeigt werden.

Arbeiten mit Bändern

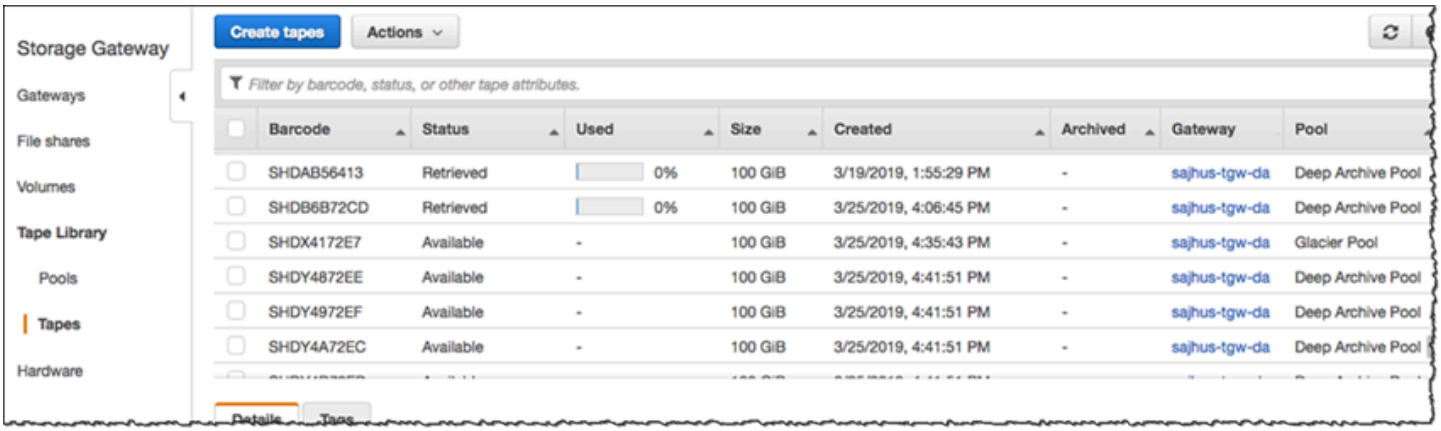
Storage Gateway stellt für jedes Tape Gateway, das Sie aktivieren, eine virtuelle Bandbibliothek (Virtual Tape Library, VTL) bereit. Die Bibliothek enthält anfangs keine Bänder, aber Sie können jederzeit Bänder erstellen. Ihre Anwendung kann von allen Bändern lesen und auf alle Bänder schreiben, die auf Ihrem Tape Gateway verfügbar sind. Der Status eines Bands muss AVAILABLE sein, damit Sie auf das Band schreiben können. Diese Bänder werden von Amazon Simple Storage Service (Amazon S3) unterstützt. Wenn Sie also auf diese Bänder schreiben, speichert das

Tape Gateway Daten in Amazon S3. Weitere Informationen finden Sie unter Grundlegendes zu Bandstatusinformationen in einer VTL.

Themen

- Archivieren von Bändern
- Abbrechen der Bandarchivierung

Die Bandbibliothek zeigt Bänder in Ihrem Tape Gateway an. Die Bibliothek zeigt den Barcode, den Status und die Größe, die verwendete Menge des Bands und das Gateway, dem das Band zugeordnet ist.



Wenn Sie über eine große Anzahl von Bändern in der Bibliothek verfügen, unterstützt die Konsole die Suche nach Bändern anhand des Barcodes, des Status oder beider. Wenn Sie nach Barcode suchen, können Sie nach Status und Gateway filtern.

So suchen Sie nach Barcode, Status und Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie im Navigationsbereich Tapes (Bänder) und geben Sie dann einen Wert in das Suchfeld ein. Der Wert kann der Barcode, der Status oder das Gateway sein. Standardmäßig sucht Storage Gateway nach allen virtuellen Bändern. Sie können die Suche jedoch auch nach Status filtern.

   Wenn Sie nach Status filtern, werden Bänder, die Ihren Kriterien entsprechen, in der Bibliothek in der Storage-Gateway-Konsole angezeigt.

Wenn Sie nach Gateway filtern, werden Bänder, die dem Gateway zugeordnet sind, in der Bibliothek in der Storage-Gateway-Konsole angezeigt.

> **Note**
>
> Standardmäßig zeigt Storage Gateway alle Bänder unabhängig vom Status an.

Archivieren von Bändern

Sie können die virtuellen Bänder, die sich in Ihrem Tape Gateway befinden, archivieren. Wenn Sie ein Band archivieren, verschiebt Storage Gateway das Band in das Archiv.

Um ein Band zu archivieren, verwenden Sie Ihre Backup-Software. Der Bandarchivierungsprozess besteht aus drei Phasen entsprechend dem Bandstatus IN TRANSIT TO VTS (IN DER ÜBERTRAGUNG ZU VTS), ARCHIVING (ARCHIVIERUNG WIRD AUSGEFÜHRT) und ARCHIVED (ARCHIVIERT):

- Um ein Band zu archivieren, verwenden Sie den Befehl der von Ihrer Backup Anwendung bereitgestellt wird. Wenn der Archivierungsprozess beginnt, wechselt der Bandstatus zu TRANSIT TO VTS (ÜBERTRAGUNG ZU VTS) und das Band ist für Ihre Backup-Anwendung nicht länger verfügbar. In dieser Phase lädt Ihr Tape Gateway Daten in hoch AWS. Bei Bedarf können Sie die Archivierung die am laufen ist, abbrechen. Weitere Informationen, über Abbrechen des Archivierens, finden Sie unter Abbrechen der Bandarchivierung.

  > **Note**
  >
  > Die Schritte zum Archivieren eines Bandes hängt von Ihrer Sicherungsanwendung ab. Detaillierte Anweisungen finden Sie in der Dokumentation zu Ihrer Sicherungsanwendung.

- Nachdem der Daten-Upload in AWS abgeschlossen ist, ändert sich der Bandstatus in ARCHIVING und Storage Gateway beginnt mit dem Verschieben des Bands in das Archiv. Sie können den Archivierungsprozess zu diesem Zeitpunkt nicht abbrechen.
- Nachdem das Band in das Archiv verschoben wurde, ändert sich der Status in ARCHIVED (ARCHIVIERT) und Sie können das Band mit allen Ihren Gateways abrufen. Weitere Informationen, zum Bänderabruf, finden Sie unter Abrufen archivierter Bänder.

Die Schritte zum Archivieren eines Bandes hängen von Ihrer Backup Software ab. Anweisungen zum Archivieren eines Bands mithilfe der Symantec- NetBackup Software finden Sie unter Archivieren des Bands.

Abbrechen der Bandarchivierung

Nachdem Sie die Archivierung eines Bandes gestartet haben, kann es vorkommen, dass Sie das Band wieder benötigen. Beispielsweise möchten Sie den Archivierungsprozess abbrechen und das Band zurück haben, weil der Archivierungsprozess zu lange dauert oder Sie Daten von dem Band lesen möchten. Ein Band, das archiviert wird, durchläuft drei Status, wie im Folgenden gezeigt:

- BEI DER ÜBERTRAGUNG ZU VTS: Das Tape Gateway lädt Daten in AWS hoch.
- ARCHIVIERUNG: Das Hochladen der Daten ist beendet und das Tape Gateway verschiebt das Band ins Archiv.
- ARCHIVED: Das Band wurde ins Archiv verschoben und steht zum Abruf zur Verfügung.

Sie können die Archivierung nur abbrechen, wenn der Status des Bandes IN TRANSIT TO VTS lautet. Abhängig von Faktoren wie Upload-Bandbreite und Menge der Daten, die hochgeladen werden, kann der Status in der Storage-Gateway-Konsole angezeigt werden oder nicht. Um eine Bandarchivierung abzubrechen, verwenden Sie die -CancelRetrievalAktion in der -API-Referenz.

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 unter ActivateGateway in der Storage Gateway-API-Referenz .

> **Note**
>
> Gateway-Aktivierungsschlüssel laufen nach 30 Minuten ab, wenn sie nicht verwendet werden.

Die Anforderung, die Sie an die Gateway-VM stellen, enthält die AWS Region, in der die Aktivierung stattfindet. 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 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 Webanforderungen 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`*: Die IPv4-Adresse Ihres Gateways, z. B. `172.31.29.201`
> - *`gateway_type`* – Der Typ des Gateways, das Sie aktivieren möchten, z. B. `STORED`, `VTLCACHED`, `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 .
- *vpc_endpoint*: Der VPC-Endpunktname für Ihr Gateway, z. B. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`.

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, 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

Das folgende Beispiel veranschaulicht, 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 bei der lokalen Konsole an. Wenn Sie auf einem Windows-Computer eine Verbindung mit Ihrer Amazon EC2-Instance herstellen, melden Sie sich als admin an.
2. 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 die AWS Region ein, in der Sie Ihr Gateway aktivieren möchten.
5. Geben Sie als Netzwerktyp 1 für „Öffentlich“ oder 2 für „VPC-Endpunkt“ ein.

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

Verbinden von iSCSI-Initiatoren

Bei der Verwaltung Ihres Gateways arbeiten Sie mit Volumes oder VTL-Geräten (Virtual Tape Library), die als iSCSI-Ziele (internet Small Computer System Interface) verfügbar gemacht werden. Bei Volume-Gateways sind iSCSI-Ziele Volumes. Bei Tape Gateways sind die Ziele VTL-Geräte. Zu Ihren Aufgaben gehören unter anderem die Einrichtung einer Verbindung mit diesen Zielen, die Anpassung der iSCSI-Einstellungen, die Anbindung eines Red Hat Linux-Clients und die Konfiguration der CHAP (Challenge Handshake Authentication Protocol)-Authentifizierung.

Themen

Der iSCSI-Standard ist ein IP (Internet Protocol)-basierter Standard für Speichernetzwerke, der die Initiierung und Verwaltung von Verbindungen zwischen IP-basierten Speichergeräten und Clients regelt. Nachfolgend haben wir eine Liste mit Definitionen von Begriffen zusammengestellt, mit denen iSCSI-Verbindungen und ihre Komponenten beschrieben werden.

iSCSI-Initiator

Hierbei handelt es sich um die Client-Komponente eines iSCSI-Netzwerks. Der Initiator sendet Anforderungen an das iSCSI-Ziel. Initiatoren können als Software oder als Hardware implementiert werden. Storage Gateway unterstützt nur Software-Initiatoren.

iSCSI-Ziel

Ein iSCSI-Ziel ist die Serverkomponente eines iSCSI-Netzwerks, die Anforderungen von Initiatoren empfängt und beantwortet. Jedes Ihrer Volumes wird als iSCSI-Ziel verfügbar gemacht. Dabei darf mit jedem iSCSI-Ziel jeweils immer nur ein einziger iSCSI-Initiator verbunden sein.

Microsoft iSCSI-Initiator

Hierbei handelt es sich um ein Softwareprogramm auf Microsoft Windows-Computern. Dieses Programm ermöglicht die Verbindung zwischen einem Client-Computer (dem Computer, auf dem

die Anwendung ausgeführt wird, deren Daten auf das Gateway geschrieben werden sollen) und einem externen iSCSI-basierten Array (dem Gateway). Die Verbindung wird über die Ethernet-Netzwerkadapterkarte des Host-Computers hergestellt. Der Microsoft iSCSI-Initiator wurde mit Storage Gateway unter Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019 validiert. Der Initiator ist in diese Betriebssysteme integriert.

Red Hat-iSCSI-Initiator

Das RPM (Resource Package Manager)-Paket `iscsi-initiator-utils` stellt einen als Software implementierten iSCSI-Initiator für Red Hat Linux bereit. Es enthält einen Server-Daemon für das iSCSI-Protokoll.

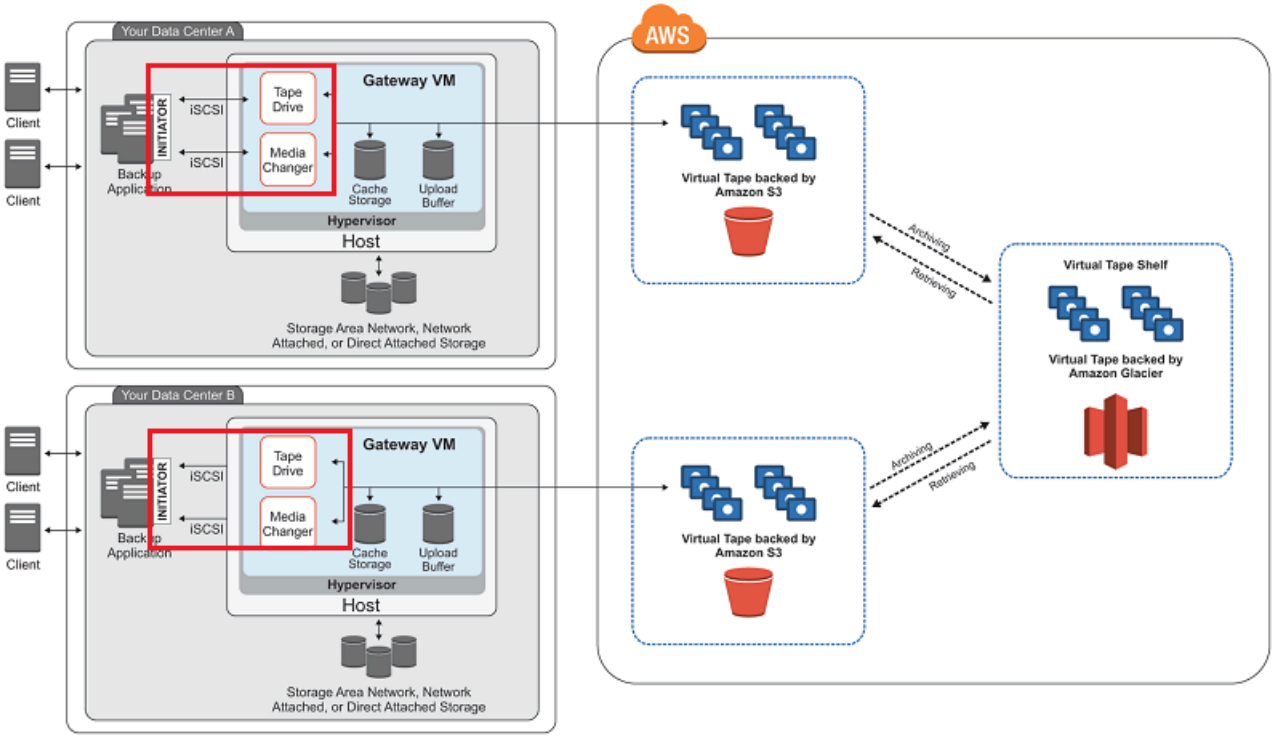
Alle Typen von Gateways lassen sich mit iSCSI-Geräten verbinden und diese Verbindungen können Sie auch anpassen. Die entsprechenden Anleitungen finden Sie nachfolgend.

Verbinden von VTL-Geräten mit einem Windows-Client

Ein Tape Gateway macht mehrere Bandlaufwerke und einen Medienwechsler, zusammenfassend VTL-Geräte genannt, als iSCSI-Ziele verfügbar. Weitere Informationen finden Sie unter Voraussetzungen.

> **Note**
>
> Mit jedem iSCSI-Ziel darf jeweils maximal eine Anwendung verbunden werden.

Die folgende Abbildung verdeutlicht die Position des iSCSI-Ziels im größeren Zusammenhang der Storage-Gateway-Architektur. Weitere Informationen zur Storage-Gateway-Architektur finden Sie unter Funktionsweise von Tape Gateway (Architektur).

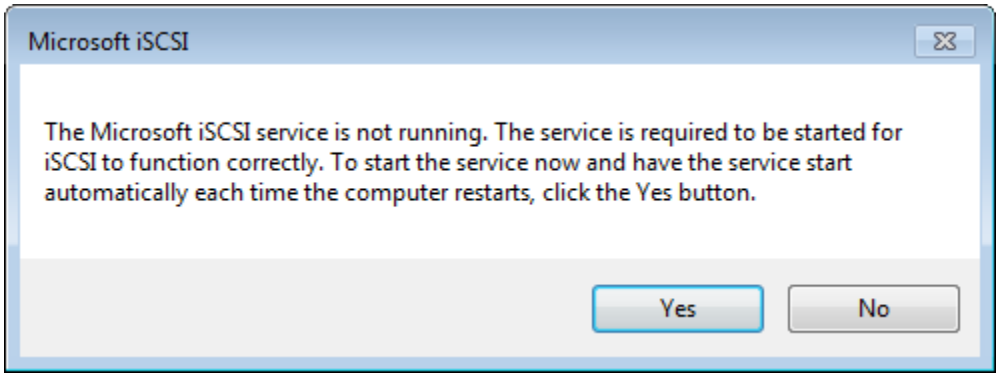


Einen Windows-Client verbinden Sie wie folgt mit VTL-Geräten:

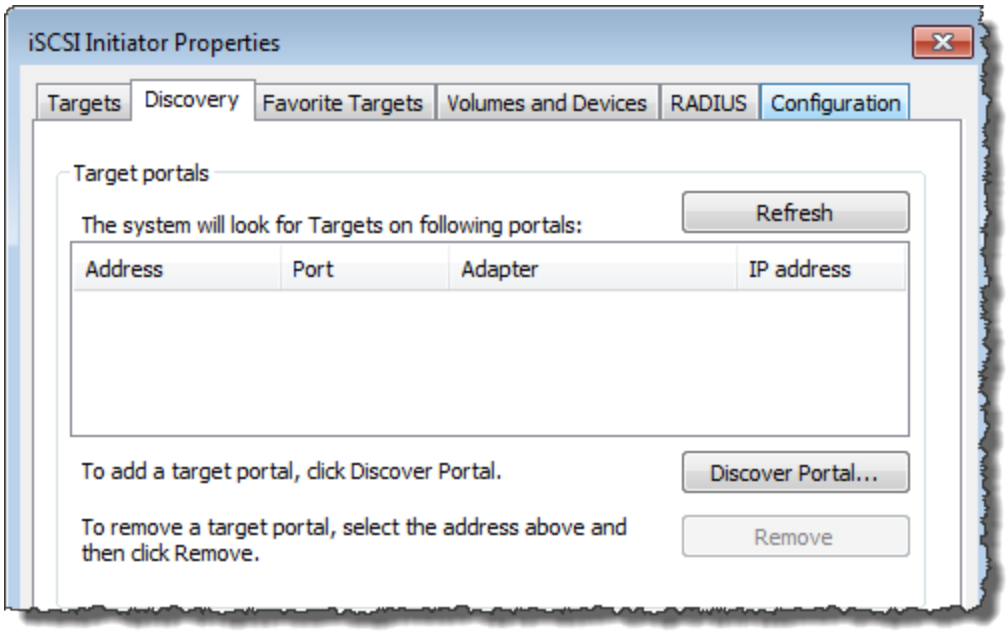
1. Geben Sie im Menü Start Ihres Windows-basierten Client-Computers **`iscsicpl.exe`** in das Feld Programme und Dateien durchsuchen ein, suchen Sie nach dem iSCSI-Initiator-Programm und führen Sie es aus.

   > **Note**
   >
   > Sie benötigen Administratorrechte auf dem Client-Computer, um den iSCSI-Initiator ausführen zu können.

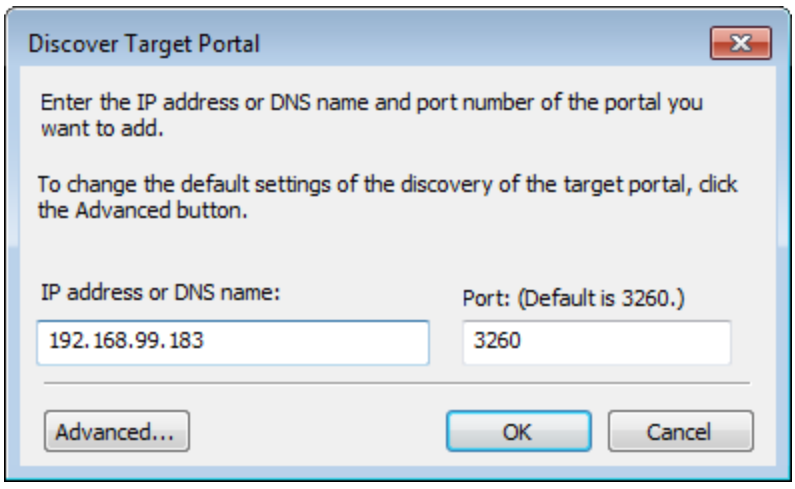
2. Klicken Sie bei Aufforderung auf Ja, um den Microsoft iSCSI-Initiator-Dienst zu starten.



3. Wählen Sie im Dialogfeld iSCSI Initiator-Eigenschaften die Registerkarte Ermittlung aus und klicken Sie dann auf Portal ermitteln.



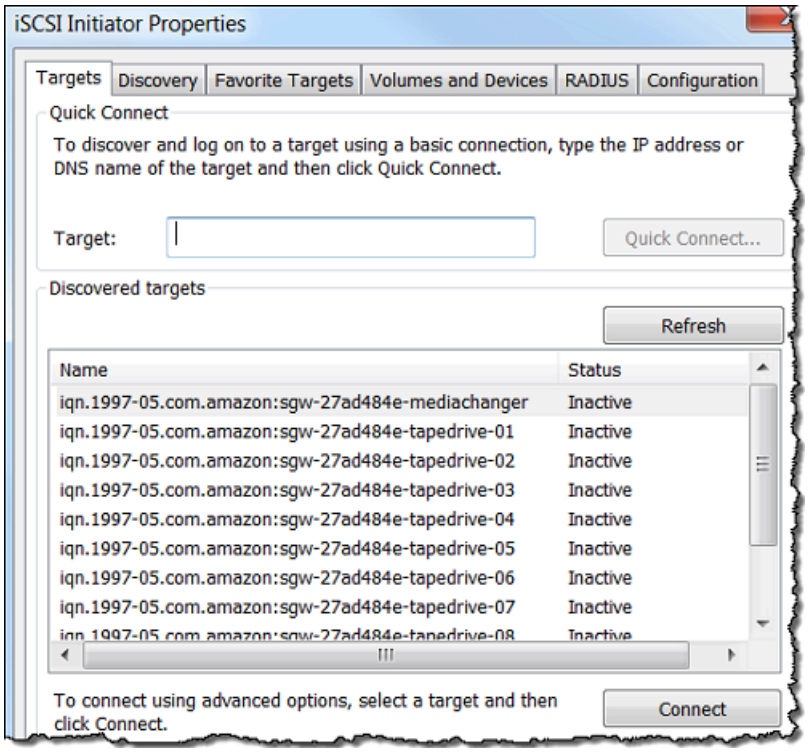
4. Geben Sie im Dialogfeld Zielportal ermitteln unter IP-Adresse oder DNS-Name die IP-Adresse Ihres Tape Gateways ein und klicken Sie auf OK. Die IP-Adresse Ihres Gateways finden Sie auf der Registerkarte Gateway in der Storage-Gateway-Konsole. Wenn Sie Ihr Gateway in einer Amazon-EC2-Instance bereitgestellt haben, finden Sie die öffentliche IP-Adresse oder die DNS-Adresse auf der Registerkarte Beschreibung in der Amazon-EC2-Konsole.



> **Warning**
>
> Auf Gateways, die in einer Amazon-EC2-Instance bereitgestellt werden, kann nicht über eine öffentliche Internetverbindung zugegriffen werden. Die Elastic IP-Adresse der Amazon-EC2-Instance kann nicht als Zieladresse verwendet werden.

5. Wählen Sie die Registerkarte Targets (Ziele) und dann Refresh (Aktualisieren) aus. Anschließend werden im Feld Erkannte Ziele alle 10 Bandlaufwerke und der Medienwechsler angezeigt. Der Status der Ziele ist Inactive (Inaktiv).

   Auf dem Screenshot unten sehen Sie die erkannten Ziele.

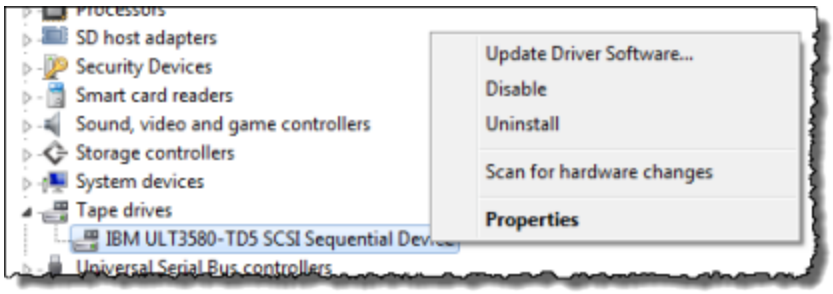


6. Wählen Sie das erste Gerät aus und klicken Sie auf Connect (Verbinden). Die einzelnen Geräte müssen nacheinander verbunden werden.
7. Klicken Sie im Dialogfeld Mit Ziel verbinden auf OK.
8. Wiederholen Sie Schritt 6 und Schritt 7 für jedes der Geräte, um sie alle zu verbinden, und klicken Sie anschließend im Dialogfeld Eigenschaften von iSCSI-Initiator auf OK.

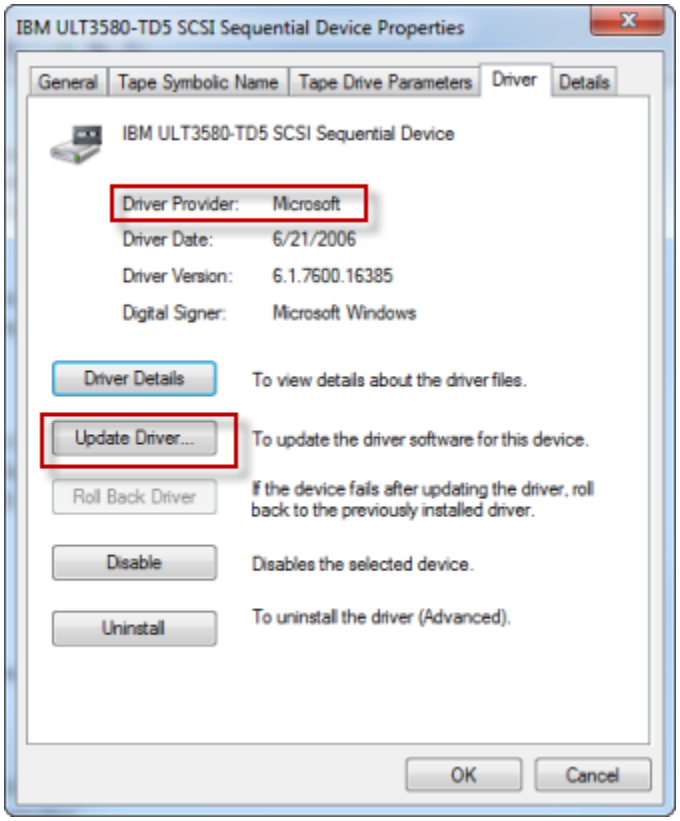
Auf einem Windows-Client muss als Treiberanbieter des Bandlaufwerks Microsoft festgelegt sein. Gehen Sie wie folgt vor, um zu überprüfen, welcher Treiberanbieter festgelegt ist. Aktualisieren Sie ggf. den Treiber und den Anbieter:

So überprüfen Sie den Treiberanbieter und aktualisieren (falls erforderlich) den Anbieter und Treiber auf einem Windows-Client

1. Starten Sie auf Ihrem Windows-Client den Geräte-Manager.
2. Erweitern Sie Tape drives (Bandlaufwerke), öffnen Sie mit einem Rechtsklick das Kontextmenü eines der Bandlaufwerke und klicken Sie auf Properties (Eigenschaften).



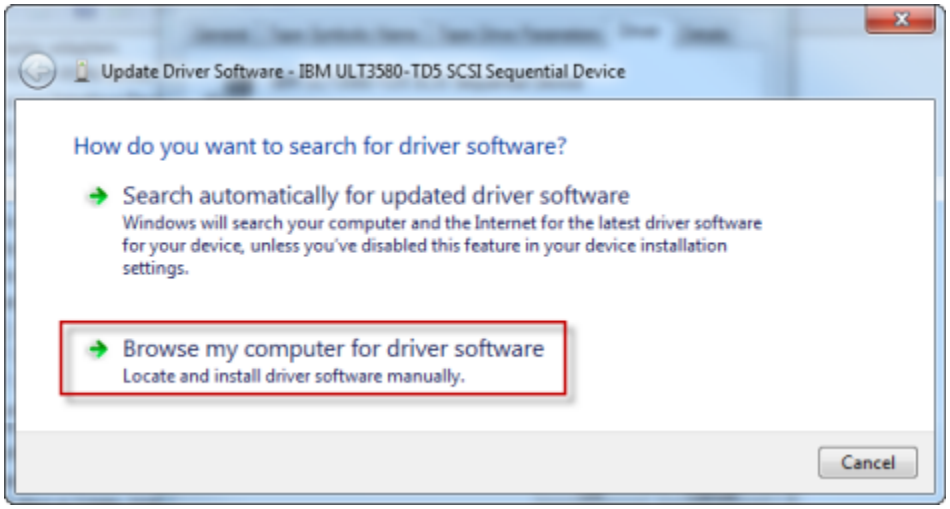
3. Überprüfen Sie auf der Registerkarte Treiber des Dialogfelds Geräteeigenschaften, ob Microsoft der Treiberanbieter ist.



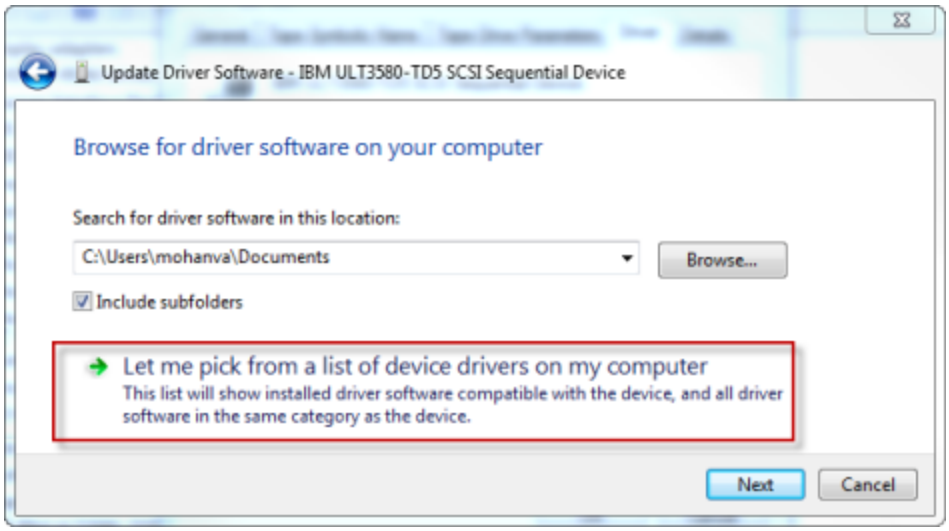
4. Wenn Treiberanbieter nicht Microsoft lautet, legen Sie den Wert wie folgt fest:

   a. Wählen Sie Update Driver (Treiber aktualisieren) aus.

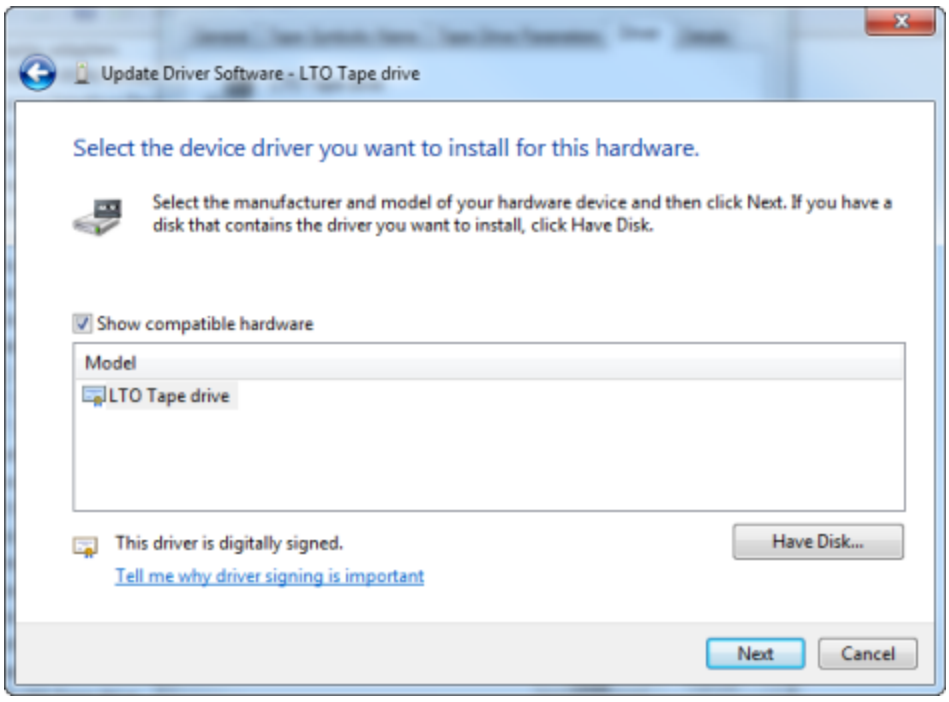
   b. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Browse my computer for driver software (Auf dem Computer nach Treibersoftware suchen) aus.



c. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Let me pick from a list of device drivers on my computer (Aus einer Liste von Gerätetreibern auf dem Computer auswählen) aus.



d. Wählen Sie LTO Tape drive (LTO-Bandlaufwerk) aus und klicken Sie auf Next (Weiter).



e. Wählen Sie Schließen aus, um das Fenster Treibersoftware aktualisieren zu schließen, und überprüfen Sie, ob Treiberanbieter nun auf den Wert Microsoft festgelegt ist.

5. Aktualisieren Sie jedes Bandlaufwerk, in dem Sie jeweils die Schritte 4.1 bis 4.5 wiederholen.

Verbinden von Volumes oder VTL-Geräten mit einem Linux-Client

Wenn Sie mit Red Hat Enterprise Linux (RHEL) arbeiten, verwenden Sie das RPM-Paket `iscsi-initiator-utils`, um eine Verbindung mit Ihren Gateway-iSCSI-Zielen (Volumes oder VTL-Geräten) herzustellen.

So verbinden Sie einen Linux-Client mit den iSCSI-Zielen

1. Installieren Sie das RPM-Paket `iscsi-initiator-utils`, falls es noch nicht auf Ihrem Client installiert ist.

   Verwenden Sie den folgenden Befehl zum Installieren des Pakets.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. Stellen Sie sicher, dass der iSCSI-Daemon ausgeführt wird.

   a. Führen Sie einen der nachfolgenden Befehl aus, um zu überprüfen, ob der iSCSI-Daemon ausgeführt wird.

      Verwenden Sie unter RHEL 5 oder 6 den folgenden Befehl.

      ```
      sudo /etc/init.d/iscsi status
      ```

      Verwenden Sie unter RHEL 7 den folgenden Befehl.

      ```
      sudo service iscsid status
      ```

   b. Falls der Statusbefehl nicht running als Status zurückgibt, starten Sie den Daemon mit einem der nachfolgenden Befehle.

      Verwenden Sie unter RHEL 5 oder 6 den folgenden Befehl.

      ```
      sudo /etc/init.d/iscsi start
      ```

      Verwenden Sie unter RHEL 7 den folgenden Befehl. Unter RHEL 7 ist es in der Regel nicht nötig, den Dienst `iscsid` explizit zu starten.

      ```
      sudo service iscsid start
      ```

3. Führen Sie den folgenden Erkennungsbefehl aus, um die auf dem Gateway als Ziele definierten Volumes oder VTL-Geräte zu erkennen:

   ```
   sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
   ```

   Ersetzen Sie die IP-Adresse Ihres Gateways für die Variable *[GATEWAY_IP]* im vorhergehenden Befehl. Sie finden die Gateway-IP in der Storage-Gateway-Konsole im Eigenschaftenbereich iSCSI-Zielinfo eines Volumes.

   Die Ausgabe des Entdeckungsbefehl gleicht der folgenden Beispielausgabe.

   Für Volume Gateways: *[GATEWAY_IP]*`:3260, 1 iqn.1997-05.com.amazon:myvolume`

   Für Tape Gateways: `iqn.1997-05.com.amazon:`*[GATEWAY_IP]*`-tapedrive-01`

   Ihr qualifizierter iSCSI-Name (IQN) wird nicht mit dem oben angegebenen identisch sein, da IQN-Werte für jede Organisation eindeutig sind. Der Name des Ziels ist der Name, den Sie angegeben haben, als Sie das Volume erstellt haben. Sie finden diesen Zielnamen auch im Eigenschaftenbereich iSCSI-Zielinfo, wenn Sie in der Storage-Gateway-Konsole ein Volume auswählen.

4. Verwenden Sie den nachfolgenden Befehl, um eine Verbindung mit einem Ziel herzustellen.

   Beachten Sie, dass Sie in dem Verbindungsbefehl die korrekte *[GATEWAY_IP]* und den korrekten IQN angeben müssen.

   > **Warning**
   >
   > Auf Gateways, die in einer Amazon-EC2-Instance bereitgestellt werden, kann nicht über eine öffentliche Internetverbindung zugegriffen werden. Die Elastic IP-Adresse der Amazon-EC2-Instance kann nicht als Zieladresse verwendet werden.

   ```
   sudo /sbin/iscsiadm --mode node --targetname
    iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
   ```

5. Überprüfen Sie mit dem folgenden Befehl, ob das Volume mit dem Client-Computer (Initiator) verbunden ist.

```
ls -l /dev/disk/by-path
```

Die Ausgabe des Befehls gleicht der folgenden Beispielausgabe.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

Wir empfehlen Ihnen dringend, nach der Einrichtung des Initiators Ihre iSCSI-Einstellungen wie unter Anpassen Ihrer Linux iSCSI-Einstellungen beschrieben anzupassen.

Anpassen von iSCSI-Einstellungen

Es wird dringend empfohlen, nach der Einrichtung des Initiators Ihre iSCSI-Einstellungen anzupassen, um die Trennung der Verbindung des Initiators zum Ziel zu vermeiden.

Durch Erhöhen der iSCSI-Werte für Zeitbegrenzungen, wie in den folgenden Schritten beschrieben, wird Ihre Anwendung besser im Umgang mit Schreibvorgängen, die viel Zeit in Anspruch nehmen und besser in anderen transienten Aufgaben wie Netzwerk-Unterbrechungen.

> **Note**
>
> Bevor Sie Änderungen an der Registrierung vornehmen, sollten Sie eine Sicherungskopie der Registrierung vornehmen. Informationen zum Erstellen einer Sicherungskopie und andere bewährte Methoden, die bei der Arbeit mit der Registrierung zu beachten sind, finden Sie unter Bewährte Methoden für die Registrierung in der Microsoft TechNet Library .

Themen

- Anpassen der Windows iSCSI-Einstellungen
- Anpassen Ihrer Linux iSCSI-Einstellungen
- Anpassen der Linux-Festplatten-Timeout-Einstellungen für Volume Gateways

Anpassen der Windows iSCSI-Einstellungen

Bei einer Tape-Gateway-Einrichtung besteht das Herstellen einer Verbindung mit Ihren VTL-Geräten unter Verwendung eines Microsoft iSCSI-Initiators aus zwei Schritten:

1. Verbinden Sie die Tape-Gateway-Geräte mit Ihrem Windows Client.
2. Wenn Sie eine Backup-Anwendung verwenden, konfigurieren Sie die Anwendung für die Verwendung der Geräte.

Das Erste-Schritte-Beispiel Einrichtung enthält Anweisungen für beide dieser folgenden Schritte. Es verwendet die Symantec NetBackup -Sicherungsanwendung. Weitere Informationen finden Sie unter Verbinden von VTL-Geräten und Konfigurieren von NetBackup Speichergeräten.

Um Ihre Windows iSCSI-Einstellungen anzupassen

1. Erhöhen Sie die maximale Dauer für die Anforderungen in der Warteschlange.

   a. Starten Sie den Registrierungs-Editor (`Regedit.exe`).

   b. Navigieren Sie zu dem globalen eindeutigem Initiator GUID-Schlüssel für die Geräte Klasse mit iSCSI-Controller Einstellungen, wie folgt angezeigt.

   > **Warning**
   >
   > Stellen Sie sicher, dass Sie im CurrentControlSet Unterschlüssel und nicht in einem anderen Kontrollsatz wie ControlSet001 oder ControlSet002 arbeiten.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
   ```

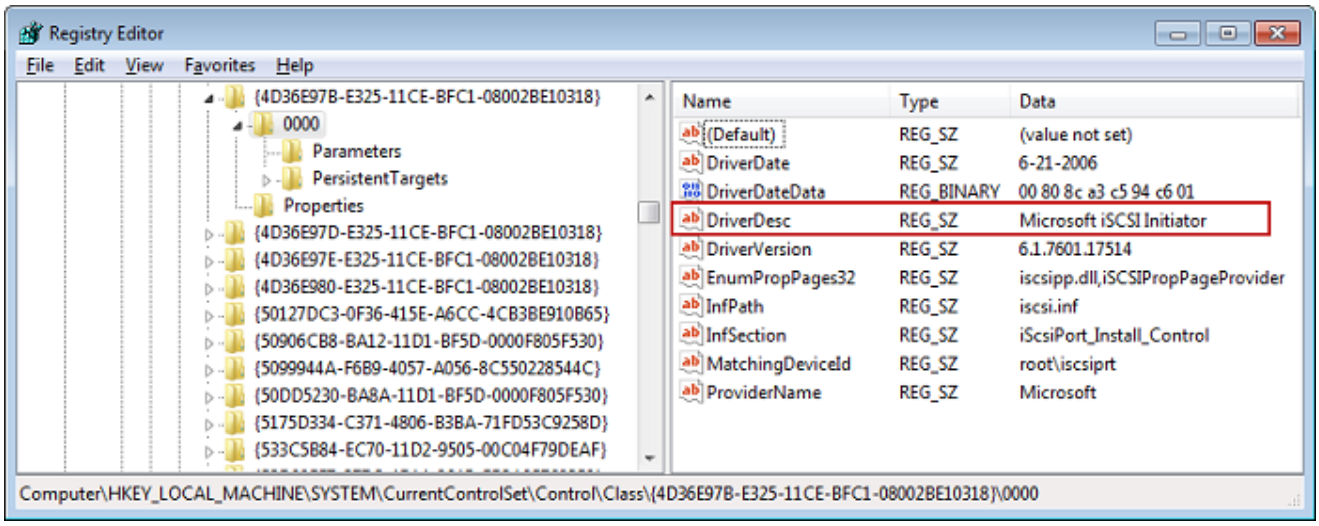
   c. Suchen Sie den Unterschlüssel für den Microsoft iSCSI Initiator, der im Format *`[<Instance-Nummer]`* angezeigt wird.

   Der Schlüssel wird durch eine vierstellige Zahl, z. B. `0000`dargestellt.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
   ```

   Je nachdem was auf Ihrem Computer installiert ist, wird der Microsoft iSCSI-Initiator möglicherweise nicht der Unterschlüssel sein `0000`. Sie können sicherstellen, dass Sie den richtigen Unterschlüssel ausgewählt haben in dem Sie die Zeichenfolge mit dem

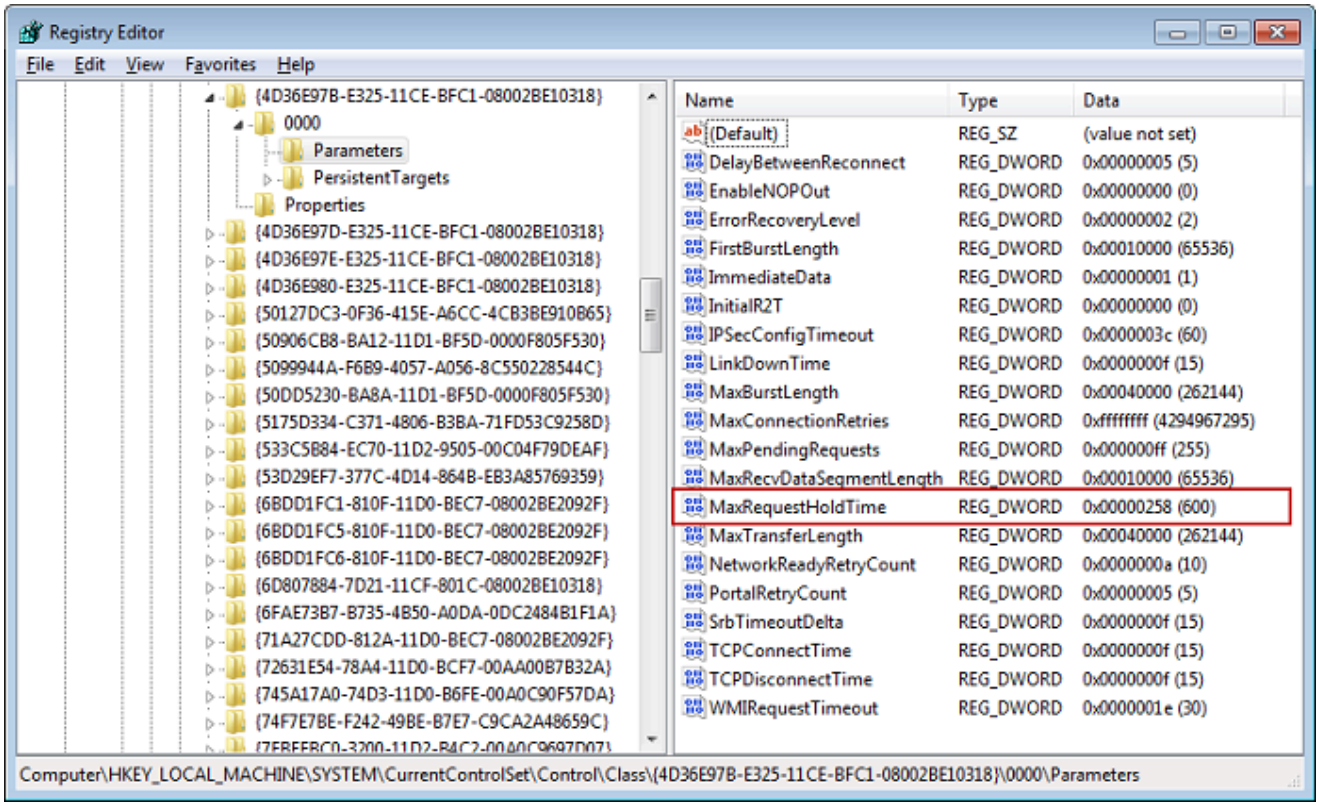
`DriverDesc` Wert `Microsoft iSCSI Initiator` prüfen, so wie im folgenden Beispiel beschrieben.



d. Um die iSCSI-Einstellungen anzuzeigen, wählen Sie den Unterschlüssel Parameters (Parameter) aus.

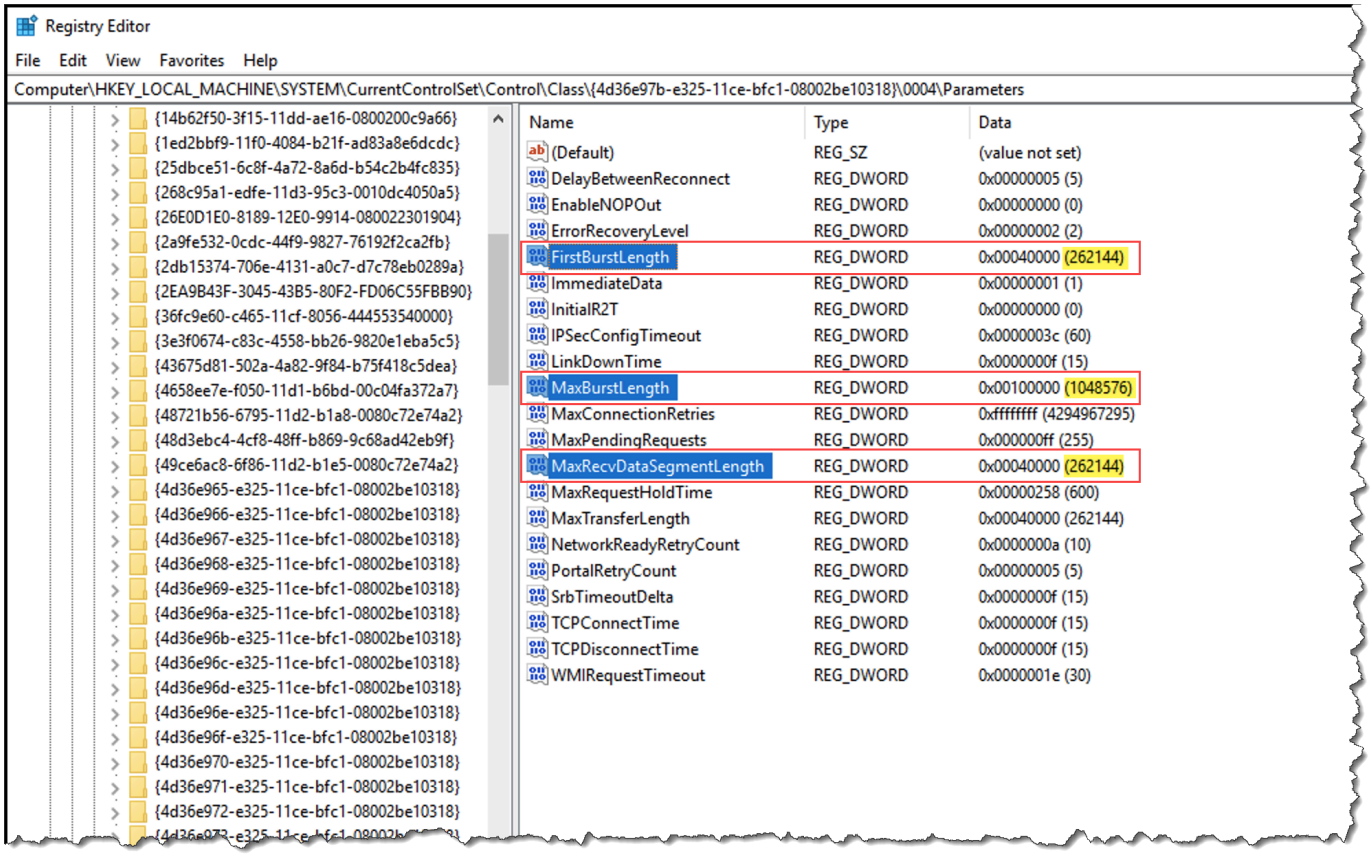
e. Öffnen Sie das Kontextmenü (rechte Maustaste) für den MaxRequestHoldTime DWORD-Wert (32-Bit), wählen Sie Ändern und ändern Sie dann den Wert in **`600`**.

   MaxRequestHoldTime gibt an, wie viele Sekunden der Microsoft iSCSI-Initiator halten und ausstehende Befehle wiederholen soll, bevor die obere Ebene eines `Device Removal` Ereignisses benachrichtigt wird. Dieser Wert stellt eine Wartezeit von 600 Sekunden dar, wie im folgenden Beispiel gezeigt.



2. Sie können die maximale Datenmenge erhöhen, die in iSCSI-Paketen gesendet werden kann, indem Sie die folgenden Parameter ändern:

   - FirstBurstLength steuert die maximale Datenmenge, die in einer unerwünschten Schreibanforderung übertragen werden kann. Legen Sie diesen Wert auf **262144** oder die Standardeinstellung des Windows-Betriebssystems fest, je nachdem, welcher Wert höher ist.
   - MaxBurstLength ist ähnlich wie FirstBurstLength, legt jedoch die maximale Datenmenge fest, die in aufgerufenen Schreibsequenzen übertragen werden kann. Legen Sie diesen Wert auf **1048576** oder die Standardeinstellung des Windows-Betriebssystems fest, je nachdem, welcher Wert höher ist.
   - MaxRecvDataSegmentLength steuert die maximale Datensegmentgröße, die einer einzelnen Protokolldateneinheit () zugeordnet ist. Legen Sie diesen Wert auf **262144** oder die Standardeinstellung des Windows-Betriebssystems fest, je nachdem, welcher Wert höher ist.



> **Note**
>
> Unterschiedliche Backup-Software kann optimiert werden, um mit verschiedenen iSCSI-Einstellungen möglichst gut zu funktionieren. Informationen zur Überprüfung, welche Werte für diese Parameter die beste Leistung bieten, finden Sie in der Dokumentation zu Ihrer Backup-Software.

3. Erhöhen Sie den Datenträger-Timeout-Wert, der wie folgt angezeigt wird:

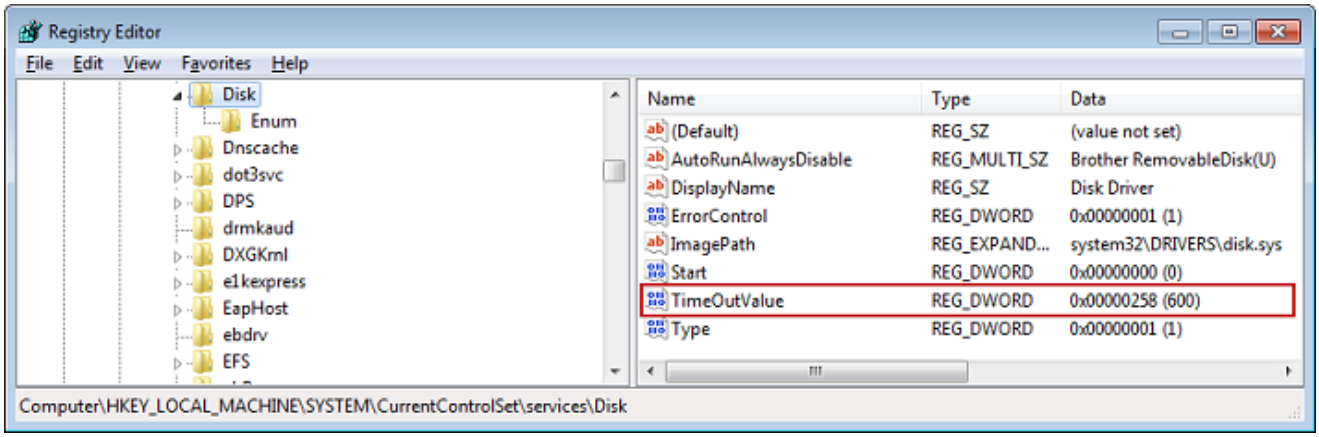
   a. Starten Sie den Registrierungs-Editor (`Regedit.exe`), falls Sie dies noch nicht getan haben.

   b. Navigieren Sie zum Unterschlüssel Datenträger im Unterschlüssel Services des CurrentControlSet, wie im Folgenden gezeigt.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. Öffnen Sie das Kontextmenü (rechte Maustaste) für den TimeOutValue DWORD-Wert (32-Bit), wählen Sie Ändern und ändern Sie dann den Wert in **`600`**.

TimeOutValue gibt an, wie viele Sekunden der iSCSI-Initiator auf eine Antwort vom Ziel wartet, bevor er die Sitzungswiederherstellung versucht, indem er die Verbindung löscht und wieder herstellt. Dieser Wert stellt einen Timeout-Zeitraum von 600 Sekunden dar, wie im folgenden Beispiel gezeigt.



4. Um sicherzustellen, dass die neuen Konfigurationswerte wirksam werden, starten Sie Ihr System erneut.

   Bevor Sie Ihr Gerät neu starten, müssen Sie sicherstellen, dass die Ergebnisse aller Schreibvorgänge zu den Volumes geleert wurden. Zu diesem Zweck, ordnen Sie eine Offline-Festplatten-Speicher-Volume zu, bevor Sie den Neustart durchführen.

Anpassen Ihrer Linux iSCSI-Einstellungen

Es wird dringend empfohlen, nach der Einrichtung des Initiators für Ihr Gateway die iSCSI-Einstellungen anzupassen, um zu vermeiden, dass der Initiator vom Ziel getrennt wird. Durch Erhöhen der iSCSI-Werte für Zeitbegrenzungen, wie in den folgenden Schritten beschrieben, wird Ihre Anwendung besser im Umgang mit Schreibvorgängen, die viel Zeit in Anspruch nehmen und besser in anderen transienten Aufgaben wie Netzwerk-Unterbrechungen.

> **Note**
>
> Befehle können sich von anderen Linux Typen unterscheiden. Die folgenden Beispiele basieren auf Red Hat Linux.

Um Ihre Linux iSCSI-Einstellungen anzupassen

1. Erhöhen Sie die maximale Dauer für die Anforderungen in der Warteschlange.

   a. Öffnen Sie die Datei `/etc/iscsi/iscsid.conf` und suchen Sie die folgenden Zeilen.

   ```
   node.session.timeo.replacement_timeout = [replacement_timeout_value]
   node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
   node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
   ```

   b. Legen Sie den Wert *[replacement_timeout_value]* auf **600** fest.

   Legen Sie den Wert *[noop_out_interval_value]* auf **60** fest.

   Legen Sie den Wert *[noop_out_timeout_value]* auf **600** fest.

   Alle drei Werte sind in Sekunden angegeben.

   > **Note**
   >
   > Die `iscsid.conf` Einstellungen müssen vor der Analyse der Gateway eingestellt werden. Wenn Sie Ihr Gateway bereits analysiert haben oder sie am Ziel angemeldet sind, oder beides, können Sie den Eintrag in der Discovery-Datenbank mithilfe des folgenden Befehls eingeben. Anschließend können erneut analysieren oder sich erneut anmelden um die neue Konfiguration zu erhalten.
   >
   > ```
   > iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
   > ```

2. Erhöhen Sie die Maximalwerte für die Datenmenge, die in jeder Antwort übertragen werden kann.

   a. Öffnen Sie die Datei `/etc/iscsi/iscsid.conf` und suchen Sie die folgenden Zeilen.

   ```
   node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
   node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
   node.conn[0].iscsi.MaxRecvDataSegmentLength
    = [replacement_segment_length_value]
   ```

   b. Wir empfehlen die folgenden Werte, um eine bessere Leistung zu erzielen. Ihre Backup-Software kann möglicherweise optimiert werden, um unterschiedliche Werte zu verwenden.

Konsultieren Sie daher die Dokumentation zur Backup-Software, um die besten Ergebnisse zu erzielen.

Legen Sie den Wert für *[replacement_first_burst_length_value]* auf **262144** oder den Standardwert des Linux-Betriebssystems fest, je nachdem, welcher Wert höher ist.

Legen Sie den Wert für *[replacement_max_burst_length_value]* auf **1048576** oder den Standardwert des Linux-Betriebssystems fest, je nachdem, welcher Wert höher ist.

Legen Sie den Wert für *[replacement_segment_length_value]* auf **262144** oder den Standardwert des Linux-Betriebssystems fest, je nachdem, welcher Wert höher ist.

> **Note**
>
> Unterschiedliche Backup-Software kann optimiert werden, um mit verschiedenen iSCSI-Einstellungen möglichst gut zu funktionieren. Informationen zur Überprüfung, welche Werte für diese Parameter die beste Leistung bieten, finden Sie in der Dokumentation zu Ihrer Backup-Software.

3. Um sicherzustellen, dass die neuen Konfigurationswerte wirksam werden, starten Sie Ihr System erneut.

   Bevor Sie Ihr Gerät neu starten, stellen Sie sicher, dass die Ergebnisse aller Schreibvorgänge auf Ihre Bänder geleert wurden. Heben Sie dazu das Mounting der Bänder auf, bevor Sie den Computer neu starten.

Anpassen der Linux-Festplatten-Timeout-Einstellungen für Volume Gateways

Wenn Sie ein Volume Gateway verwenden, können Sie zusätzlich zu den im vorigen Abschnitt beschriebenen iSCSI-Einstellungen die folgenden Linux-Festplatten-Timeout-Einstellungen anpassen.

So passen Sie Ihre Linux-Festplatten-Timeout-Einstellungen an

1. Erhöhen Sie die Datenträger-Zeitüberschreitungswert in den Regeldateien.

   a. Wenn Sie den RHEL 5 Initiator verwenden, öffnen Sie die `/etc/udev/rules.d/50-udev.rules` Datei und suchen Sie die folgende Zeile.

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Diese Regeldateien existieren nicht in RHEL 6- oder 7-Initiatoren, Sie müssen Sie deshalb mit der folgenden Regel erstellen.

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Um Zeitbeschränkungswert in RHEL 6 zu modifizieren, verwenden Sie den folgenden Befehl und fügen Sie dann die Zeile an Codes hinzu, wie oben angezeigt.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

Um Zeitbeschränkungswert in RHEL 7 zu modifizieren, verwenden Sie den folgenden Befehl und fügen Sie dann die Zeile an Codes hinzu, wie oben angezeigt.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

b. Legen Sie den Wert *[timeout]* auf **600** fest.

Dieser Wert stellt ein Timeout von 600 Sekunden dar.

2. Um sicherzustellen, dass die neuen Konfigurationswerte wirksam werden, starten Sie Ihr System erneut.

Bevor Sie Ihr Gerät neu starten, stellen Sie sicher, dass die Ergebnisse aller Schreibvorgänge auf Ihren Volumes geleert wurden. Zu diesem Zweck unmounten Sie die Speicher-Volumes, bevor Sie den Neustart durchführen.

3. Sie können die Konfiguration testen, indem Sie den folgenden Befehl eingeben.

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

Dieser Befehl zeigt die udev-Regeln, die auf den iSCSI-Gerät angewendet werden.

Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele

Storage Gateway unterstützt die Authentifizierung zwischen Ihrem Gateway und iSCSI-Initiatoren mithilfe des Challenge-Handshake Authentication Protocol (CHAP). CHAP bietet Schutz vor Playback-Angriffen, indem die Identität eines iSCSI-Initiators, der für den Zugriff auf ein Volume und ein VTL-Gerätеziel authentifiziert wurde, regelmäßig überprüft wird.

> **Note**
>
> Die CHAP-Konfiguration ist optional, wird jedoch dringend empfohlen.

Zur Einrichtung von CHAP müssen Sie das Protokoll sowohl in der Storage-Gateway-Konsole als auch in der iSCSI-Initiator-Software konfigurieren, über die Sie die Verbindung mit dem Ziel herstellen. Storage Gateway arbeitet mit wechselseitiger CHAP-Authentifizierung: Der Initiator authentifiziert das Ziel und das Ziel authentifiziert den Initiator.

Eine wechselseitige CHAP-Authentifizierung richten Sie wie folgt für Ihre Ziele ein:

1. Konfigurieren Sie CHAP in der Storage-Gateway-Konsole wie unter So konfigurieren Sie CHAP für ein VTL-Gerät in der Storage-Gateway-Konsole beschrieben.
2. Konfigurieren Sie CHAP in der Initiator-Software auf Ihrem Client:
   - Wie Sie die wechselseitige CHAP-Authentifizierung auf einem Windows-Client konfigurieren, erfahren Sie unter Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.
   - Wie Sie die wechselseitige CHAP-Authentifizierung auf einem Red Hat Linux-Client konfigurieren, erfahren Sie unter Auf einem Red Hat Linux-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.

So konfigurieren Sie CHAP für ein VTL-Gerät in der Storage-Gateway-Konsole

In dieser Anleitung geben Sie zwei geheime Schlüssel an, die verwendet werden, um von dem virtuellen Bandlaufwerk zu lesen und auf das virtuelle Bandlaufwerk zu schreiben. Dieselben Schlüssel werden auch in der Anleitung zur Konfiguration des Client-Initiators verwendet.

1. Wählen Sie im Navigationsbereich Gateways aus.

2. Wählen Sie Ihr Gateway aus und wechseln Sie dann auf die Registerkarte VTL Devices (VTL-Geräte). Hier werden alle Ihre VTL-Geräte aufgeführt.
3. Wählen Sie das Gerät aus, für das Sie CHAP konfigurieren möchten.
4. Geben Sie die erforderlichen Informationen im Dialogfeld CHAP-Authentifizierung konfigurieren ein.

   a. Geben Sie im Feld Initiatorname den Namen Ihres iSCSI-Initiators ein. Dieser Name ist ein qualifizierter Amazon-iSCSI-Name (IQN), dem `iqn.1997-05.com.amazon:` vorangestellt wird und der Name des Ziels folgt. Im Folgenden wird ein Beispiel gezeigt.

      `iqn.1997-05.com.amazon:`*`your-tape-device-name`*

      Den Namen des Initiators finden Sie in Ihrer iSCSI-Initiator-Software. Auf Windows-Clients beispielsweise ist der Name der Wert auf der Registerkarte Konfiguration des iSCSI-Initiators. Weitere Informationen finden Sie unter Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.

      > **Note**
      >
      > Wenn Sie den Namen des Initiators ändern möchten, müssen Sie zunächst CHAP deaktivieren. Anschließend ändern Sie den Namen des Initiators in Ihrer iSCSI-Initiator-Software und aktivieren dann CHAP mit dem neuen Namen.

   b. Geben Sie unter Für Authentifizierung des Initiators verwendeter geheimer Schlüssel den entsprechenden geheimen Schlüssel ein.

      Dieser geheime Schlüssel muss mindestens 12 Zeichen lang sein und darf höchstens 16 Zeichen lang sein. Dieser Wert ist der geheime Schlüssel, den der Initiator (Windows-Client) kennen muss, um an der CHAP-Authentifizierung mit dem Ziel teilnehmen zu können.

   c. Geben Sie unter Für Authentifizierung des Ziels verwendeter geheimer Schlüssel (wechselseitige CHAP-Authentifizierung) den entsprechenden geheimen Schlüssel ein.

      Dieser geheime Schlüssel muss mindestens 12 Zeichen lang sein und darf höchstens 16 Zeichen lang sein. Dieser Wert ist der geheime Schlüssel, den das Ziel kennen muss, um an der CHAP-Authentifizierung mit dem Initiator teilnehmen zu können.

> **Note**
>
> Für die Authentifizierung des Ziels müssen Sie einen anderen geheimen Schlüssel verwenden als für die Authentifizierung des Initiators.

d. Wählen Sie Speichern.

5. Vergewissern Sie sich, dass auf der Registerkarte VTL Devices (VTL-Geräte) für das Feld "iSCSI CHAP authentication (iSCSI CHAP-Authentifizierung)" der Wert auf true (wahr) gesetzt ist.

Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:

In dieser Anleitung konfigurieren Sie CHAP im Microsoft iSCSI-Initiator. Hierzu verwenden Sie dieselben Schlüssel wie bei der konsolenbasierten Konfiguration von CHAP für das Volume.

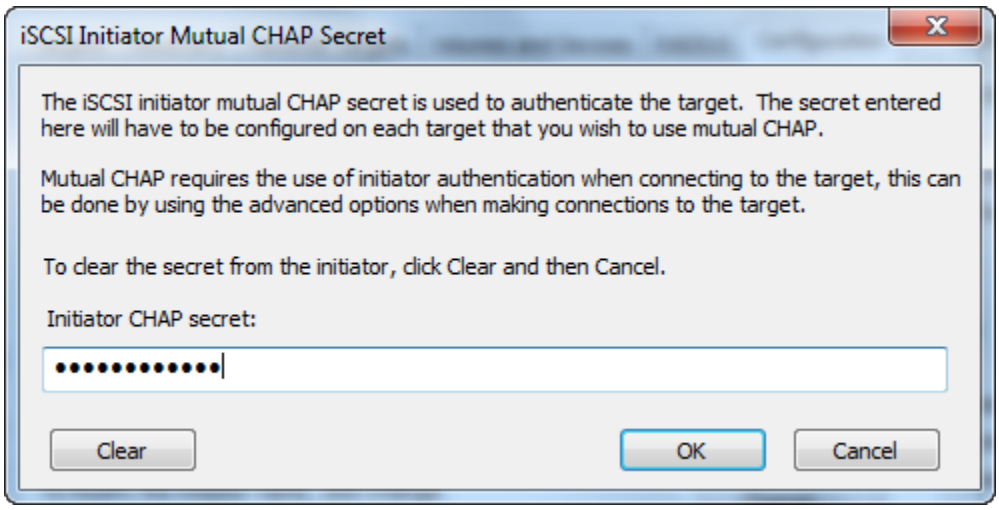
1. Falls der iSCSI-Initiator noch nicht ausgeführt wird, klicken Sie im Menü Start Ihres Windows-basierten Client-Computers auf Ausführen, geben Sie **`iscsicpl.exe`** ein und klicken Sie dann auf OK, um das Programm auszuführen.
2. Konfigurieren Sie die wechselseitige CHAP-Authentifizierung für den Initiator (Windows-Client):

   a. Wählen Sie die Registerkarte Konfiguration aus.

   > **Note**
   >
   > Der Wert im Feld Initiatorname ist für Ihren Initiator und Ihre Firma eindeutig. Bei dem oben angezeigten Name handelt es sich um den Wert, den Sie im Dialogfeld CHAP-Authentifizierung konfigurieren in der Storage-Gateway-Konsole verwendet haben.
   > Der Name auf dem Screenshot dient ausschließlich Demonstrationszwecken.

   b. Klicken Sie auf CHAP.

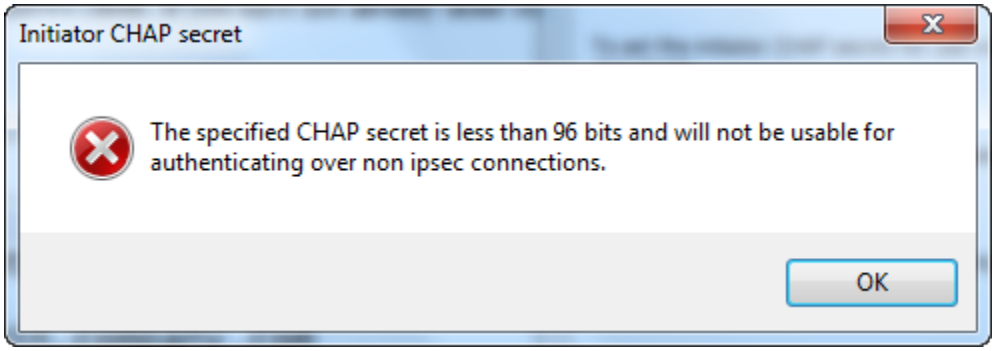
   c. Geben Sie im Dialogfeld iSCSI-Initiator: Geheimer Schlüssel für wechselseitige CHAP-Authentifizierung den geheimen Schlüssel für die wechselseitige CHAP-Authentifizierung ein.



In diesem Dialogfeld geben Sie den geheimen Schlüssel ein, den der Initiator (Windows-Client) zur Authentifizierung des Ziels (Speicher-Volume) verwendet. Dieser geheime Schlüssel gewährt dem Ziel Lese- und Schreibrechte für den Initiator. Es handelt sich hierbei um denselben geheimen Schlüssel, den Sie im Feld Für Authentifizierung des Ziels verwendeter geheimer Schlüssel (wechselseitige CHAP-Authentifizierung) im Dialogfeld CHAP-Authentifizierung konfigurieren eingegeben haben. Weitere Informationen finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.

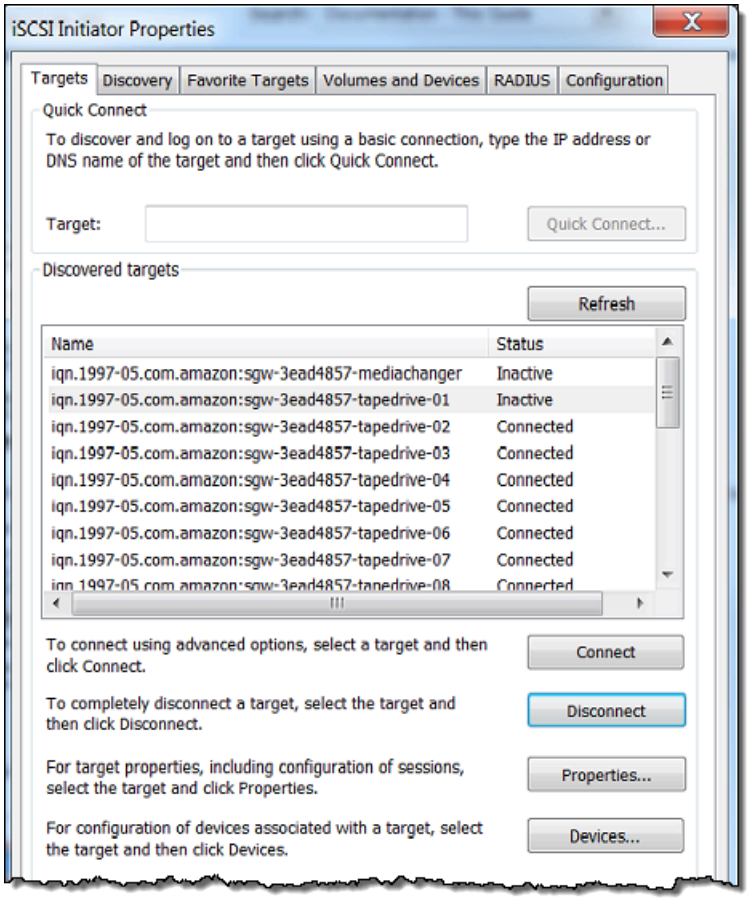
d. Falls Sie einen Schlüssel eingeben, der weniger als 12 Zeichen oder mehr als 16 Zeichen umfasst, wird das Fehlerdialogfeld Geheimer CHAP-Schlüssel des Initiators angezeigt.

   Klicken Sie auf OK und geben Sie den Schlüssel erneut ein.



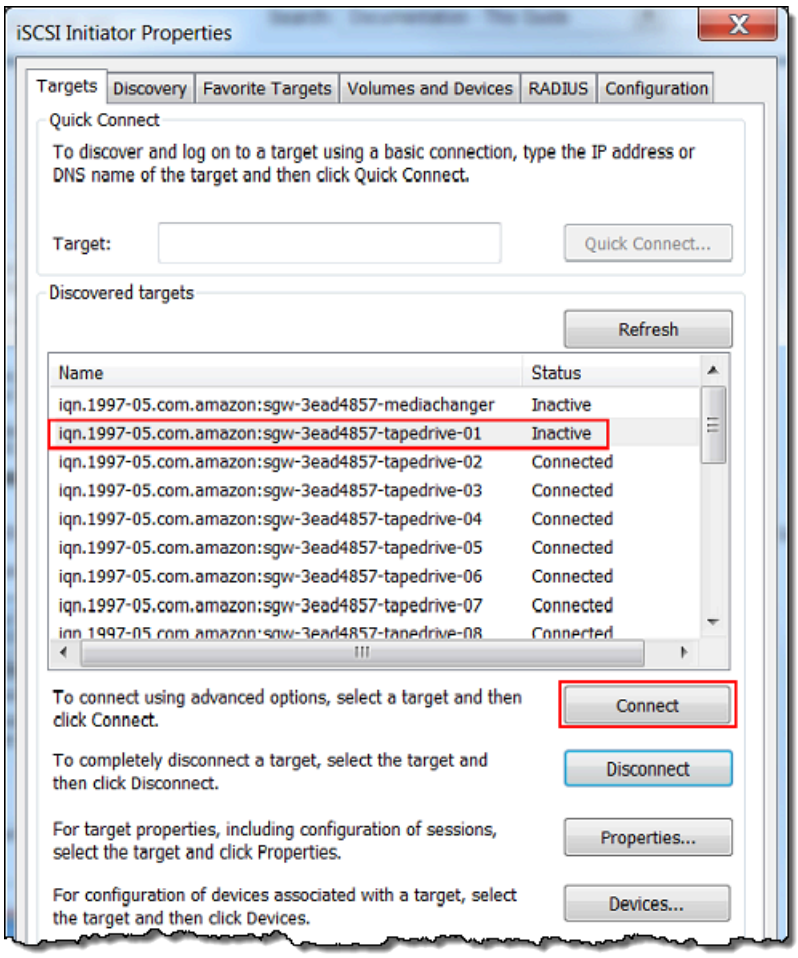
3. Konfigurieren Sie das Ziel mit dem geheimen Schlüssel des Initiators, um die Konfiguration der wechselseitigen CHAP-Authentifizierung abzuschließen:

   a. Wählen Sie die Registerkarte Ziele.

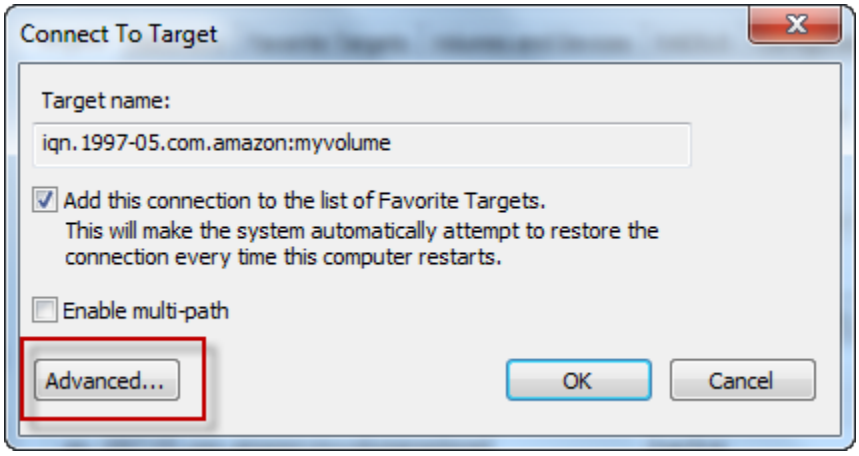


b. Falls das Ziel, das Sie für CHAP konfigurieren möchten, aktuell verbunden ist: Wählen Sie das Ziel aus und klicken Sie auf Disconnect (Trennen), um die Verbindung mit dem Ziel zu trennen.

c. Wählen Sie das Ziel aus, das Sie für CHAP konfigurieren möchten, und klicken Sie auf Connect (Verbinden).



d. Klicken Sie im Dialogfeld Connect to Target (Mit Ziel verbinden) auf Advanced (Erweitert).



e. Konfigurieren Sie CHAP im Dialogfeld Advanced Settings (Erweiterte Einstellungen).

   i. Wählen Sie CHAP-Anmeldung aktivieren aus.

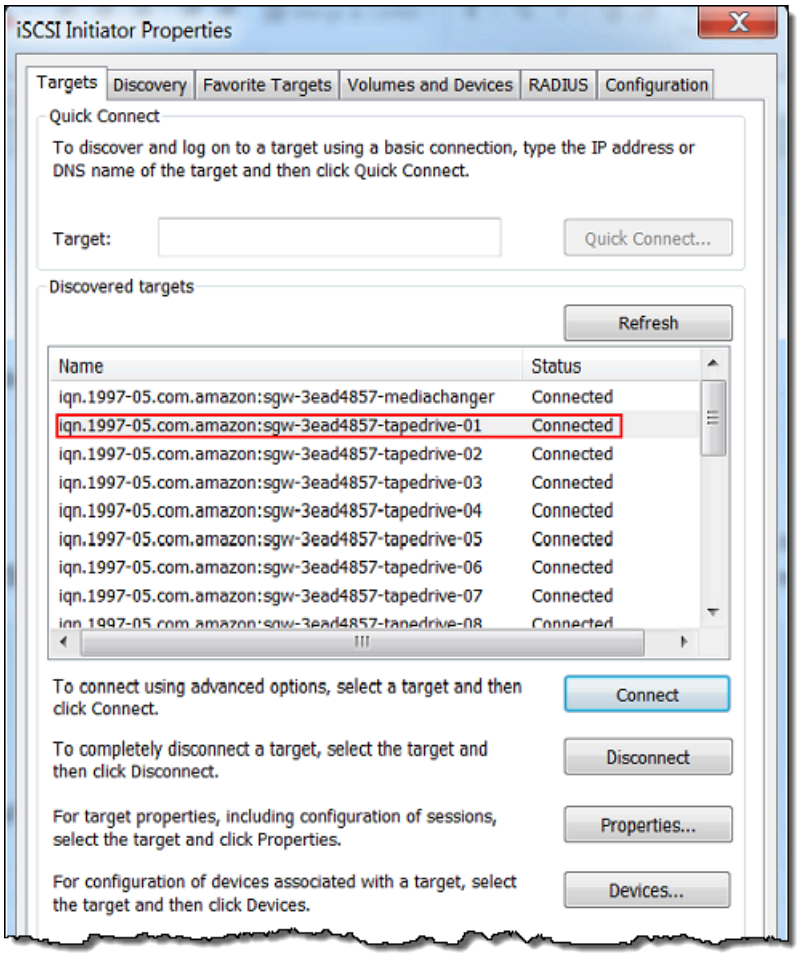
ii. Geben Sie den zum Authentifizieren des Initiators erforderlichen geheimen Schlüssel ein. Es handelt sich hierbei um denselben geheimen Schlüssel, den Sie im Feld Für Authentifizierung des Initiators verwendeter geheimer Schlüssel im Dialogfeld CHAP-Authentifizierung konfigurieren eingegeben haben. Weitere Informationen finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.

iii. Wählen Sie Perform mutual authentication (Wechselseitige Authentifizierung ausführen) aus.

iv. Klicken Sie auf OK, um die Änderungen anzuwenden.

f. Klicken Sie im Dialogfeld Mit Ziel verbinden auf OK.

4. Wenn Sie den richtigen geheimen Schlüssel angegeben haben, wird für das Ziel der Status Connected (Verbunden) angezeigt.



Auf einem Red Hat Linux-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:

In dieser Anleitung konfigurieren Sie CHAP im Linux-iSCSI-Initiator. Hierzu verwenden Sie dieselben Schlüssel, die Sie auch verwendet haben, als Sie in der Storage-Gateway-Konsole CHAP für das Volume konfiguriert haben.

1. Vergewissern Sie sich, dass der ISCSI-Daemon ausgeführt wird und dass bereits eine Verbindung zu einem Ziel besteht. Falls Sie diese beiden Aufgaben nicht abgeschlossen haben, finden Sie weitere Informationen unter Herstellen einer Verbindung mit einem Linux-Client.
2. Trennen Sie die Verbindung zu dem Ziel, für das Sie CHAP konfigurieren möchten, und entfernen Sie alle bereits vorhandenen Konfigurationen.

   a. Listen Sie mithilfe des folgenden Befehls die gespeicherten Konfigurationen auf, um den Zielnamen zu ermitteln und sich zu vergewissern, dass es sich um eine definierte Konfiguration handelt:

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. Trennen Sie die Verbindung mit dem Ziel.

   Der folgende Befehl trennt die Verbindung mit dem Ziel **`myvolume`**, das im qualifizierten Amazon-iSCSI-Namen (IQN) definiert ist. Passen Sie den Zielnamen und den IQN entsprechend Ihrer konkreten Umgebung an.

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. Entfernen Sie die Konfiguration des Ziels.

   Der folgende Befehl entfernt die Konfiguration für das Ziel **`myvolume`**.

   ```
   sudo /sbin/iscsiadm --mode node --op delete --targetname
    iqn.1997-05.com.amazon:myvolume
   ```

3. Bearbeiten Sie die iSCSI-Konfigurationsdatei, um CHAP zu aktivieren.

   a. Rufen Sie den Namen des Initiators ab (also den des Clients, den Sie verwenden).

   Der folgende Befehl ruft den Namen des Initiators aus der Datei `/etc/iscsi/initiatorname.iscsi` ab:

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

Die Ausgabe dieses Befehls sieht in etwa wie folgt aus:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. Öffnen Sie die `/etc/iscsi/iscsid.conf` Datei.

c. Heben Sie die Auskommentierung der folgenden Zeilen in der Datei auf und geben Sie die korrekten Werte für *username*, *password*, *username_in* und *password_in* an.

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

Einen Überblick über die anzugebenden Werte finden Sie in der nachfolgenden Tabelle.

Konfigurationseinstellung	Wert
username (Benutzername	Gibt den Initiatornamen an, den Sie im vorherigen Schritt der Anleitung abgerufen haben. Der Wert beginnt mit iqn. **iqn.1994-05.com.redhat:8e89b27b5b8** ist beispielsweise ein gültiger Wert für *username*.
password	Gibt den geheimen Schlüssel an, der zur Authentifizierung des Initiators (also des verwendeten Clients) verwendet wird, wenn dieser mit dem Volume kommuniziert.
username_in	Gibt den IQN des Ziel-Volumes an. Der Wert beginnt mit iqn und endet mit dem Namen des Ziels. **iqn.1997-05.com.amazon:myvolume** ist beispielsweise ein gültiger Wert für *username_in* .

Konfigurationseinstellung	Wert
password_in	Gibt den geheimen Schlüssel an, der zur Authentifizierung des Ziels (also des Volumes) verwendet wird, wenn dieses mit dem Initiator kommuniziert.

d. Speichern Sie die Änderungen in der Konfigurationsdatei und schließen Sie die Datei.

4. Führen Sie eine Erkennung des Ziels durch und melden Sie sich beim Ziel an. Folgen Sie dazu den Schritten unter Herstellen einer Verbindung mit einem Linux-Client.

Verwenden von AWS Direct Connect mit Storage Gateway

AWS Direct Connect verknüpft Ihr internes Netzwerk mit der Amazon Web Services Cloud. Durch die Verwendung von AWS Direct Connect mit Storage Gateway können Sie eine Verbindung für Workload-Anforderungen mit hohem Durchsatz herstellen und eine dedizierte Netzwerkverbindung zwischen Ihrem On-Premises-Gateway und bereitstellen AWS.

Storage Gateway verwendet öffentliche Endpunkte. Wenn eine - AWS Direct Connect Verbindung vorhanden ist, können Sie eine öffentliche virtuelle Schnittstelle erstellen, damit Datenverkehr an die Storage Gateway-Endpunkte weitergeleitet werden kann. Die öffentliche virtuelle Schnittstelle umgeht Internetdienstanbieter in Ihrem Netzwerkpfad. Der öffentliche Endpunkt des Storage Gateway-Service kann sich in derselben AWS Region wie der AWS Direct Connect Standort befinden oder er kann sich in einer anderen AWS Region befinden.

Die folgende Abbildung zeigt ein Beispiel dafür, wie mit Storage Gateway AWS Direct Connect funktioniert.
-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.

So verwenden Sie AWS Direct Connect mit Storage Gateway

1. Erstellen und richten Sie eine AWS Direct Connect Verbindung zwischen Ihrem On-Premises-Rechenzentrum und Ihrem Storage Gateway-Endpunkt ein. Weitere Informationen zum Erstellen

einer Verbindung finden Sie unter Erste Schritte mit AWS Direct Connect im Benutzerhandbuch zu AWS Direct Connect .

2. Verbinden Sie Ihre lokale Storage Gateway-Appliance mit dem AWS Direct Connect Router.
3. Erstellen Sie eine öffentliche virtuelle Schnittstelle und konfigurieren Sie Ihren lokalen Router entsprechend. Auch bei Direct Connect müssen VPC-Endpunkte mit dem HAProxy erstellt werden. Weitere Informationen finden Sie unter Erstellen einer virtuellen Schnittstelle im Benutzerhandbuch zu AWS Direct Connect .

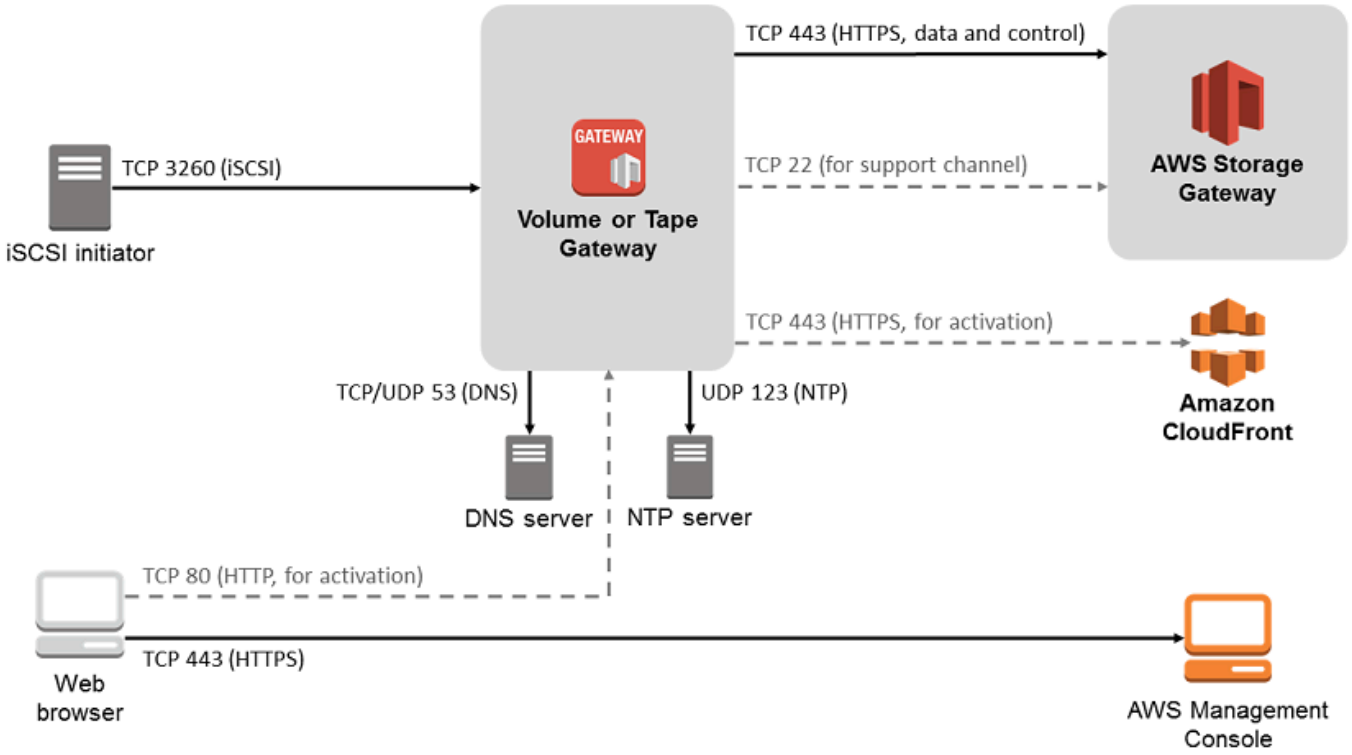
Weitere Informationen zu AWS Direct Connect finden Sie unter Was ist AWS Direct Connect? im AWS Direct Connect -Benutzerhandbuch.

Port-Anforderungen

Damit Storage Gateway korrekt arbeiten kann, sind die nachfolgend aufgeführten Ports erforderlich. Einige Ports werden von allen Gateway-Typen verwendet und sind für alle Gateway-Typen erforderlich. Andere Ports werden für bestimmte Gateway-Typen benötigt. In diesem Abschnitt finden Sie eine Abbildung und eine Liste der erforderlichen Ports für Tape Gateway.

Tape Gateway

Die folgende Abbildung zeigt die Ports, die für den Betrieb von Gateways vom Typ Tape Gateway offen sein müssen.



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

Aus	Bis	Protokoll	Port	Verwendung	
Storage-Gateway-VM	AWS	Transmission Control Protocol (TCP)	443 (HTTPS)	Für die Kommunikation von einer ausgehenden Storage Gateway-VM zu einem - AWS Service-Endpunkt. Informationen über Service-Endpunkte finden	

Aus	Bis	Protokoll	Port	Verwendung	
				Sie unter Zulassen des AWS Storage Gateway Zugriffs über Firewalls und Router.	

Aus	Bis	Protokoll	Port	Verwendung	
Ihr Webbrowser	Storage-Gateway-VM	TCP	80 (HTTP)	Von lokalen Systemen zum Abrufen des Storage-Gateway-Aktivierungsschlüssels. 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 Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie das Gateway von der	

Aus	Bis	Protokoll	Port	Verwendung	
				Storage-Gateway-Managementkonsole aus aktivieren, muss der Host, von dem aus Sie die Verbindung zur Konsole herstellen, Zugriff auf Port 80 des Gateways haben.	
Storage-Gateway-VM	Domain Name Service (DNS)-Server	User Datagram Protocol (UDP)/UDP	53 (DNS)	Für die Kommunikation zwischen einer Storage-Gateway-VM und dem DNS-Server.	

Aus	Bis	Protokoll	Port	Verwendung	
Storage-Gateway-VM	AWS	TCP	22 (Support-Kanal)	Ermöglicht AWS 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 jedoch erforderlich.	

Aus	Bis	Protokoll	Port	Verwendung	
Storage-Gateway-VM	Network Time Protocol (NTP)-Server	UDP	123 (NTP)	Verwendet von lokalen Systemen zur Synchronisierung der VM-Zeit mit der Host-Zeit. Eine Storage-Gateway-VM ist so konfiguriert, dass die folgenden NTP-Server verwendet werden: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org	
Storage Gateway-Hardware-Appliance	Hypertext Transfer Protocol (HTTP)-Proxy	TCP	8080 (HTTP)	Für die Aktivierung kurz erforderlich.	

Neben den allgemeinen Ports benötigt Tape Gateway auch den folgenden Port.

Aus	Bis	Protokoll	Port	Verwendung	
iSCSI-Initiatoren	Storage-Gateway-VM	TCP	3260 (iSCSI)	Durch lokale Systeme zum Herstellen einer Verbindung zu von einem Gateway verfügbar gemachten iSCSI-Zielen.	

Herstellen einer Verbindung mit einem Gateway

Nachdem Sie einen Host ausgewählt und eine Gateway-VM bereitgestellt haben, verbinden und aktivieren Sie das Gateway. Hierzu benötigen Sie die IP-Adresse der Gateway-VM. Rufen Sie die IP-Adresse von der lokalen Konsole des Gateways ab. Sie melden sich bei der lokalen Konsole an und rufen die IP-Adresse im oberen Bereich der Konsole ab.

Für lokal bereitgestellte Gateways können Sie auch die IP-Adresse vom Hypervisor abrufen. Im Fall von Amazon EC2-Gateways können Sie die IP-Adresse Ihrer Amazon EC2-Instance auch aus der Amazon EC2 Management Console abrufen. Informationen zum Abrufen der IP-Adresse des Gateways finden unter:

- VMware-Host: Zugreifen auf die lokale Konsole mit VMware ESXi
- Hyper-V-Host: Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V
- Linux Kernel-basierte virtuelle Maschine (KVM)-Host: Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
- EC2-Host: Abrufen einer IP-Adresse von einem Amazon EC2-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. Anweisungen finden Sie unter Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.

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.
4. Nachdem Ihr Gateway aktiviert wurde, wählen Sie das Gateway aus, das Sie gerade aktiviert haben, und dann die Registerkarte VTL devices (VTL-Geräte) im unteren Bereich aus.
5. Rufen Sie die Namen aller VTL-Geräte ab.
6. Führen Sie für jedes Ziel den folgenden Befehl aus, um das Ziel zu konfigurieren.

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. Führen Sie für jedes Ziel den folgenden Befehl aus, um sich anzumelden.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   Ihr Gateway ist jetzt mit der Elastic IP-Adresse der EC2 Instance verbunden.

Grundlegendes zu Ressourcen und Ressourcen-IDs von Storage Gateway

In Storage Gateway ist die primäre Ressource ein Gateway. Zu den anderen Ressourcentypen gehören Volume, virtuelles Band, iSCSI-Ziel und VTL-Gerät. Diese werden als Subressourcen bezeichnet und existieren nur, wenn sie mit einem Gateway verknüpft sind.

Diesen Ressourcen und Unterressourcen sind eindeutige Amazon-Ressourcennamen (ARN) zugeordnet, wie in der folgenden Tabelle zu sehen ist.

Ressourcentyp	ARN-Format
Gateway-ARN	`arn:aws:storagegateway:` *region*`:`*account-id*` :gateway/` *gateway-id*
Band-ARN	`arn:aws:storagegateway:` *region*`:`*account-id*` :tape/`*tapebarcode*
Ziel-ARN (iSCSI-Ziel)	`arn:aws:storagegateway:` *region*`:`*account-id*` :gateway/` *gateway-id* `/target/`*iSCSItarget*
VTL-Geräte-ARN	`arn:aws:storagegateway:` *region*`:`*account-id*` :gateway/` *gateway-id* `/device/`*vtldevice*

Storage Gateway unterstützt auch die Verwendung von EC2-Instances sowie EBS-Volumes und -Snapshots. Diese Ressourcen sind Amazon-EC2-Ressourcen, die in Storage Gateway verwendet werden.

Arbeiten mit Ressourcen-IDs

Wenn Sie eine Ressource erstellen, weist Storage Gateway der Ressource eine eindeutige Ressourcen-ID zu. Diese Ressourcen-ID ist Teil des Ressourcen-ARN. Eine Ressourcen-ID besteht aus einer Ressourcenkennung, gefolgt von einem Bindestrich und einer eindeutigen Kombination aus acht Buchstaben und Zahlen. Eine Gateway-ID beispielsweise hat die Form `sgw-12A3456B`, wobei `sgw` die Ressourcenkennung für Gateways ist. Ein Volume-ID hat die Form `vol-3344CCDD`, wobei `vol` die Ressourcenkennung für Volumes ist.

Bei virtuellen Bändern können Sie der Barcode-ID ein Präfix von bis zu vier Zeichen voranstellen, um Ihre Bänder zu organisieren.

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.

Kennzeichnen der Storage 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, das sie einfacher zu verwalten sind. Jedes Tag besteht aus einem Schlüssel-Wert-Paar, das Sie definieren. Sie können Tags zu Gateways, Volumes und virtuellen Bändern hinzufügen. Sie können diese Ressourcen auf der Grundlage der hinzugefügten Tags filtern und danach suchen.

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.

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 AWS Verwendung reserviert.
- Gültige Zeichen der Schlüsseleigenschaft sind UTF-8-Buchstaben und Zahlen, Leerzeichen und die Sonderzeichen + - = . _ : / und @.

Arbeiten mit Tags

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-Konsole unter https://console.aws.amazon.com/storagegateway/home.
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-Konsole unter https://console.aws.amazon.com/storagegateway/home.
2. Wählen Sie die Ressource aus, deren Tag Sie bearbeiten möchten.
3. Wählen Sie Tags, um das Dialogfeld Add/edit tags (Tags hinzufügen/bearbeiten) zu öffnen.
4. Wählen Sie das Bleistiftsymbol neben dem Tag aus, das Sie bearbeiten möchten, und bearbeiten Sie dann das Tag.
5. Wenn Sie das Tag bearbeitet haben, wählen Sie Save (Speichern).

So löschen Sie ein Tag

1. Öffnen Sie die Storage-Gateway-Konsole unter https://console.aws.amazon.com/storagegateway/home.
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 Tools und Lizenzen von Drittanbietern beschrieben, auf die wir für die Bereitstellung der Storage Gateway-Funktionalität angewiesen sind.

Der Quellcode einiger der in der AWS Storage Gateway -Software enthaltenen Open-Source-Softwarekomponenten steht unter folgenden Links zum Download zur Verfügung:

- Laden Sie für Gateways, die auf VMware ESXi bereitgestellt werden, sources.tar herunter.
- Laden Sie für Gateways, die auf Microsoft Hyper-V bereitgestellt werden, sources_hyperv.tar herunter.

- Laden Sie für Gateways, die auf einer Kernel-basierten virtuellen Maschine unter Linux (KVM) bereitgestellt werden, sources_KVM.tar herunter.

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.

AWS Storage Gateway -Kontingente

In diesem Thema finden Sie Informationen zu den für Storage Gateway geltenden Kontingenten für Dateifreigaben, Volumes und Bänder sowie zu den Konfigurations- und Leistungslimits des Service.

Themen

Kontingente für Bänder

In der folgenden Tabelle sind die Kontingente für Bänder aufgeführt.

Beschreibung	Tape Gateway
Mindestgröße eines virtuellen Bands	100 GiB
Maximale Größe eines virtuellen Bands	15 TiB
Maximale Anzahl virtueller Bänder, die einem Gateway zugewiesen sind	1.500
Gesamtgröße aller pro Gateway zugewiesener Bänder	1 PiB
Maximale Anzahl von virtuellen Bändern pro Archiv	Kein Limit
Gesamtgröße aller Bänder im Archiv	Kein Limit

Empfohlene Kapazität für die lokalen Datenträger des Gateways

In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt.

Gateway-Typ	Cache (Minimum)	Cache (Maximum)	Upload-Puffer (Minimum)	Upload-Puffer (Maximum)	Andere erforderliche lokale Festplatten
Tape Gateway	150 GiB	64 TiB	150 GiB	2 TiB	—

> **Note**
>
> Sie können ein oder mehrere lokale Laufwerke für Ihren Cache und Upload-Puffer konfigurieren, bis die maximale Kapazität erreicht ist.
> Wenn Sie einen Cache oder Upload-Puffer zu einem vorhandenen Gateway hinzufügen, müssen neue Festplatten auf Ihrem Host (Hypervisor oder Amazon-EC2-Instance) erstellt werden. Ändern Sie nicht die Größe von vorhandenen Datenträgern, wenn die Datenträger vorher bereits als Cache oder Upload-Puffer zugeordnet wurden.

API-Referenz für Storage Gateway

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 Operationen, die Anforderungssignatur für die 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 die AWS SDKs auch bei der Entwicklung von Anwendungen mit verwenden AWS Storage Gateway. Die AWS SDKs für Java, .NET und PHP umschließen die zugrunde liegende AWS Storage Gateway API, wodurch Ihre Programmieraufgaben vereinfacht werden. Weitere Informationen zum Herunterladen der SDK-Bibliotheken finden Sie unter Beispiel-Code-Bibliotheken.

Themen

Für die Storage Gateway-Abfrage erforderliche Header

In diesem Abschnitt werden die erforderlichen Header beschrieben, die Sie mit jeder POST-Abfrage an Storage Gateway senden müssen. 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
```

Die folgenden Kopfzeilen müssen mit in den POST-Abfragen an Storage Gateway enthalten sein. Die unten gezeigten Header, die mit „x-amz“ beginnen, sind AWS-spezifische Header. Alle anderen aufgeführten Header sind allgemeine Header für HTTP-Transaktionen.

Header	Beschreibung
`Authorization`	Der Autorisierungs-Header enthält mehrere Informationen über die Abfrage, mit denen Storage Gateway bestimmt, ob die Abfrage eine gültige Aktion für den Auftraggeber ist. Das Format dieses Headers lautet wie folgt (Zeilenumbrüche dienen besserer Lesbarkeit): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` In der vorherigen Syntax geben Sie , YourAccessKeydas Jahr, den Monat und den Tag (jjjjmmdd), die Region und die anCalculatedSignature. Das Format des Autorisierungs-Headers hängt von den Anforderungen des AWS V4-Signaturprozesses ab. Detaillierte Informationen zum Signieren finden Sie unter dem Thema Signieren von Anforderungen.
`Content-Type`	Verwenden Sie `application/x-amz-json-1.1` als Inhaltstyp für alle Abfragen an Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Header	Beschreibung
`Host`	Verwenden Sie den Host-Header, um den Storage Gateway-Endpunkt anzugeben, an den Sie die Abfrage senden. `storagegateway.us-east-2.amazonaws.com` steht beispielsweise für den Endpunkt der Region USA Ost (Ohio). Weitere Informationen zu den für Storage Gateway verfügbaren Endpunkte finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der Allgemeine AWS-Referenz. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Sie müssen den Zeitstempel entweder im HTTP-`Date`Header oder im AWS `x-amz-date` -Header angeben. (Einige HTTP-Client-Biblio theken lassen den Header `Date` nicht zu.) Ist der Header `x-amz-date` vorhanden, ignoriert das Storage Gateway System bei der Abfrageauthentifizierung alle Header des Typs `Date`. Das Format `x-amz-date` muss ISO8601 Basic dem Format JJJJMMTT'T'HHMMSS' Z' entsprechen. Wenn sowohl der `Date`- als auch der `x-amz-date` -Header verwendet werden, muss das Format des Datum-Headers nicht ISO8601 entsprechen. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	In diesem Header werden die Version der API und die angefragte Operation angegeben. Die Werte des Ziel-Headers werden durch Verknüpfung der API-Version mit dem API-Namen gebildet und haben folgendes Format. `x-amz-target: StorageGateway_ APIversion .operationName` Der Wert operationName (z. B. „ActivateGateway“) finden Sie in der API-Liste API-Referenz für Storage Gateway.

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 unter Nutzung des geheimen Zugriffsschlüssels und der Zeichenfolge mit dem Umfang der Anmeldeinformationen berechnet, um

eine Reihe von Hash-Nachrichtenauthentifizierungscodes (Hashed Message Authentication Code, HMAC) zu erstellen.

Signatur-Berechnungsbeispiel

Das folgende Beispiel macht Sie damit vertraut, wie Sie eine Signatur für ListGateways erstellen. Das Beispiel kann als Referenz verwendet werden, um Ihre Signaturberechnungsmethode zu überprüfen. Andere Referenzberechnungen finden Sie in der Signature Version 4 Test Suite des Amazon Web Services-Glossars.

In diesem Beispiel wird Folgendes angenommen:

- Der Zeitstempel für die Anforderung ist „Mon, 10 Sep 2012 00:00:00“ GMT.
- Der Endpunkt ist die Region USA Ost (Ohio).

Die allgemeine Anforderungssyntax (einschließlich JSON-Text) ist:

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

Die kanonische Form der für Aufgabe 1: Erstellen einer kanonischen Anforderung berechneten Anforderung ist:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

Die letzte Zeile der kanonischen Anforderungen ist der Hash des Anforderungstextes. Beachten Sie auch die leere dritte Zeile in der kanonischen Anforderung. Der Grund dafür ist, dass es keine Abfrageparameter für diese API (oder beliebige Storage Gateway-APIs) gibt.

Die zu signierende Zeichenfolge für Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge ist:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

Die erste Zeile der zu signierenden Zeichenfolge ist der Algorithmus, die zweite Zeile der Zeitstempel, die dritte Zeile der Umfang der Anmeldeinformationen und die letzte Zeile ein Hash der kanonischen Anforderung aus Aufgabe 1.

Für Aufgabe 3: Erstellen einer Signatur kann der abgeleitete Schlüssel wie folgt dargestellt werden:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Wenn der geheime Zugriffsschlüssel wJalrXUtnFEMI /K7MDENG/bPxRfiCYEXAMPLEKEY verwendet wird, ist 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 Operationsfehlercode `ActivationKeyInvalid` wird jedoch nur für die ActivateGateway API zurückgegeben.

Abhängig von der Art des Fehlers kann Storage Gateway nur eine Ausnahme oder eine Ausnahme und einen Fehlercode für die Operation zurückgegeben. Beispiele für Fehlermeldungen finden Sie unter Fehlermeldungen.

Ausnahmen

In der folgenden Tabelle sind AWS Storage Gateway API-Ausnahmen aufgeführt. Wenn eine AWS Storage Gateway Operation eine Fehlerantwort zurückgibt, enthält der Antworttext eine dieser Ausnahmen. Die Codes `InternalServerError` und `InvalidGatewayRequestException` geben eine Operationsfehlercodes-Nachricht zurück, in der der entsprechende Operationsfehlercode angegeben ist.

Exception	Fehlermeldung	HTTP-Statuscode
`IncompleteSignatureException`	Die angegebene Signatur ist unvollständig.	400 Ungültige Anfrage
`InternalFailure`	Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.	500 Internal Server Error
`InternalServerError`	Eine der Operationsfehlercode-Nachrichten Operationsfehlercodes.	500 Internal Server Error
`InvalidAction`	Die angeforderte Aktion oder Operation ist ungültig.	400 Ungültige Anfrage

Exception	Fehlermeldung	HTTP-Statuscode
`InvalidClientTokenId`	Das bereitgestellte X.509-Zertifikat oder die bereitgestellte AWS Zugriffsschlüssel-ID ist in unseren Datensätzen nicht vorhanden.	403 Verboten
`InvalidGatewayRequestException`	Eine der Operationsfehlercode-Nachrichten in Operationsfehlercodes.	400 Ungültige Anfrage
`InvalidSignatureException`	Die berechnete Anforderungssignatur entspricht nicht der angegebenen Signatur. Überprüfen Sie Ihren - AWS Zugriffsschlüssel und Ihre Signaturmethode.	400 Ungültige Anfrage
`MissingAction`	In der Anforderung fehlt ein Aktions- oder Operationsparameter.	400 Ungültige Anfrage
`MissingAuthenticationToken`	Die Anforderung muss entweder eine gültige (registrierte) AWS Zugriffsschlüssel-ID oder ein X.509-Zertifikat enthalten.	403 Verboten
`RequestExpired`	Die Anforderung liegt nach dem Ablaufdatum oder dem Anforderungsdatum (jeweils in 15-Minuten-Schritten) oder das Anforderungsdatum liegt mehr als 15 Minuten in der Zukunft.	400 Ungültige Anfrage
`SerializationException`	Fehler bei der Serialisierung. Stellen Sie sicher, dass Ihre JSON-Nutzdaten wohlgeformt sind.	400 Ungültige Anfrage

Exception	Fehlermeldung	HTTP-Statuscode
`ServiceUnavailable`	Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.	503 Service Unavailable (503 Service nicht verfügbar)
`SubscriptionRequiredException`	Die AWS Zugriffsschlüssel-ID benötigt ein Abonnement für den Service.	400 Ungültige Anfrage
`ThrottlingException`	Rate überschritten.	400 Ungültige Anfrage
`UnknownOperationException`	Eine unbekannte Operation wurde angegeben. Gültige Operationen werden in Operationen im Storage Gateway aufgeführt.	400 Ungültige Anfrage
`UnrecognizedClientException`	Das Sicherheits-Token der Anfrage ist nicht gültig.	400 Ungültige Anfrage
`ValidationException`	Der Wert des Parameters ist ungültig oder außerhalb des Bereichs.	400 Ungültige Anfrage

Operationsfehlercodes

Die folgende Tabelle zeigt die Zuordnung zwischen AWS Storage Gateway Operationsfehlercodes und 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

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`ActivationKeyInvalid`	Der angegebene Aktivierungsschlüssel ist nicht gültig.	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 CreateStorediSCSIVolume
`DiskDoesNotExist`	Der angegebene Datenträger ist nicht vorhanden.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`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

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 falsche 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 falsch.	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 nicht gültig.	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 nicht gültig.	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 nicht gültig.	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 angegebene Volume ist nicht einsatzbereit.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Fehlermeldungen

Bei einem Fehler enthalten die Informationen im Antwort-Header:

- Inhaltstyp: application/x-amz-json-1.1
- Einen passenden `4xx`- oder `5xx`-HTTP-Statuscode

Der Textkörper einer Fehlermeldung enthält Informationen zu dem aufgetretenen Fehler. Das folgende Beispiel zeigt eine Fehlerantwort mit der Ausgabesyntax von Antwortelementen für alle Fehlermeldungen.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

In der folgenden Tabellen werden die Felder der JSON-Fehlerantwort in dieser Syntax erläutert.

__type

Eine der Ausnahmen aus Ausnahmen.

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-Text wird zurückgegeben, wenn Sie die DescribeStorediSCSIVolumes-API verwenden und eine Gateway-ARN-Anforderungseingabe angeben, die nicht vorhanden ist.

```
{
  "__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."
}
```

Operationen im Storage Gateway

Eine vollständige Liste der Storage Gateway-Operationen finden Sie unter Aktionen in der AWS Storage Gateway -API-Referenz.

Dokumentenverlauf für das Tape Gateway Benutzerhandbuch

- API-Version: 2013-06-30
- Letzte Aktualisierung der Dokumentation: 24. November 2020

In der folgenden Tabelle sind wichtige Änderungen der einzelnen Versionen des AWS Storage Gateway Benutzerhandbuchs nach April 2018 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Veraltete Unterstützung für Tape Gateway auf Snowball Edge	Es ist nicht mehr möglich, Tape Gateway auf Snowball-Edge-Geräten zu hosten.	14. März 2024
Aktualisierte Anweisungen zum Testen Ihrer Gateway-Einrichtung mit Anwendungen von Drittanbietern	Die Anweisungen zum Testen Ihrer Gateway-Einrichtung mithilfe von Drittanbieteranwendungen beschreiben jetzt das erwartete Verhalten, wenn Ihr Gateway während einer laufenden Backup-Aufgabe neu gestartet wird. Weitere Informationen finden Sie unter Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung.	24. Oktober 2023
Empfohlene CloudWatch Alarme wurden aktualisiert	Der CloudWatch `HealthNotifications` Alarm gilt jetzt für und wird für alle Gateway-Typen und Hostplattformen empfohlen. Die empfohlenen Konfigurationseins	2. Oktober 2023

	tellungen wurden auch für `HealthNotifications` und `AvailabilityNotifications` aktualisiert. Weitere Informationen finden Sie unter Grundlegendes zu CloudWatch Alarmen	
Erhöhung der maximalen Bandgröße auf 15 TiB für Tape Gateways	Außerdem wurde für Tape Gateways die maximale Größe virtueller Bänder jetzt von 5 TiB auf 15 TiB erhöht. Weitere Informationen finden Sie unter Kontingente für Bänder im Storage Gateway-Benutzerhandbuch.	4. Oktober 2022
Separate Benutzerhandbücher für Tape und Volume Gateway	Das Storage Gateway-Benutzerhandbuch, das zuvor Informationen sowohl zu den Tape- als auch zu den Volume Gateway-Typen enthielt, wurde in das Tape Gateway-Benutzerhandbuch und das Volume Gateway-Benutzerhandbuch aufgeteilt, die jeweils nur Informationen zu einem Gateway-Typ enthalten. Weitere Informationen finden Sie im Tape Gateway-Benutzerhandbuch und im Volume Gateway-Benutzerhandbuch.	23. März 2022

Aktualisierte Verfahren zur Gateway-Erstellung	Die Verfahren zum Erstellen aller Gateway-Typen mit der Storage-Gateway-Konsole wurden aktualisiert. Weitere Informationen finden Sie unter Erstellen eines Gateways.	18. Januar 2022
Neue Bandoberfläche	Die Seite Bandübersicht in der AWS Storage Gateway Konsole wurde mit neuen Such- und Filterfunktionen aktualisiert. Alle relevante n Verfahren in diesem Handbuch wurden aktualisi ert, um die neuen Funktione n zu beschreiben. Weitere Informationen finden Sie unter Verwalten des Tape Gateways.	23. September 2021
Unterstützung für Bol NetVault Backup 13 für Tape Gateway	Tape Gateways unterstützen jetzt Bol NetVault Backup 13, das auf Microsoft Windows Server 2012 R2 oder Microsoft Windows Server 2016 ausgeführt wird. Weitere Informationen finden Sie unter Testen Ihrer Einrichtu ng mithilfe von Quest NetVault Backup.	22. August 2021

Die Themen zu S3 File Gateway wurden aus den Tape- und Volume Gateway-Benutzerhandbüchern entfernt	Um Kunden, die ihre jeweiligen Gateway-Typen einrichten, die Benutzerhandbücher für Tape Gateway und Volume Gateway leichter verständlich zu machen, wurden einige überflüssige Themen entfernt.	21. Juli 2021
Unterstützung für IBM Spectrum Protect 8.1.10 unter Windows und Linux für Tape Gateway	Tape Gateways unterstützen jetzt IBM Spectrum Protect Version 8.1.10, das auf Microsoft Windows Server und Linux läuft. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mithilfe von IBM Spectrum Protect.	24. November 2020
FedRAMP-Compliance	Storage Gateway ist jetzt FedRAMP-konform. Weitere Informationen finden Sie unter Compliance-Validierung für Storage Gateway .	24. November 2020
Zeitplanbasierte Bandbreitendrosselung	Storage Gateway unterstützt jetzt die zeitplanbasierte Bandbreitendrosselung für Tape und Volume Gateways. Weitere Informationen finden Sie unter Planen der Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole.	9. November 2020

Der lokale Cache-Speicher von zwischengespeicherten Volume und Tape Gateways wird vervierfacht	Storage Gateway unterstützt jetzt einen lokalen Cache von bis zu 64 TB für zwischeng espeicherte Volume und Tape Gateways und verbessert so die Leistung für On-Premis es-Anwendungen, indem der Zugriff mit geringer Latenz auf größere Arbeitsdatensätze ermöglicht wird. Weitere Informationen finden Sie unter Empfohlene lokale Festplatt engrößen für Ihr Gateway.	9. November 2020
Gateway-Migration	Storage Gateway unterstüt zt jetzt die Migration zwischengespeicherter Volume Gateways auf neue virtuelle Maschinen. Weitere Informationen finden Sie unter Verschieben zwischeng espeicherter Volumes auf eine neue virtuelle zwischeng espeicherte Volume Gateway-Maschine.	10. September 2020

Unterstützung für Bandaufbewahrungssperre und write-once-read-many (WORM)-Bandschutz	Storage Gateway unterstützt die Bandaufbewahrungssperre auf virtuellen Bändern und Write Once Read Many (WORM). Mit der Bandaufbewahrungssperre können Sie den Aufbewahrungsmodus und den Aufbewahrungszeitraum für archivierte virtuelle Bänder festlegen und so verhindern, dass diese für einen festen Zeitraum von bis zu 100 Jahren gelöscht werden. Dazu gehören Zugriffsrechte, die festlegen, wer Bänder löschen oder Aufbewahrungseinstellungen ändern kann. Weitere Informationen finden Sie unter Verwenden von Bandaufbewahrungssperre. Durch WORM-aktivierte virtuelle Bänder stellen Sie sicher, dass Daten auf aktiven Bändern in Ihrer virtuellen Bandbibliothek nicht überschrieben oder gelöscht werden können. Weitere Informationen finden Sie unter Write Once, Read Many (WORM)-Bandschutz.	19. 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 Storage Gateway-Hardware-Appliance.	12. August 2020
Unterstützung von Endpunkten für den Federal Information Processing Standard (FIPS) in neuen AWS -Regionen	Sie können jetzt ein Gateway mit FIPS-Endpunkten in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Nordkalifornien), USA West (Oregon) und Kanada (Zentral) aktivieren. Weitere Informationen finden Sie unter AWS Storage Gateway - Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	31. Juli 2020
Gateway-Migration	Storage Gateway unterstützt jetzt die Migration von Tape und zwischengespeicherter Volume Gateways auf neue virtuelle Maschinen. Weitere Informationen finden Sie unter Verschieben Ihrer Daten auf ein neues Gateway .	31. Juli 2020
Anzeigen von Amazon-CloudWatch Alarmen in der Storage Gateway-Konsole	Sie können jetzt CloudWatch Alarme in der Storage 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 zum Auswählen eines FIPS-Endpunkts für ein Volume-Gateway finden Sie unter Auswählen eines Service-Endpunkts. Informationen zur Auswahl eines FIPS-Endpunkts für ein Tape Gateway finden Sie unter Verbinden Ihres Tape Gateways mit AWS.	22. Mai 2020
Neue AWS Regionen	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
Erhöhung der Schreib- und Leseleistung des Band-Gateways auf das Doppelte	Storage Gateway verdoppelt die Schreib- und Leseleistung auf und von virtuellen Bändern in Tape Gateway für schnellere Backups und Wiederherstellungen als zuvor. Weitere Informationen finden Sie unter Leistungsleitfaden für Tape Gateways im Storage Gateway-Benutzerhandbuch.	23. April 2020

Unterstützung für die automatische Banderstellung	Storage Gateway bietet jetzt die Möglichkeit, neue virtuelle Bänder automatisch zu erstellen. Tape Gateway erstellt automatisch neue virtuelle Bänder, um die Anzahl der von Ihnen konfigurierten verfügbaren Bänder minimal zu halten und diese neuen Bänder für den Import durch die Speicheranwendung verfügbar zu machen. So können Ihre Backup-Aufgaben unterbrechungsfrei ausgeführt werden. Weitere Informationen finden Sie unter Automatisches Erstellen von Bändern im Storage Gateway-Benutzerhandbuch.	23. 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 stellt jetzt Support für hohe Verfügbarkeit auf VMware bereit, um Speicher-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-Benutzerhandbuch. Diese Version enthält auch Leistungsverbesserungen. Weitere Informationen finden Sie unter Leistung im Storage Gateway-Benutzerhandbuch.	20. November 2019

Neue AWS Region für Tape Gateway	Tape Gateway ist jetzt in der Region Südamerika (Sao Paulo) verfügbar. Weitere Informationen finden Sie unter AWS Storage Gateway - Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	24. September 2019
Unterstützung für IBM Spectrum Protect Version 7.1.9 auf Linux und Steigerung der maximalen Bandgröße für Band-Gateways auf 5 TiB	Tape Gateways unterstützen jetzt IBM Spectrum Protect (Tivoli Storage Manager) Version 7.1.9 auf Linux, zusätzlich zu Microsoft Windows. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mithilfe von IBM Spectrum Protect im Storage Gateway-Benutzerhandbuch. Außerdem wurde für Tape Gateways die maximale Größe virtueller Bänder jetzt von 2,5 TiB auf 5 TiB erhöht. Weitere Informationen finden Sie unter Kontingente für Bänder im Storage Gateway-Benutzerhandbuch.	10. September 2019

Unterstützung 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 den Zustand und die Fehler von Gateway mit Amazon- CloudWatch Protokollgruppen im Storage Gateway-Benutzerhandbuch.	4. September 2019
Neue 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
Neue 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
Unterstützung für das Verschieben virtueller Bänder von S3 Glacier Flexible Retrieval nach S3 Glacier Deep Archive	Sie können Ihre virtuellen Bänder, die in der Speicherklasse S3 Glacier Flexible Retrieval archiviert sind, für kostengünstige und langfristige Datenaufbewahrung jetzt zur Speicherklasse S3 Glacier Deep Archive verschieben. Weitere Informationen finden Sie unter Verschieben eines Bands von S3 Glacier Flexible Retrieval zu S3 Glacier Deep Archive.	28. Mai 2019
Unterstützung der SMB-Dateifreigabe für Microsoft Windows-ACLs	Für File Gateways können Sie jetzt Microsoft Windows-Zugriffskontrolllisten (ACLs) verwenden, um den Zugriff auf Server Message Block (SMB)-Dateifreigaben zu steuern. Weitere Informationen finden Sie unter Verwenden von Microsoft Windows-ACLs zum Steuern des Zugriffs auf eine SMB-Dateifreigabe .	8. Mai 2019

Integration in S3 Glacier Deep Archive	Tape Gateway lässt sich in S3 Glacier Deep Archive integrieren. Sie können jetzt virtuelle Bänder in S3 Glacier Deep Archive für die langfristige Aufbewahrung von Daten archivieren. Weitere Informationen finden Sie unter Archivierung virtueller Bänder.	27. März 2019
Verfügbarkeit der Storage Gateway-Hardware-Appliance in Europa	Die Storage Gateway-Hardware-Appliance ist 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 in der Storage Gateway-Hardware-Appliance von 5 TB auf 12 TB erhöhen und die installierte Kupfer-Netzwerkkarte mit einer 10-Gigabit-Glasfaser-Netzwerkkarte ersetzen. Weitere Informationen finden Sie unter Einrichten Ihrer Hardware-Appliance.	25. Februar 2019

Integration mit AWS Backup	Storage Gateway lässt sich in integrieren AWS Backup. Sie können jetzt verwenden AWS Backup , um lokale Geschäfts anwendungen zu sichern, die Storage Gateway-Volumes für Cloud-gestützten Speicher verwenden. Weitere Informati onen finden Sie unter Sichern Ihrer Volumes.	16. Januar 2019
Unterstützung für Bacula Enterprise und IBM Spectrum Protect	Tape Gateways unterstüt zen jetzt Bacula Enterprise und IBM Spectrum Protect. Storage Gateway unterstützt jetzt auch neuere Versionen von Ver Bols NetBackup, Ver Bols Backup Exec und Bol NetVault Backup. Sie können nun diese Sicherung sanwendungen verwenden , um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Verwenden Ihrer Sicherung ssoftware zum Testen Ihrer Gateway-Einrichtung.	13. November 2018

Unterstützung für Storage Gateway-Hardware-Appliance	Die Storage Gateway-Hardware-Applicance enthält auf einem Drittanbieterserver vorinstallierte Storage Gateway-Software. Sie können die Appliance in der AWS Management Console verwalten. Die Appliance kann Datei-, Band- und Volume Gateways hosten. Weitere Informationen finden Sie unter Verwenden der Storage Gateway-Hardware-Appliance.	18. September 2018
Kompatibilität mit dem Microsoft System Center 2016 DPM Data Protection Manager (DPM)	Tape Gateways sind jetzt mit dem Microsoft System Center 2016 DPM Data Protection Manager (DPM) kompatibel. Sie können nun Microsoft DPM verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mithilfe von Microsoft System Center Data Protection Manager.	18. Juli 2018

Support für Server Message Block (SMB)-Protokolle	File Gateways bieten jetzt Unterstützung für Server Message Block (SMB)-Protokolle bei Dateifreigaben. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	20. Juni 2018
Unterstützung für Dateifreigaben, Cached-Volumes und Verschlüsselung von Daten auf einem virtuellen Band	Sie können jetzt AWS Key Management Service (AWS KMS) verwenden, um Daten zu verschlüsseln, die auf eine Dateifreigabe, ein zwischengespeichertes Volume oder ein virtuelles Band geschrieben wurden. Derzeit können Sie dies mit der AWS Storage Gateway -API durchführen. Weitere Informationen finden Sie unter Datenverschlüsselung mit AWS KMS.	12. Juni 2018

Unterstützung für NovaStor DataCenter/Network	Tape Gateways unterstützen jetzt NovaStor DataCente r/Network. Sie können jetzt NovaStor DataCenter/ Network Version 6.4 oder 7.1 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt im Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informati onen finden Sie unter Testen Ihrer Einrichtung mithilfe von NovaStor DataCenter/Network .	24. Mai 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.

Änderung	Beschreibung	Änderungsdatum
Support für S3 One Zone_IA-S peicherklasse	Für File Gateways können Sie jetzt die S3 One Zone_IA als Standard-Speicherklasse für Ihre Dateifrei gaben wählen. Diese Speicherklasse ermöglicht Ihnen das Speichern Ihrer Objektdaten in einer einzelnen Availability Zone in Amazon S3. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	4. April 2018
Neue -Region	Tape Gateway ist jetzt in der Region Asien-Pazifik (Singapur) erhältlich. Weitere Informationen hierzu finden Sie unter AWS Regionen.	3. April 2018
Unterstützung für Benachric	Mit File Gateways können Sie nun eine Benachric htigung erhalten, wenn ein Gateway die Aktualisierung	1. März 2018

Änderung	Beschreibung	Änderungsdatum
htigungen zur Cache-Aktualisierung, Zahlung durch den Anforderer und vorgefertigte ACLs für Amazon S3-Buckets.	des Caches für Ihren Amazon S3-Bucket abgeschlossen hat. Weitere Informationen finden Sie unter RefreshCache.html in der Storage Gateway-API-Referenz . Mithilfe von File Gateways kann nun der Anforderer oder Abrufende anstelle des Bucket-Eigentümers für den Zugriff zahlen. Mithilfe von File Gateways können Sie nun dem Eigentümer des S3-Buckets, der der NFS-Datei freigabe zugeordnet ist, die volle Kontrolle gewähren. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	
Unterstützung für Dell EMC NetWorker V9.x	Tape Gateways unterstützen jetzt Dell EMC NetWorker V9.x. Sie können jetzt Dell EMC NetWorker V9.x verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt im Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mit Dell EMC. NetWorker	27. Februar 2018
Neue -Region	Storage Gateway ist jetzt in der Region Europa (Paris) verfügbar. Weitere Informationen hierzu finden Sie unter AWS Regionen.	18. Dezember 2017

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Datei-Upload-Benachrichtigung und zur Bestimmung des MIME-Typs	Mit File Gateways können Sie jetzt Benachrichtigungen erhalten, sobald alle Dateien, die auf Ihre NFS-Dateifreigabe geschrieben werden, zu Amazon S3 hochgeladen wurden. Weitere Informationen finden Sie unter NotifyWhenUploaded in der Storage Gateway-API-Referenz. Mit File Gateways können Sie jetzt den MIME-Typ für hochgeladene Objekte basierend auf Dateierweiterungen bestimmen. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	21. November 2017
Unterstützung für die Version 6.5 des Hypervisors VMware ESXi	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
Kompatibilität mit CommVault 11	Tape Gateways sind jetzt mit Commvault 11 kompatibel. Sie können nun Commvault verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mit Commvault.	12. 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

Änderung	Beschreibung	Änderungsdatum
Unterstützung für das Abrufen von Bändern aus Archiven innerhalb von 3 bis 5 Stunden	In der Tape Gateway-Konfiguration können Bänder jetzt innerhalb von 3 bis 5 Stunden aus einem Archiv abgerufen werden. Sie können zudem ermitteln, wie viele Daten von Ihrer Sicherungsanwendung oder Ihrer virtuellen Bandbibliothek (VTL, Virtual Tape Library) auf das Band geschrieben wurden. Weitere Informationen finden Sie unter Anzeigen von Benutzerdetails.	23. Mai 2017
Neue -Region	Storage Gateway ist jetzt in der Region Asien-Pazifik (Mumbai) erhältlich. Weitere Informationen hierzu finden Sie unter AWS Regionen.	02. Mai 2017
Updates bei den Einstellungen für Dateifreigaben Unterstützung für die Cache-Aktualisierung in Dateifreigaben	Die Einstellungen für Dateifreigaben in der File Gateway-Konfiguration wurden um Mounting-Optionen erweitert. Nun stehen für Dateifreigaben eine Squash-Option und eine schreibgeschützte Option zur Verfügung. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe. In der File-Gateway-Konfiguration lassen sich nun alle Objekte im Amazon-S3-Bucket finden, die hinzugefügt oder entfernt wurden, seit das Gateway letztmals die Inhalte des Buckets aufgelistet und die Ergebnisse zwischengespeichert hat. Weitere Informationen finden Sie unter RefreshCache in der -API-Referenz.	28. März 2017
Unterstützung für das Klonen von Volumes	Für zwischengespeicherte Volume Gateways unterstützt AWS Storage Gateway jetzt die Möglichkeit, ein Volume von einem vorhandenen Volume zu klonen. Weitere Informationen finden Sie unter Klonen eines Volumes.	16. März 2017

Änderung	Beschreibung	Änderungsdatum
Unterstützung für File Gateways in Amazon EC2	AWS Storage Gateway bietet jetzt die Möglichkeit, ein File Gateway in Amazon EC2 bereitzustellen. Sie können in Amazon EC2 einen File Gateway auf der Basis des Storage Gateway-Amazon Machine Image (AMI) starten, das nun als Community-AMI verfügbar ist. Informationen zum Erstellen und Bereitstellen eines File Gateways auf einer EC2-Instance finden Sie unter Erstellen und Aktivieren eines Amazon S3 File Gateways oder Erstellen und Aktivieren eines Amazon FSx File Gateways. Informationen zum Starten eines File Gateway-AMI finden Sie unter Bereitstellen eines S3 File Gateways auf einem Amazon-EC2-Host oder Bereitstellen eines FSx File Gateways auf einem Amazon-EC2-Host.	08. Februar 2017
Kompatibilität mit Arcserve 17	Tape-Gateway ist nun mit Arcserve 17 kompatibel. Sie können jetzt Arcserve verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in S3 Glacier Flexible Retrieval zu archivieren. Weitere Informati onen finden Sie unter Testen Ihres Einrichtung mithilfe von Arcserve Backup r17.0.	17. Januar 2017
Neue -Region	Storage Gateway ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen hierzu finden Sie unter AWS Regionen.	13. Dezember 2016
Neue -Region	Storage Gateway ist jetzt in der Region Kanada (Zentral) verfügbar. Weitere Informationen hierzu finden Sie unter AWS Regionen.	08. Dezember 2016

Änderung	Beschreibung	Änderungsdatum
Unterstützung für File Gateway	Zusätzlich zu Volume Gateways und Tape Gateway bietet Storage Gateway jetzt File Gateway. File Gateway kombiniert einen Service und eine virtuelle Software-Appliance. So können Sie Objekte in Amazon S3 mit Dateiprotokollen nach Branchens tandard wie beispielsweise NFS (Network File System) speichern und abrufen. Das Gateway stellt Objekte in Amazon S3 als Dateien auf einem NFS-Mounting-Punkt bereit.	29. November 2016
Backup Exec 16	Tape-Gateway ist nun mit Backup Exec 16 kompatibel. Sie können nun Backup Exec 16 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-S peicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihres Einrichtung mithilfe von Veritas Backup Exec.	7. November 2016
Kompatibilität mit Micro Focus (HPE) Data Protector 9.x	Tape Gateways sind nun mit Micro Focus (HPE) Data Protector 9.x kompatibel. Sie können jetzt HPE Data Protector verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in S3 Glacier Flexible Retrieval zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Konfiguration mithilfe von Micro Focus (HPE) Data Protector.	2. November 2016
Neue -Region	Storage Gateway ist nun in der Region USA Ost (Ohio)) verfügbar. Weitere Informationen hierzu finden Sie unter AWS Regionen.	17. Oktober 2016

Änderung	Beschreibung	Änderungsdatum
Überarbeitung der Storage Gateway-Konsole	Die Storage Gateway-Managementkonsole wurde überarbeitet. Die Konfiguration, die Verwaltung und die Überwachung von Gateways, Volumes und virtuellen Bändern sind jetzt einfacher. Die Benutzeroberfläche bietet jetzt Ansichten, die gefiltert werden können, und bietet direkte Links zu integrierten AWS Services wie CloudWatch und Amazon EBS. Weitere Informationen finden Sie unter Registrieren für AWS Storage Gateway.	30. August 2016
Kompatibilität mit Veeam Backup & Replication V9 Update 2 und höher	Tape-Gateway ist nun kompatibel mit Veeam Backup & Replication V9 Update 2 und höher (d. h. mit Version 9.0.0.1715 und höheren Versionen). Sie können nun Veeam Backup Replication V9 Update 2verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen der Einrichtung mithilfe von Veeam Backup & Replication.	15. August 2016
Längere IDs für Volumes und Snapshots	Storage Gateway unterstützt jetzt längere IDs für Volumes und Snapshots. Sie können das längere ID-Format für Ihre Volumes, Snapshots und andere unterstützte AWS Ressourcen aktivieren. Weitere Informationen finden Sie unter Grundlegendes zu Ressourcen und Ressourcen-IDs von Storage Gateway.	25. April 2016

Änderung	Beschreibung	Änderungsdatum
Neue -Region Unterstützung für Stored Volumes mit bis zu 512 TiB Speicherkapazität Sonstige Gateway-Updates und -Verbesserungen in der lokalen Storage-Gateway-Konsole	Tape Gateway ist nun in der Region Asien-Pazifik (Seoul) verfügbar. Weitere Informationen finden Sie unter AWS Regionen. Stored Volumes unterstützen jetzt bis zu 32 Speicher-Volumes mit je bis zu 16 TiB und damit eine maximale Speicherkapazität von 512 TiB. Weitere Informationen finden Sie unter Architektur mit Stored Volumes und AWS Storage Gateway -Kontingente. Die zulässige Gesamtgröße aller Bänder in einer virtuellen Bandbibliothek wurde auf 1 PiB erhöht. Weitere Informationen finden Sie unter AWS Storage Gateway -Kontingente. Das Passwort der lokalen VM-Konsole kann jetzt in der Storage-Gateway-Konsole festgelegt werden. Weitere Informationen finden Sie unter Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole.	21. März 2016
Kompatibilität mit für Dell EMC NetWorker 8.x	Tape Gateway ist jetzt mit Dell EMC NetWorker 8.x kompatibel. Sie können jetzt Dell EMC verwenden NetWorker , um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mit Dell EMC. NetWorker	29. Februar 2016

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Version 6.0 des Hypervisors VMware ESXi sowie den Red Hat Enterprise Linux 7-iSCSI-Initiator	AWS Storage Gateway unterstützt jetzt den VMware ESXi Hypervisor Version 6.0 und den iSCSI-Initiator von Red Hat Enterprise Linux 7. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen und Unterstützte iSCSI-Initiatoren.	20. Oktober 2015
Inhaltsumstrukturierung	Diese Version umfasst die folgende Verbesserung: Die Dokumentation wurde um einen Abschnitt zur Verwaltung aktivierter Gateways ergänzt. Dort finden Sie eine Übersicht über Verwaltungsaufgaben, die für alle Gateway-Lösungen gleich sind. Zudem finden Sie Anweisungen zur Verwaltung von Gateways nach der Bereitstellung und Aktivierung. Weitere Informationen finden Sie unter Verwalten von Gateways.	

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Cached Volumes mit bis zu 1 024 TiB Speicherkapazität Unterstützung für Netzwerkadapter des Typs VMXNET3 (10GbE) im Hypervisor VMware ESXi Leistungsverbesserungen Verschiedene Verbesserungen und Aktualisierungen in der lokalen Storage Gateway-Konsole	Cached Volumes unterstützen jetzt bis zu 32 Speicher-Volumes mit je bis zu 32 TiB und damit eine maximale Speicherkapazität von 1 024 TiB. Weitere Informationen finden Sie unter Architektur mit zwischengespeicherten Volumes und AWS Storage Gateway -Kontingente. Auf einem VMware ESXi-Hypervisor gehostete Gateways können jetzt so konfiguriert werden, dass sie den Adaptertyp VMXNET3 verwenden. Weitere Informationen finden Sie unter Konfigurieren von Networkadaptern für Ihr Gateway. Die maximale Upload-Rate für Storage Gateway wurde auf 120 MB pro Sekunde erhöht, die maximale Download-Rate auf 20 MB pro Sekunde. Die lokale Storage-Gateway-Konsole wurde aktualisiert und um zusätzliche Funktionen erweitert, die Sie bei Verwaltungsaufgaben unterstützen. Weitere Informationen finden Sie unter Konfigurieren Ihres Gateway-Netzwerks.	16. September 2015
Support für Markierungen	Storage Gateway unterstützt nun das Markieren von Ressourcen. Gateways, Volumes und virtuellen Bändern lassen sich zur einfacheren Verwaltung nun Tags hinzufügen. Weitere Informationen finden Sie unter Kennzeichnen der Storage Gateway-Ressourcen .	2. September 2015

Änderung	Beschreibung	Änderungsdatum
Kompatibilität mit Bol (früher Dell) NetVault Backup 10.0	Tape Gateway ist jetzt mit Bol NetVault Backup 10.0 kompatibel. Sie können jetzt Bol NetVault Backup 10.0 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt im Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivier en. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mithilfe von Quest NetVault Backup.	22. Juni 2015

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Speicher-Volumes mit 16 TiB in Gateway-Konfigurationen mit Stored Volumes	Storage Gateway unterstützt jetzt Speicher-Volumes mit 16 TiB in Gateway-Konfigurationen mit Stored Volumes. Sie können nun 12 Speicher-Volumes mit je 16 TiB erstellen, für eine maximale Speicherkapazität von 192 TiB. Weitere Informationen finden Sie unter Architektur mit Stored Volumes.	3. Juni 2015
Unterstützung für eine Überprüfung der Systemressourcen in der lokalen Storage-Gateway-Konsole	Sie können jetzt ermitteln, ob ausreichend Systemressourcen (virtuelle CPU-Kerne, Kapazität des Stamm-Volumes und RAM) für die ordnungsgemäße Funktionsweise Ihres Gateways verfügbar sind. Weitere Informationen finden Sie unter Anzeigen des Gateway-Systemressourcen-Status oder Anzeigen des Gateway-Systemressourcen-Status.	
Unterstützung für den Red Hat Enterprise Linux 6-iSCSI-Initiator	Storage Gateway unterstützt jetzt den Red Hat Enterprise Linux 6-iSCSI-Initiator. Weitere Informationen finden Sie unter Voraussetzungen. Diese Version umfasst die folgenden Verbesserungen und Aktualisierungen für Storage Gateway: • In der Storage-Gateway-Konsole können Sie jetzt das Datum und die Uhrzeit des letzten erfolgreichen Software-Updates auf Ihrem Gateway sehen. Weitere Informationen finden Sie unter Verwalten von Gateway-Updates über die AWS Storage Gateway -Konsole. • Storage Gateway bietet nun eine API, über die Sie alle iSCSI-Initiatoren auflisten können, die mit Ihren Speicher-Volumes verbunden sind. Weitere	

Änderung	Beschreibung	Änderungsdatum
	Informationen finden Sie unter ListVolumeInitiators in der -API-Referenz.	
Unterstützung für die Versionen 2012 und 2012 R2 des Hypervisors Microsoft Hyper-V	Storage Gateway unterstützt jetzt die Versionen 2012 und 2012 R2 des Hypervisors Microsoft Hyper-V. Unterstützung für die Version 2008 R2 des Hypervisors Microsoft Hyper-V war bereits zuvor implementiert. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	30. April 2015
Kompatibilität mit Symantec Backup E:	Tape Gateway ist nun mit Symantec Backup Exec 15 kompatibel. Sie können nun Symantec Backup Exec 15 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec.	6. April 2015
Unterstützung für die CHAP-Auth entifizierung für Speicher-Volumes	Storage Gateway unterstützt jetzt die Konfiguration von CHAP-Authentifizierung für Speicher-Volumes. Weitere Informationen finden Sie unter Konfigurieren der CHAP-Authentifizierung für Ihre Volumes.	2. April 2015
Unterstützung für die Versionen 5.1 und 5.5 des Hypervisors VMware ESXi	Storage Gateway unterstützt nun VMware ESXi Hypervisor 5.1 und 5.5. Diese Versionen werden zusätzlich zu VMware ESXi Hypervisor 4.1 und 5.0 unterstützt. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	30. März 2015

Änderung	Beschreibung	Änderungsdatum
Unterstützung für das Windows-Dienstprogramm CHKDSK	Storage Gateway unterstützt jetzt das Windows-Dienstprogramm CHKDSK. Mithilfe dieses Dienstprogramms können Sie die Integrität Ihrer Volumes überprüfen und Volume-Fehler beheben. Weitere Informationen finden Sie unter Fehlerbehebung bei Volume-Problemen.	04. März 2015
Integration mit AWS CloudTrail zur Erfassung von API-Aufrufen	Storage Gateway ist jetzt in AWS CloudTrail. AWS CloudTrail captures-API-Aufrufe integriert, die von oder im Namen von Storage Gateway in Ihrem Amazon-Web-Services-Konto getätigt wurden, und stellt die Protokolldateien in einem von Ihnen angegebenen Amazon S3-Bucket bereit. Weitere Informationen finden Sie unter Protokollierung und Überwachung in AWS Storage Gateway. Diese Version umfasst die folgenden Verbesserungen und Aktualisierungen für Storage Gateway: • Virtuelle Bänder, in deren Cache-Speicher ungültige Daten abgelegt sind (d. h. in denen nicht in AWS hochgeladene Inhalte abgelegt sind), werden jetzt wiederhergestellt, wenn das zwischengespeicherte Laufwerk eines Gateways geändert wird. Weitere Informationen finden Sie unter Wiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway.	16. Dezember 2014

Änderung	Beschreibung	Änderungsdatum
Kompatibilität mit weiterer Sicherungssoftware und einem weiteren Medienwechsler	Tape-Gateway ist nun kompatibel mit der folgenden Sicherungssoftware: • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 Sie können jetzt diese vier Sicherungssoftware-Produkte mit der virtuellen Bandbibliothek (Virtual Tape Library, VTL) von Storage Gateway verwenden , um Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung. Storage Gateway bietet nun einen zusätzlichen Medienwechsler, der mit der neuen Sicherungssoftware kompatibel ist. Diese Version enthält verschiedene AWS Storage Gateway Verbesserungen und Updates.	3. November 2014
Region Europa (Frankfurt)	Storage Gateway ist jetzt in der Region Europa (Frankfurt) verfügbar. Weitere Informationen hierzu finden Sie unter AWS Regionen.	23. Oktober 2014

Änderung	Beschreibung	Änderungsdatum
Inhaltsumstrukturierung	Wir haben einen gemeinsamen Erste-Schritte-Abschnitt für sämtliche Gateway-Lösungen verfasst. Dort finden Sie Links zu Anweisungen für den Download, die Bereitstellung und die Aktivierung von Gateways. Sobald Sie ein Gateway bereitgestellt und aktiviert haben, können Sie anhand weiterer Anleitungen Stored Volume-, Cached Volume- und Tape Gateway-Konfigurationen einrichten. Weitere Informationen finden Sie unter Erstellen eines Tape Gateways.	19. Mai 2014
Kompatibilität mit Symantec Backup E:	Tape Gateway ist nun mit Symantec Backup Exec 2012 kompatibel. Sie können nun Symantec Backup Exec 2012 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec.	28. April 2014

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Windows Server Failover Clustering Unterstützung für den VMware ESX-Initiator Unterstützung für die Durchführung von Konfigurationsaufgaben in der lokalen Storage Gateway-Konsole	• Storage Gateway unterstützt jetzt Verbindungen zwischen mehreren Hosts und ein und demselben Volume, wenn die Hosts den Zugriff über Windows Server Failover Clustering (WSFC) koordinieren. Nicht über WSFC koordinierte Verbindungen zwischen mehreren Hosts und ein und demselben Volume werden jedoch nicht unterstützt. • Storage Gateway unterstützt jetzt die Verwaltung der Speicheranbindung direkt über den ESX-Host. Dadurch ist es nicht mehr nötig, Initiatoren im Gastbetriebssystem von VMs zu verwenden. • Storage Gateway unterstützt jetzt die Durchführung von Konfigurationsaufgaben in der lokalen Storage-Gateway-Konsole. Weitere Informationen zur Durchführung von Konfigurationsaufgaben für lokal bereitgestellte Gateways finden Sie unter Ausführen von Aufgaben in der lokalen VM-Konsole von oder Ausführen von Aufgaben in der lokalen VM-Konsole von . Weitere Informationen zur Durchführung von Konfigurationsaufgaben für Gateways, die in einer EC2-Instance bereitgestellt sind, finden Sie unter Ausführen von Aufgaben in der lokalen Amazon-EC2-Konsole oder Ausführen von Aufgaben in der lokalen Amazon-EC2-Konsole.	31. Januar 2014

Änderung	Beschreibung	Änderungsdatum
Unterstützung für virtuelle Bandbibliotheken und Einführung der API-Version 2013-06-30	Storage Gateway verbindet eine On-Premises-Software-Appliance mit cloudbasiertem Speicher, um Ihre On-Premises-IT-Umgebung in die AWS Speicherinfrastruktur zu integrieren. Neben der Option Volume Gateway (zwischengespeicherte und gespeicherte Volumes) unterstützt Storage Gateway jetzt auch Gateways des Typs Virtual Tape Library (VTL). Ein Tape Gateway lässt sich mit bis zu 10 virtuellen Bandlaufwerken konfigurieren. Jedes virtuelle Bandlaufwerk reagiert auf den SCSI-Befehlssatz, sodass Ihre vorhandenen lokalen Sicherungsanwendungen ohne Anpassungen funktionieren. Weitere Informationen finden Sie in folgenden Themen im AWS Storage Gateway -Benutzerhandbuch: • Einen Überblick über die Architektur finden Sie unter So funktioniert Tape Gateway (Architektur). • Informationen zu den ersten Schritten mit Tape Gateway finden Sie unter Erstellen eines Tape Gateways.	5. November 2013
Unterstützung für Microsoft Hyper-V	Storage Gateway unterstützt jetzt die Bereitstellung eines On-Premises-Gateways auf der Virtualisierungsplattform Microsoft Hyper-V. Auf Microsoft Hyper-V bereitgestellte Gateways verfügen über denselben Funktionsumfang wie das vorhandene On-premises-Storage Gateway. Erste Schritte für die Bereitstellung eines Gateways mit Microsoft Hyper-V finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	10. April 2013

Änderung	Beschreibung	Änderungsdatum
Unterstützung für die Bereitstellung von Gateways in Amazon EC2	Storage Gateway bietet nun die Möglichkeit, ein Gateway in Amazon Elastic Compute Cloud (Amazon EC2) bereitzustellen. Sie können eine Gateway-Instance in Amazon EC2 mit dem Storage-Gateway-AMI starten, das im AWS Marketplace verfügbar ist. Informationen zu den ersten Schritten für die Bereitstellung eines Gateways mithilfe des Storage Gateway-AMI finden Sie unter Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Tape Gateway.	15. Januar 2013

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Cached Volumes und Einführung der API-Version 2012-06-30	Ab dieser Version unterstützt Storage Gateway Cached Volumes. Cached Volumes reduzieren die Notwendigkeit für Skalierungen Ihrer lokalen Speicherinfrastruktur auf ein Minimum und gewährleisten dabei gleichzeitig, dass Ihre Anwendungen mit niedriger Latenz auf ihre aktiven Daten zugreifen können. Sie können Speicher-Volumes mit bis zu 32 TiB erstellen und sie über Ihre lokalen Anwendungsserver als iSCSI-Geräte mounten. Auf zwischengespeicherten Volumes geschriebene Daten werden in Amazon Simple Storage Service (Amazon S3) gespeichert. Auf der On-Premises-Speicherhardware wird nur ein Cache mit den vor kurzem geschriebenen und gelesenen Daten lokal gespeichert. Dank Cached Volumes können Sie Daten, bei deren Abruf höhere Latenzen akzeptabel sind, in Amazon S3 speichern, beispielsweise ältere Daten, auf die selten zugegriffen wird. Daten, auf die Zugriff mit niedriger Latenz möglich sein muss, bleiben On-Premises gespeichert. In dieser Version von Storage Gateway wird zudem eine neue API-Version eingeführt, die neben den aktuell bereits verfügbaren Operationen neue Operationen für Cached Volumes bereitstellt. Weitere Informationen zu den beiden Storage Gateway-Lösungen finden Sie unter So funktioniert Tape Gateway (Architektur). Sie können auch eine Testkonfiguration einrichten. Anweisungen finden Sie unter Erstellen eines Tape Gateways.	29. Oktober 2012

Änderung	Beschreibung	Änderungsdatum
API- und IAM-Unterstützung	In dieser Version führt Storage Gateway API-Unterstützung sowie Unterstützung für AWS Identity and Access Management(IAM) ein. • API-Unterstützung – Storage Gateway-Ressourcen lassen sich jetzt programmgesteuert konfigurieren und verwalten. Weitere Informationen zur API finden Sie unter API-Referenz für Storage Gateway im AWS Storage Gateway -Benutzerhandbuch. • IAM-Unterstützung: Mithilfe von AWS Identity and Access Management (IAM) können Sie Benutzer erstellen und den Benutzerzugriff auf Ihre Storage Gateway-Ressourcen mithilfe von IAM-Richtlinien verwalten. Beispiele für IAM-Richtlinien finden Sie unter Identity and Access Management für AWS Storage Gateway. Weitere Informationen zu IAM finden Sie auf der Detailseite zu AWS Identity and Access Management (IAM).	9. Mai 2012
Unterstützung für statische IPs	Sie können nun eine statische IP für Ihr lokales Gateway festlegen. Weitere Informationen finden Sie unter Konfigurieren Ihres Gateway-Netzwerks.	5. März 2012
Neues Handbuch	Dies ist die erste Version des AWS Storage Gateway -Benutzerhandbuchs.	24. Januar 2012

Versionshinweise für die Tape Gateway-Appliance-Software

In diesen Versionshinweisen werden die neuen und aktualisierten Funktionen, Verbesserungen und Korrekturen beschrieben, die in jeder Version der Tape Gateway enthalten sind. Jede Softwareversion wird durch ihr Veröffentlichungsdatum und eine eindeutige Versionsnummer identifiziert.

Sie können die Softwareversionsnummer eines Gateways ermitteln, indem Sie die Seite „Details“ in der Storage Gateway Gateway-Konsole überprüfen oder die DescribeGatewayInformationAPI-Aktion mit einem AWS CLI Befehl aufrufen, der dem folgenden ähnelt:

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

Die Versionsnummer wird im `SoftwareVersion` Feld der API-Antwort zurückgegeben.

> **Note**
>
> Ein Gateway meldet unter den folgenden Umständen keine Informationen zur Softwareversion:
>
> - Das Gateway ist offline.
> - Auf dem Gateway wird ältere Software ausgeführt, die keine Versionsberichterstattung unterstützt.
> - Der Gateway-Typ ist FSx File Gateway.

Weitere Informationen zu Tape , einschließlich der Änderung des standardmäßigen automatischen Wartungs- und Aktualisierungszeitplans für ein Gateway, finden Sie unter Gateway-Updates mit der AWS Storage Gateway Console verwalten.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-04-10	2.8.1	• Ein in 2.8.0 eingeführtes Problem mit der Speichern utzung wurde behoben • Sicherheitspatch-Updates

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		• Verbesserter Software-Aktualisierungsprozess • Die fehlende NTP-Komponente (Network Time Protocol) für neue Gateways wurde behoben
2024-03-06	2.8.0	• Betriebssystem-Updates für neue Gateways • Sicherheitspatch-Updates • Verbesserte Leistung für gleichzeitige Backup- und Wiederherstellungs-Workloads
2023-12-19	2.7.0	• Betriebssystem-Updates für neue Gateways
2023-12-14	2,6.6	• Es wurde ein Problem mit der relativen Positionierung auf Bändern mit mehr als 5 TiB behoben
2023-10-19	2,6.5	• Es wurden Schutzmaßnahmen gegen das Überschreiben von Bändern durch Clients nach einem Gateway-Neustart hinzugefügt