



Benutzerhandbuch für Volume Gateway

AWS Storage Gateway



API-Version 2013-06-30

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Benutzerhandbuch für Volume Gateway

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

.....	x
Was ist Volume Gateway?	1
Volume Gateway	1
Verwenden Sie Storage Gateway zum ersten Mal?	2
So funktioniert Volume Gateway	2
Volume Gateways	3
Preisgestaltung	7
Planen der Gateway-Bereitstellung	8
Erste Schritte	10
Registrieren für AWS Storage Gateway	10
AWS Regionen	11
Voraussetzungen	11
Hardware- und Speicheranforderungen	11
Netzwerk- und Firewall-Anforderungen	14
Unterstützte Hypervisoren und Host-Anforderungen	25
Unterstützte iSCSI-Initiatoren	27
Zugriff auf AWS Storage Gateway	28
Verwenden der Hardware-Appliance	29
Informationen zur Bestellung	30
Unterstützte Regionen AWS	30
Einrichten Ihrer Hardware-Appliance	30
Rackmontage Ihrer Hardware-Appliance und Anschluss an die Stromversorgung	32
Abmessungen der Hardware-Appliance	32
Konfigurieren von Netzwerkparametern	37
Aktivieren Ihrer Hardware-Appliance	40
Erstellen eines Gateways	41
Konfigurieren einer IP-Adresse für das Gateway	42
Konfigurieren Ihres Gateways	44
Entfernen eines Gateways	45
Löschen Ihrer Hardware-Appliance	45
Erstellen eines Gateways	47
Überblick – Gateway-Aktivierung	47
Einrichten eines Gateways	47
Verbinden mit AWS	47

Überprüfen und aktivieren	47
Überblick – Gateway-Konfiguration	48
Überblick – Speicherressourcen	48
Erstellen eines Volume Gateways	48
Erstellen eines Gateways	49
Erstellen eines Volumes	54
Verwenden des Volumes	58
Sichern von Volumes	69
Aktivieren eines Gateways in einer Virtual Private Cloud	74
Erstellen eines VPC-Endpunkts für Storage Gateway	75
Verwalten von Gateways	77
Verwalten Ihres Volume Gateways	77
Bearbeiten von Gateway-Informationen	79
Hinzufügen einer Volume	79
Die Größe einer Volume erweitern	80
Klonen einer Volume	80
Anzeigen von Volume-Nutzung	84
Reduzieren des für ein Volume fakturierten Speichers	85
Löschen eines Volumes	85
Verschieben Ihrer Volumes zu einem anderen Gateway	86
Erstellen eines einmaligen Snapshots	89
Bearbeiten Sie einen Snapshot-Zeitplan	90
Löschen von Snapshots	90
Grundlagen zu Status und Übergängen bei Volumes	104
Verschieben Ihrer Daten auf ein neues Gateway	116
Verschieben gespeicherter Volumes auf ein neues gespeichertes Volume Gateway	117
Verschieben zwischengespeicherter Volumes auf eine neue zwischengespeicherte virtuelle Volume-Gateway-Maschine	120
Überwachen von Storage Gateway	125
Grundlagen zu Gateway-Metriken	125
Dimensionen für Storage Gateway-Metriken	132
Überwachen des Upload-Puffers	132
Überwachen des Cache-Speichers	135
Grundlegendes zu CloudWatch Alarmen	137
Erstellen empfohlener CloudWatch Alarme	139
Erstellen eines benutzerdefinierten CloudWatch Alarms	140

Überwachen des Volume Gateways	142
Abrufen von Zustandsprotokollen zu Volume Gateways	143
Verwenden von Amazon CloudWatch Metrics	144
Messung der Leistung zwischen Ihrer Anwendung und dem Gateway	146
Messung der Leistung zwischen Ihrem Gateway und AWS	149
Grundlagen zu Volumen-Metriken	153
Warten eines Gateways	162
Herunterfahren der Gateway-VM	162
Starten und Anhalten von Volume Gateway	163
Verwalten von lokalen Festplatten	164
Bestimmen der Größe des lokalen Festplattenspeichers	164
Festlegen der Upload-Puffergröße	166
Bestimmen der Cache-Speichergröße	168
Hinzufügen von Upload-Puffer oder Cache-Speicher	168
Verwalten der Bandbreite	169
Ändern der Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole	170
Planung der Bandbreitendrosselung	171
Verwenden der AWS SDK for Java	173
Verwenden der AWS SDK for .NET	175
Verwenden der AWS Tools for Windows PowerShell	177
Verwalten von Gateway-Updates	178
Ausführen von Wartungsaufgaben in der lokalen Konsole	180
Ausführen von Aufgaben in der lokalen VM-Konsole von	180
Ausführen von Aufgaben in der lokalen EC2-Konsole	200
Zugreifen auf die lokale Konsole des Gateways	206
Konfigurieren von Networkadaptern für Ihr Gateway	212
Löschen des Gateways und Entfernen von Ressourcen	216
Löschen eines Gateways mithilfe der Storage-Gateway-Konsole	216
Entfernen von Ressourcen von einem lokal bereitgestellten Gateway	218
Entfernen von Ressourcen von einem auf einer Amazon-EC2-Instance bereitgestellten Gateway	218
Leistung	220
Optimieren der Gateway-Leistung	220
Empfohlene Konfiguration	220
Hinzufügen von Ressourcen zu Ihrem Gateway	221
Optimieren von iSCSI-Einstellungen	224

Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung	225
Verwenden von VMware High Availability mit Storage Gateway	225
Konfigurieren Ihres vSphere VMware HA-Clusters	226
Herunterladen des OVA-Image von der Storage-Gateway-Konsole	228
Bereitstellen des Gateways	228
(Optional) Hinzufügen von Überschreibungsoptionen für andere VMs auf Ihrem Cluster	229
Aktivieren des Gateways	230
Testen der Konfiguration von VMware High Availability	230
Sicherheit	232
Datenschutz	233
Datenverschlüsselung	234
Konfigurieren der CHAP-Authentifizierung	236
Identitäts- und Zugriffsverwaltung	238
Zielgruppe	238
Authentifizierung mit Identitäten	239
Verwalten des Zugriffs mit Richtlinien	243
Funktionsweise von AWS Storage Gateway mit IAM	246
Beispiele für identitätsbasierte Richtlinien	253
Fehlerbehebung	256
Protokollieren und Überwachen	258
Storage Gateway-Informationen in CloudTrail	259
Informationen zu Storage-Gateway-Protokolldateieinträgen	260
Compliance-Validierung	262
Ausfallsicherheit	263
Sicherheit der Infrastruktur	263
AWS Bewährte Methoden für die Sicherheit	264
Fehlerbehebung bei Gateway-Problemen	265
Fehlerbehebung bei lokalen Gateway-Problemen	265
Aktivieren von AWS Support zur Unterstützung bei der Fehlerbehebung Ihres Gateways	270
Fehlerbehebung bei Problemen mit der Einrichtung von Microsoft Hyper-V	272
Fehlerbehebung bei Problemen mit Amazon-EC2-Gateway	276
Die Aktivierung des Gateways ist nach einigen Momenten nicht erfolgt.	277
EC2-Gateway-Instance in der Instance-Liste nicht gefunden	277
Ein Amazon-EBS-Volume kann nicht an die EC2-Gateway-Instance angefügt werden	278
Sie können keinen Initiator an ein Volume-Ziel auf dem EC2-Gateway anfügen	278

Beim Hinzufügen von Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind	278
So entfernen Sie einen als Upload-Pufferspeicher zugewiesenen Datenträger, um die Größe des Upload-Pufferspeichers zu reduzieren	278
Durchsatz zum oder vom EC2-Gateway sinkt auf Null	279
Aktivieren von AWS Support zur Unterstützung bei der Fehlerbehebung des Gateways	279
Verbindung mit Ihrem Amazon-EC2-Gateway über die serielle Konsole	281
Fehlerbehebung bei Hardware-Appliance-Problemen	281
So ermitteln Sie die Service-IP-Adresse	282
So führen Sie eine Zurücksetzung auf die Werkseinstellungen durch	282
So führen Sie einen Remote-Neustart durch	282
So erhalten Sie Dell iDRAC-Support	282
So finden Sie die Seriennummer der Hardware-Appliance	282
So erhalten Sie Hardware-Appliance-Support	283
Fehlerbehebung bei Volume-Problemen	284
Die Konsole behauptet, dass Ihre Volume nicht konfiguriert ist	284
Die Konsole gibt an, dass Ihre Volume verloren ist	285
Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen	285
Die Konsole gibt an, das Ihre Volume WEITERGABE Status hat	286
Sie möchten Volume-Integrität überprüfen und möglicher Fehler beheben	287
Ihre Volume-iSCSI-Target erscheint nicht in Windows Disk Management Konsole	287
Sie möchten den iSCSI-Volumen-Zielnamen ändern	287
Ihr geplanter Volume Snapshot taucht nicht auf	287
Sie müssen eine Festplatte entfernen oder ersetzen, die ausgefallen ist	287
Durchsatz von Ihrer Anwendung zu einem Volume ist auf Null abgefallen	288
In einer Cache-Festplatte in Ihrem Gateway tritt ein Fehler auf	289
Ein Volume Snapshot hat einen PENDING Status länger als erwartet	289
High Availability-Zustandsbenachrichtigungen	290
Beheben von Problemen mit Hochverfügbarkeit	290
Zustandsbenachrichtigungen	290
Metriken	292
Wiederherstellen Ihrer Daten: Bewährte Methoden	292
Wiederherstellung nach dem unerwarteten Herunterfahren einer VM	293
Wiederherstellen von Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM	293
Wiederherstellung von Daten von einem nicht wiederherstellbaren Volume	294
Wiederherstellen von Daten von einer fehlerhaften Festplatte	295

Wiederherstellen von Daten von einem beschädigten Datensystem	295
Wiederherstellen von Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann	296
Weitere Ressourcen	298
Host-Setup	298
Konfiguration von VMware für Storage Gateway	298
Synchronisieren der Gateway-VM-Zeit	306
Bereitstellen eines Amazon-EC2-Hosts für Volume Gateway	308
Bereitstellen von Amazon EC2 mit Standardeinstellungen	313
Ändern von Amazon EC2-Instance-Metadatenoptionen	315
Volume Gateway	316
Entfernen von Datenträgern aus dem Gateway	316
EBS-Volumes für EC2-Gateways	320
Den Aktivierungsschlüssel erhalten	321
Linux (curl)	322
Linux (bash/zsh)	323
Microsoft Windows PowerShell	324
Verwenden der lokalen Konsole	324
Verbinden von iSCSI-Initiatoren	325
Verbinden eines Windows-Clients mit Volumes	326
Verbinden von Volumes oder VTL-Geräten mit einem Linux-Client	331
Anpassen von iSCSI-Einstellungen	333
Konfigurieren der CHAP-Authentifizierung	342
Verwenden von AWS Direct Connect mit Storage Gateway	351
Port-Anforderungen	352
Herstellen einer Verbindung mit einem Gateway	359
Abrufen einer IP-Adresse von einem Amazon EC2-Host	360
Grundlegendes zu Ressourcen und Ressourcen-IDs	361
Arbeiten mit Ressourcen-IDs	362
Markieren Ihrer Ressourcen	362
Arbeiten mit Tags	363
Open-Source-Komponenten	364
Storage-Gateway-Kontingente	365
Kontingente für Volumes	365
Empfohlene Kapazität für die lokalen Datenträger des Gateways	366
API-Referenz	368

Erforderliche Abfrage-Header	368
Signieren von Anforderungen	371
Signatur-Berechnungsbeispiel	372
Fehlermeldungen	373
Ausnahmen	374
Operationsfehlercodes	376
Fehlermeldungen	396
Operationen	398
Dokumentverlauf	399
Frühere Aktualisierungen	417
Versionshinweise	438

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 Tape Gateway-Dokumentation wurde nach [Was ist Tape 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 Volume 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 zwischengespeicherte) Speicherlösungen und bandbasierte Speicherlösungen.

Themen

- [Volume Gateway](#)
- [Verwenden Sie Storage Gateway zum ersten Mal?](#)
- [So funktioniert Volume Gateway \(Architektur\)](#)
- [Storage Gateway – Preisgestaltung](#)
- [Planen Ihrer Storage-Gateway-Bereitstellung](#)

Volume Gateway

Volume Gateway – Ein Volume Gateway bietet Cloud-gestützte Speicher-Volumes, die Sie als Internet Small Computer System Interface (iSCSI)-Geräte über Ihre lokalen Anwendungsserver mounten können.

Sie können ein Volume Gateway entweder lokal 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.

Das Gateway unterstützt die folgenden Volume-Konfigurationen:

- **Zwischengespeicherte Volumes** – Sie speichern Ihre Daten in Amazon Simple Storage Service (Amazon S3) und halten lokal eine Kopie von Datenteilmengen vor, auf die häufig zugegriffen wird. Zwischengespeicherte Volumes bieten substanzielle Kosteneinsparungen bei primärem Speicher und minimieren den Anpassungsbedarf für lokalen Speicher. Sie behalten auch einen schnellen Zugriff auf Daten, auf die häufig zugegriffen wird.

- **Gespeicherte Volumes** – Wenn Sie schnellen Zugriff auf alle Ihre Daten benötigen, können Sie Ihr lokales Gateway zunächst so konfigurieren, dass alle Ihre Daten lokal gespeichert werden. Sichern Sie dann asynchron point-in-time Snapshots dieser Daten in Amazon S3. Diese Konfiguration ermöglicht dauerhafte und kostengünstige externe Sicherungen, die Sie in einem lokalen Rechenzentrum oder in Amazon Elastic Compute Cloud (Amazon EC2) wiederherstellen können. Wenn Sie beispielsweise für eine Notfallwiederherstellung Ersatzkapazität benötigen, können Sie die Sicherungen auf Amazon EC2 wiederherstellen.

Dokumentation: Die Dokumentation für Volume Gateway finden Sie unter [Erstellen eines Volume 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:

- Unter [Erstellen eines Volume Gateways](#) wird beschrieben, wie Sie ein Volume Gateway erstellen und verwenden. Hier erfahren Sie, wie Sie Speicher-Volumes anlegen und Daten auf den Volumes sichern.
- 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 Volume Gateway (Architektur)

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

Volume Gateways

Für Volume Gateways können Sie entweder zwischengespeicherte Volumes oder gespeicherte Volumes verwenden.

Themen

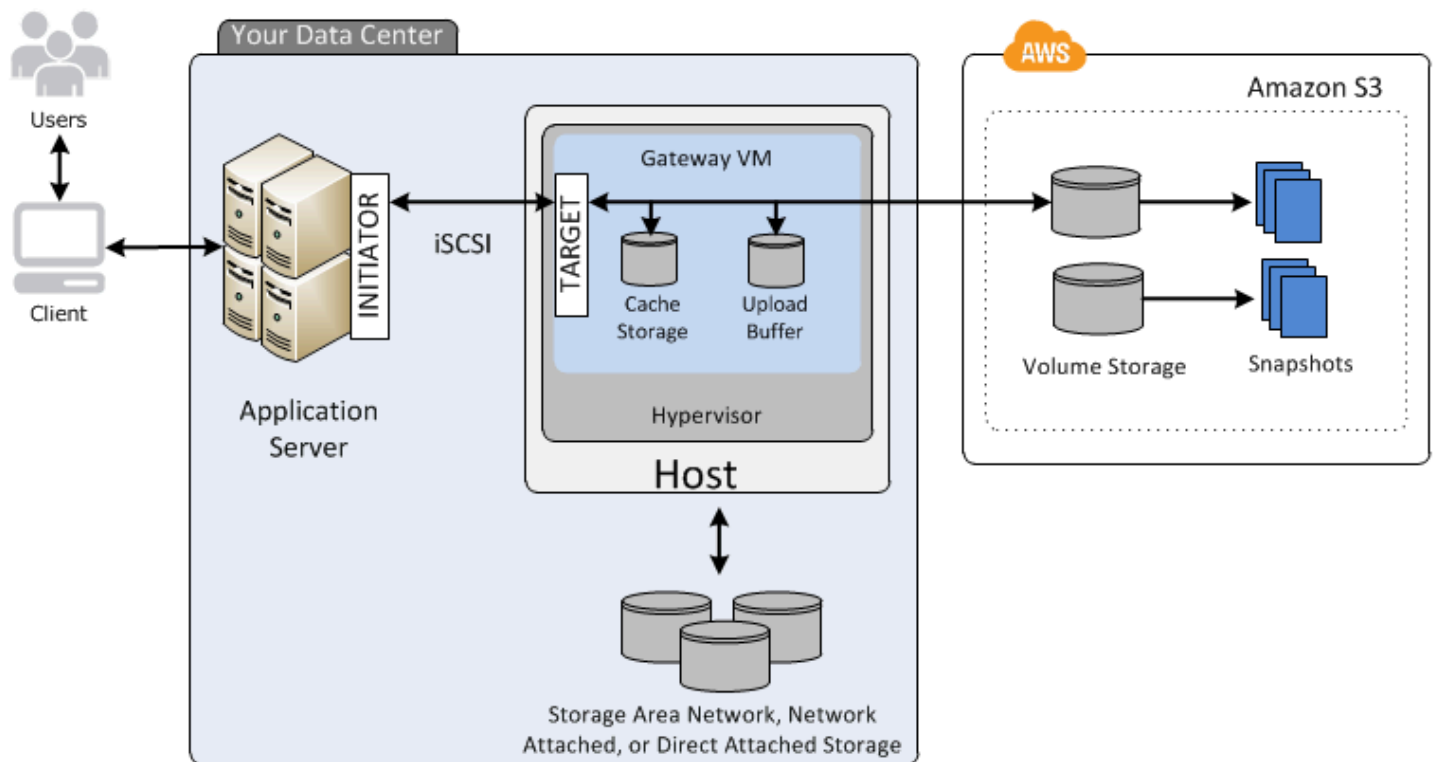
- [Architektur mit zwischengespeicherten Volumes](#)
- [Architektur mit Stored Volumes](#)

Architektur mit zwischengespeicherten Volumes

Mit zwischengespeicherten Volumes können Sie Amazon S3 als primären Datenspeicher verwenden und gleichzeitig regelmäßig verwendete Daten lokal im Storage Gateway aufbewahren. Zwischengespeicherte Volumes minimieren die erforderliche Skalierung Ihrer On-Premises-Speicherinfrastruktur, während Ihre Anwendungen weiterhin mit niedriger Latenz auf häufig aufgerufene Daten zugreifen können. Sie können Speicher-Volumes mit bis zu 32 TB erstellen und sie über Ihre lokalen Anwendungsserver als iSCSI-Geräte anfügen. Ihr Gateway speichert Daten, die Sie auf diese Volumes schreiben, in Amazon S3 und behält kürzlich gelesenen Daten im Cache des lokalen Storage Gateways und im Upload-Pufferspeicher.

Die Größe von zwischengespeicherten Volumes liegt im Bereich von 1 GB bis 32 TB. Der Wert muss auf den nächsten GB-Wert gerundet werden. Jedes für zwischengespeicherte Volumes konfigurierte Gateway kann bis zu 32 Volumes mit einem maximalen Speicher-Volume von insgesamt 1.024 TB (1 PB) unterstützen.

In der Lösung mit zwischengespeicherten Volumes speichert Storage Gateway alle lokalen Anwendungsdaten in einem Speicher-Volume in Amazon S3. In dieser Abbildung finden Sie eine Übersicht über die Bereitstellung von zwischengespeicherten Volumes.



Nachdem Sie die Storage Gateway-Software-Appliance – die VM – auf einem Host in Ihrem Rechenzentrum installiert und aktiviert haben, verwenden Sie die , AWS Management Console um Speicher-Volumes bereitzustellen, die von Amazon S3 unterstützt werden. Sie können Speicher-Volumes auch programmgesteuert mithilfe der Storage Gateway-API oder der AWS SDK-Bibliotheken bereitstellen. Anschließend können Sie diese Speicher-Volumes auf lokalen Anwendungsservern als iSCSI-Geräte mounten.

Sie können auch Datenträger lokal zur VM zuweisen. Diese lokalen Datenträger werden für die folgenden Zwecke verwendet:

- Datenträger zur Verwendung durch das Gateway als Cache-Speicher – Wenn Ihre Anwendungen Daten auf die Speicher-Volumes in schreiben AWS, speichert das Gateway die Daten zunächst auf den On-Premises-Festplatten, die für die Cache-Speicherung verwendet werden. Danach werden die Daten vom Gateway in Amazon S3 hochgeladen. Der Cache-Speicher fungiert wie der dauerhafte On-Premises-Speicher für Daten, die vom Upload-Puffer aus in Amazon S3 hochgeladen werden sollen.

Dank der Cache-Speicherung kann das Gateway auch die Daten, auf die die Anwendung zuletzt zugegriffen hat, lokal speichern, sodass ein schneller Zugriff möglich ist. Wenn die Anwendung

Daten anfordert, überprüft das Gateway zunächst den Cache-Speicher auf Daten, bevor Amazon S3 überprüft wird.

Verwenden Sie die folgenden Richtlinien, um zu bestimmen, wie viel Speicherplatz für die Cache-Speicherung zugewiesen werden soll. Im Allgemeinen sollten Sie mindestens 20 Prozent der Größe des vorhandenen Dateispeichers als Cache-Speicher zuweisen. Der Cache-Speicher sollte ebenfalls größer als der Upload-Puffer sein. Mithilfe dieser Richtlinie können Sie sicherstellen, dass der Cache-Speicher groß genug ist, um alle Daten, die noch nicht in Amazon S3 hochgeladen wurden, dauerhaft im Upload-Puffer zu speichern.

- Datenträger, die vom Gateway als Upload-Puffer verwendet werden – Als Vorbereitung auf das Hochladen in Amazon S3 speichert das Gateway auch eingehende Daten in einem Staging-Bereich, der als Upload-Puffer bezeichnet wird. Ihr Gateway lädt diese Pufferdaten über eine verschlüsselte SSL-Verbindung (Secure Sockets Layer) zu hoch AWS, wo sie verschlüsselt in Amazon S3 gespeichert werden.

Sie können inkrementelle Sicherungen, sogenannte Snapshots Ihrer Speicher-Volumes, in Amazon S3 durchführen. Diese point-in-time Snapshots werden auch in Amazon S3 als Amazon-EBS-Snapshots gespeichert. Für jeden neuen Snapshot werden nur die Daten gespeichert, die seit dem letzten Snapshot geändert wurden. Wenn der Snapshot erstellt wurde, lädt das Gateway die Änderungen bis zum Snapshot-Punkt hoch und erstellt dann den neuen Snapshot mithilfe von Amazon EBS. Sie können Snapshots nach einem Zeitplan oder zu einem bestimmten Zeitpunkt starten. Ein einzelnes Volume unterstützt das schnelle Aneinanderreihen mehrerer Snapshots in einer Warteschlange, aber jeder Snapshot muss fertig erstellt sein, bevor der nächste erstellt werden kann. Wenn Sie einen Snapshot löschen, werden nur die Daten entfernt, die nicht für andere Snapshots benötigt werden. Weitere Informationen zu Amazon-EBS-Snapshots finden Sie unter [Amazon-EBS-Snapshots](#).

Wenn Sie eine Sicherung Ihrer Daten wiederherstellen müssen, können Sie einen Amazon-EBS-Snapshot auf einem Gateway-Speicher-Volume wiederherstellen. Alternativ können Sie für Snapshots mit einer Größe von bis zu 16 TiB den Snapshot als Ausgangspunkt für ein neues Amazon-EBS-Volume verwenden. Sie können dann das neue Amazon-EBS-Volume an eine Amazon-EC2-Instance anfügen.

Alle Gateway- und Snapshot-Daten für zwischengespeicherte Volumes werden in Amazon S3 gespeichert und mit serverseitiger Verschlüsselung (SSE) verschlüsselt. Sie können jedoch nicht über die Amazon S3 API oder mit anderen Tools wie der Amazon-S3-Managementkonsole auf diese Daten zugreifen.

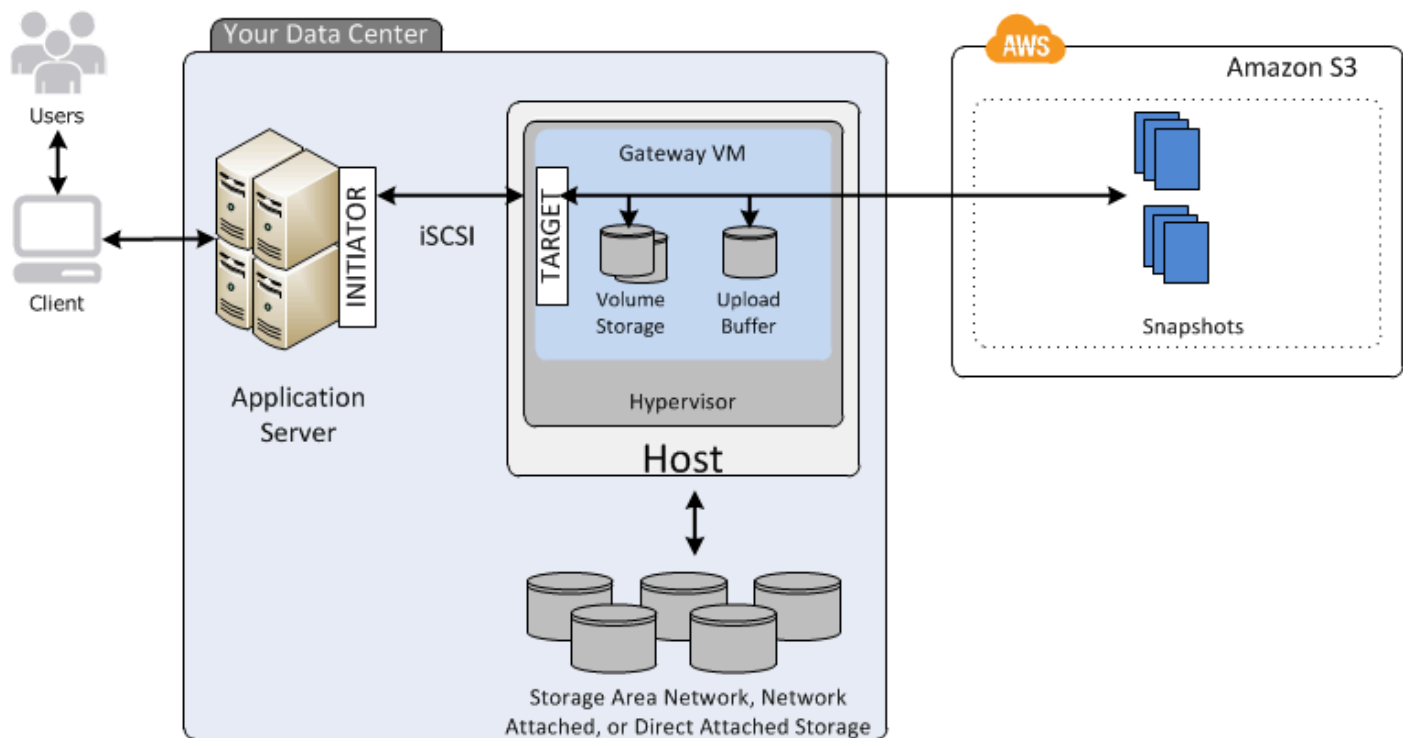
Architektur mit Stored Volumes

Durch die Verwendung von gespeicherten Volumes können Sie Ihre primären Daten lokal speichern und diese Daten gleichzeitig asynchron in sichern AWS. Gespeicherte Volumes bieten Ihren On-Premises-Anwendungen Zugriff mit niedriger Latenz auf ihre gesamten Datensätze. Zugleich ermöglichen sie zuverlässige, externe Sicherungen. Sie können Speicher-Volumes erstellen und diese als iSCSI-Geräte von lokalen Anwendungsservern mounten. Daten, die auf die Stored Volumes geschrieben werden, werden auf lokaler Speicherhardware gespeichert. Diese Daten werden asynchron als Amazon-Elastic-Block-Store (Amazon-EBS)-Snapshots auf Amazon S3 gesichert.

Die Größe von Stored Volumes liegt im Bereich von 1 GB bis 16 TB. Der Wert muss auf den nächsten GB-Wert gerundet werden. Jedes für Stored Volumes konfigurierte Gateway kann bis zu 32 Volumes mit einem maximalen Volume-Speicher von insgesamt 512 TB (0,5 PB) unterstützen.

Mit Stored Volumes bleibt der Volume-Speicher lokal im Rechenzentrum. Das heißt, dass Sie alle Anwendungsdaten auf der lokalen Speicherhardware speichern. Anschließend lädt das Gateway Daten mithilfe von Funktionen für die Datensicherheit in Amazon Web Services Cloud hoch, um eine kostengünstige Datensicherung und schnelle Notfallwiederherstellung sicherzustellen. Diese Lösung ist ideal, wenn Sie Daten lokal speichern möchten, weil Sie Zugriff mit geringer Latenz auf alle Ihre Daten benötigen, und wenn Sie Sicherungen in AWS durchführen möchten.

In dieser Abbildung finden Sie eine Übersicht über die Bereitstellung von Stored Volumes.



Nachdem Sie die Software-Appliance für Storage Gateway – die VM – auf einem Host in Ihrem Rechenzentrum installiert und aktiviert haben, können Sie Gateway-Speicher-Volumes erstellen. Sie können sie Direct Attached Storage (DAS)- oder Storage Area Network (SAN)-Festplatten zuweisen. Dabei können sowohl mit einem neuen Datenträger beginnen oder Datenträger verwenden, auf denen bereits Daten gespeichert sind. Sie können diese Speicher-Volumes auf lokalen Anwendungsservern als iSCSI-Geräte mounten. Wenn Ihre lokalen Anwendungen Daten auf ein Gateway-Speicher-Volume schreiben oder aus dem Speicher-Volume des Gateways lesen, werden diese Daten auf den den Volumes zugeordneten Datenträgern gespeichert und abgerufen.

Als Vorbereitung auf das Hochladen in Amazon S3 speichert das Gateway auch eingehende Daten in einem Staging-Bereich, der als Upload-Puffer bezeichnet wird. Als Arbeitsspeicher können Sie lokale DAS- oder SAN-Datenträger verwenden. Ihr Gateway lädt Daten aus dem Upload-Puffer über eine verschlüsselte Secure Sockets Layer (SSL)-Verbindung in den Storage-Gateway-Service hoch, der in der Amazon Web Services Cloud ausgeführt wird. Anschließend speichert der Service die verschlüsselten Daten in Amazon S3.

Sie können inkrementelle Sicherungen, sogenannte Snapshots, der Speicher-Volumes durchführen. Das Gateway speichert diese Snapshots in Amazon S3 als Amazon-EBS-Snapshots. Für jeden neuen Snapshot werden nur die Daten gespeichert, die seit dem letzten Snapshot geändert wurden. Wenn der Snapshot erstellt wurde, lädt das Gateway die Änderungen bis zum Snapshot-Punkt hoch und erstellt dann den neuen Snapshot mithilfe von Amazon EBS. Sie können Snapshots nach einem Zeitplan oder zu einem bestimmten Zeitpunkt starten. Ein einzelnes Volume unterstützt das schnelle Aneinanderreihen mehrerer Snapshots in einer Warteschlange, aber jeder Snapshot muss fertig erstellt sein, bevor der nächste erstellt werden kann. Wenn Sie einen Snapshot löschen, werden nur die Daten entfernt, die nicht für einen anderen Snapshot benötigt werden.

Wenn Sie eine Sicherung Ihrer Daten wiederherstellen müssen, können Sie einen Amazon-EBS-Snapshot auf einem lokalen Gateway-Speicher-Volume wiederherstellen. Außerdem können Sie den Snapshot als Ausgangspunkt für ein neues Amazon-EBS-Volume verwenden, das Sie anschließend an eine Amazon-EC2-Instance anfügen können.

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:

- Volume Gateway – mithilfe von Volume Gateways können Sie Speicher-Volumes in der Amazon Web Services Cloud erstellen. Ihre lokalen Anwendungen können darauf als Internet Small Computer System Interface (iSCSI)-Ziele zugreifen. Es gibt zwei Optionen: zwischengespeicherte Volumes (Cached Volumes) und gespeicherte Volumes (Stored Volumes).
- Bei zwischengespeicherten Volumes speichern Sie Volume-Daten in , wobei ein kleiner Teil der Daten AWS, auf die zuletzt zugegriffen wurde, On-Premises im Cache vorhanden ist. Dieser Ansatz ermöglicht einen schnellen Zugriff auf Daten, auf die oft zugegriffen wird. Es bietet auch nahtlosen Zugriff auf Ihren gesamten Datensatz, der in gespeichert ist AWS. Unter Verwendung zwischengespeicherter Volumes können Sie Ihre Speicherressourcen skalieren, ohne zusätzliche Hardware bereitstellen zu müssen.
- Bei gespeicherten Volumes speichern Sie den gesamten Satz von Volume-Daten On-Premises und regelmäßige point-in-time Backups (Snapshots) in AWS. Bei diesem Modell ist Ihr On-Premises-Speicher primär und bietet Zugriff mit niedriger Latenz auf Ihren gesamten Datensatz. AWS Speicher ist das Backup, das Sie im Notfall in Ihrem Rechenzentrum wiederherstellen können.

Sowohl für zwischengespeicherte als auch für gespeicherte Volumes können Sie point-in-time Snapshots Ihrer Volume Gateway-Volumes in Form von Amazon EBS-Snapshots erstellen. Außerdem können Sie einen Snapshot als Ausgangspunkt für ein neues Amazon-EBS-Volume verwenden, das Sie an eine Amazon-EC2-Instance anfügen können. Mit diesem Ansatz können Sie Daten aus Ihren lokalen Anwendungen für Ihre Anwendungen bereitstellen, die auf Amazon EC2 ausgeführt werden, wenn Sie zusätzliche On-Demand-Rechenkapazität für die Datenverarbeitung oder Ersatzkapazität für die Notfallwiederherstellung benötigen. Auf diese Weise können Sie platzsparende versionierte Kopien Ihrer Volumes für Datenschutz, Wiederherstellung, Migration und verschiedene andere Datenübertragungsanforderungen erstellen.

Informationen zum Erstellen eines Volumes auf der Grundlage eines Amazon-EBS-Snapshots finden Sie unter [Erstellen eines Volumes](#).

Einen Überblick über die Architektur von Volume Gateways finden Sie unter [Architektur mit zwischengespeicherten Volumes](#) und [Architektur mit gespeicherten Volumes](#).

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:

- 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](#).

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](#)
- [AWS Regionen](#)
- [Voraussetzungen](#)
- [Zugriff auf AWS Storage Gateway](#)

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](#)

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 Volume 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 Volume 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
Gateway für zwischengespeicherte Volumes	150 GiB	64 TiB	150 GiB	2 TiB	—
Gateway für gespeicherte Volumes	—	—	150 GiB	2 TiB	1 oder mehr für gespeicherte Volumes oder Volumes

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-Teilmenge 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](#)
- [Netzwerk- und Firewall-Anforderungen für das Storage-Gateway-Hardwaregerät](#)
- [Zulassen des AWS Storage Gateway Zugriffs über Firewalls und Router](#)
- [Konfigurieren von Sicherheitsgruppen für eine Amazon-EC2-Gateway-Instance](#)

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

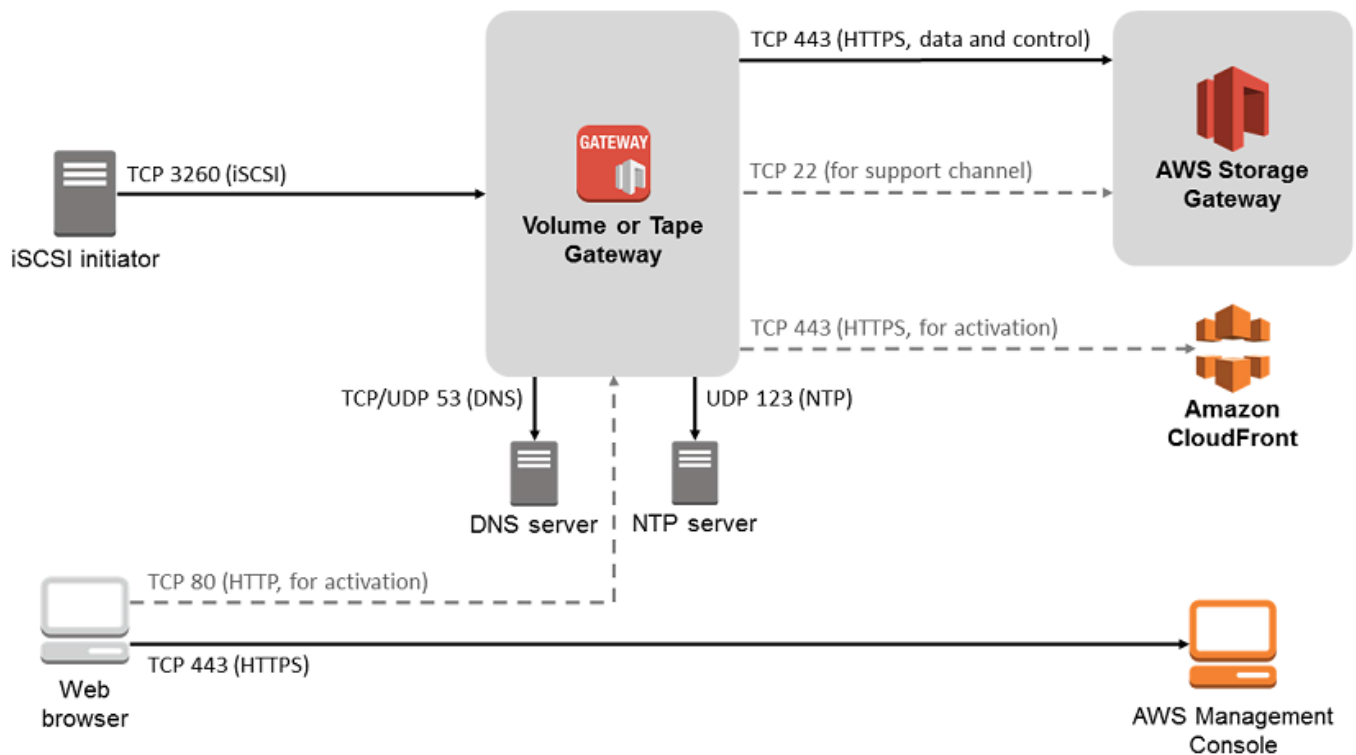
Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
			Verbindung zur - AWS Managementkonsole herstellen.		<p>des Storage-Gateway-Aktivierungsschlüssels. Port 80 wird nur während der Aktivierung einer Storage Gateway-Appliance verwendet.</p> <p>Für Storage Gateway ist es nicht erforderlich, dass Port 80 öffentlich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

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 Fehlerbehebung ist dies jedoch erforderlich.
UDP	123 (NTP)	Ausgehend	NTP-Client	NTP-Server	Verwendet von lokalen Systemen zur Synchronisierung der VM-Zeit mit der Host-Zeit.

Ports für Volume Gateway und Tape Gateway

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



Neben den allgemeinen Ports benötigt ein Volume 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 verfügbaren 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

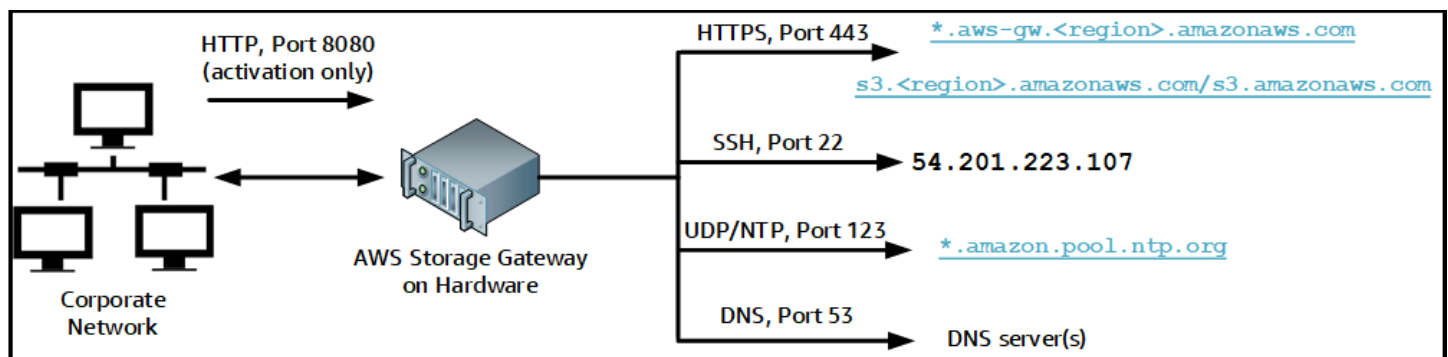
Jedes Storage-Gateway-Hardwaregerät benötigt die folgenden Netzwerkdienste:

- 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.

Es gibt fünf physische Netzwerkports am Ende des Dell PowerEdge R640-Servers. 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)

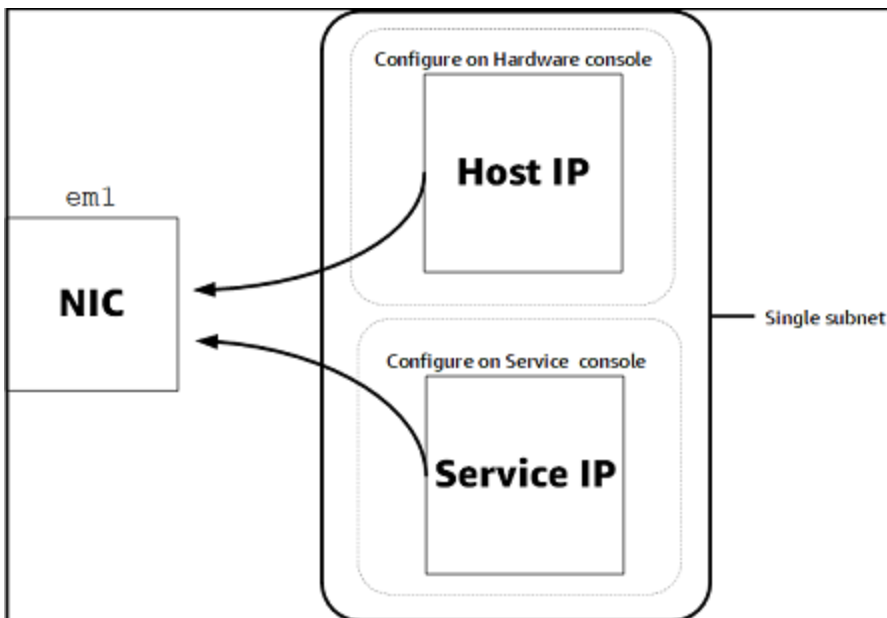
Eine Hardware-Appliance erfordert die folgenden Netzwerk- und Firewall-Einstellungen, um richtig zu funktionieren:

- 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-Endpoint durch die richtige Regionszeichenfolge.

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

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

Die folgenden Service-Endpoints 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-Endpoint ist für API-Aufrufe erforderlich.

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

Das folgende Beispiel ist ein Gateway-Service-Endpoint in der Region „USA West (Oregon)“ (us-west-2).

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

Der Amazon-S3-Service-Endpoint unten wird ausschließlich von File Gateways genutzt. Ein File Gateway benötigt diesen Endpoint, 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-Endpoint 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 Volume 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 Volume Gateway für zwischengespeicherte oder gespeicherte Volumes bereitstellen, können Sie iSCSI-Speicher-Volumes auf Ihrem Gateway erstellen.

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
- VMware 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).

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 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](#)
- [Unterstützte Regionen AWS](#)
- [Einrichten Ihrer Hardware-Appliance](#)
- [Rackmontage Ihrer Hardware-Appliance und Anschluss an die Stromversorgung](#)
- [Konfigurieren von Netzwerkparametern](#)
- [Aktivieren Ihrer Hardware-Appliance](#)
- [Erstellen eines Gateways](#)
- [Konfigurieren einer IP-Adresse für das Gateway](#)
- [Konfigurieren Ihres Gateways](#)
- [Entfernen eines Gateways von einer Hardware-Appliance](#)
- [Löschen Ihrer Hardware-Appliance](#)

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 Netzkabel 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

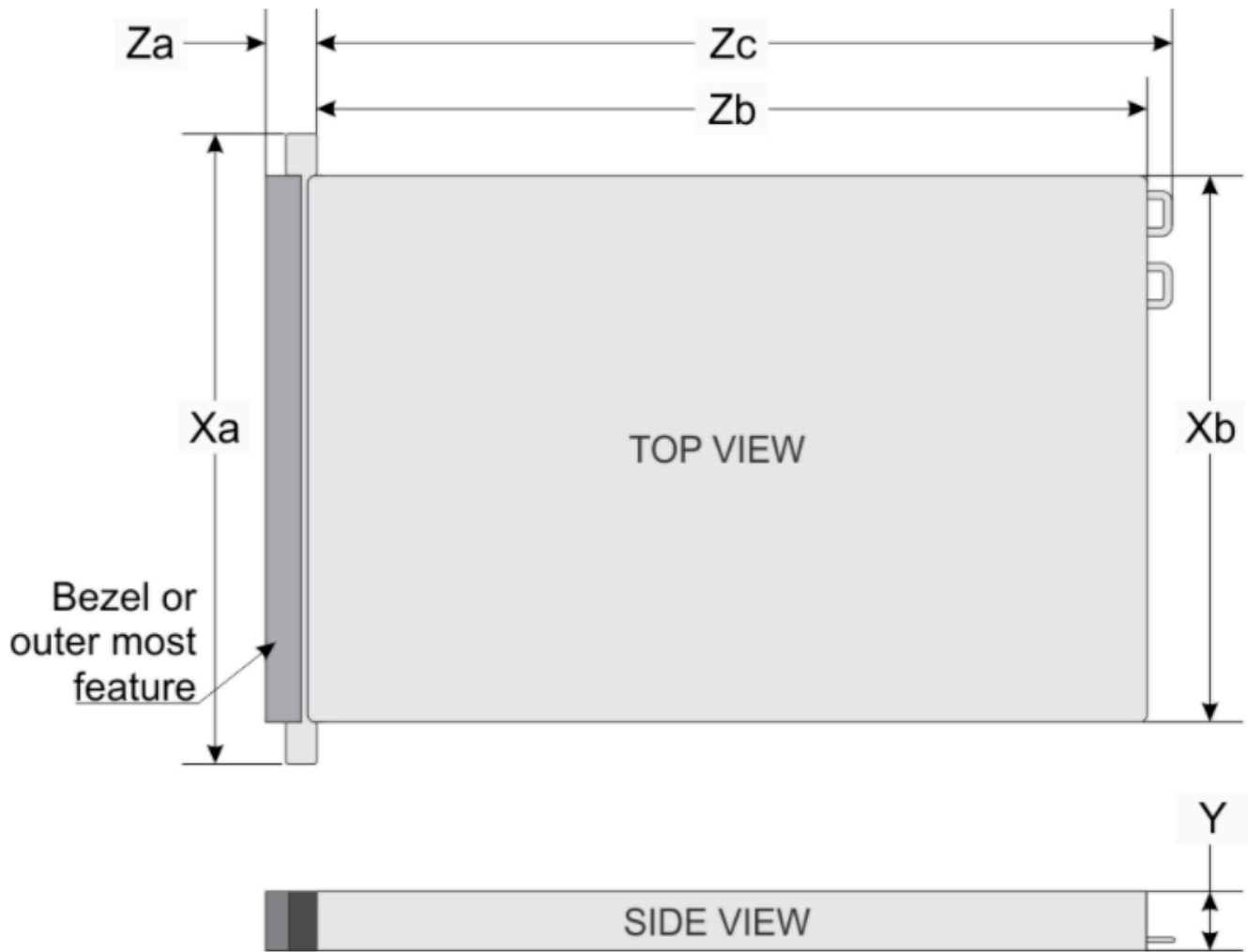
Folgen Sie nach dem Erhalt Ihrer Storage Gateway-Hardware-Appliance den im Lieferumfang enthaltenen Anleitungen für das Mounten des Servers im Rack. Bei Ihrer Appliance handelt es sich um einen 1U-Server, der in ein 19-Zoll-Rack nach dem International Electrotechnical Commission (IEC)-Branchenstandard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

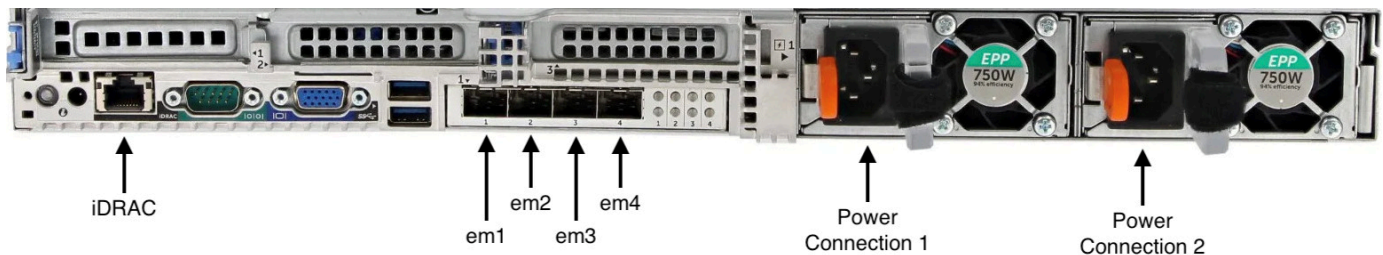
So schließen Sie die Hardware-Appliance an die Stromversorgung an

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.

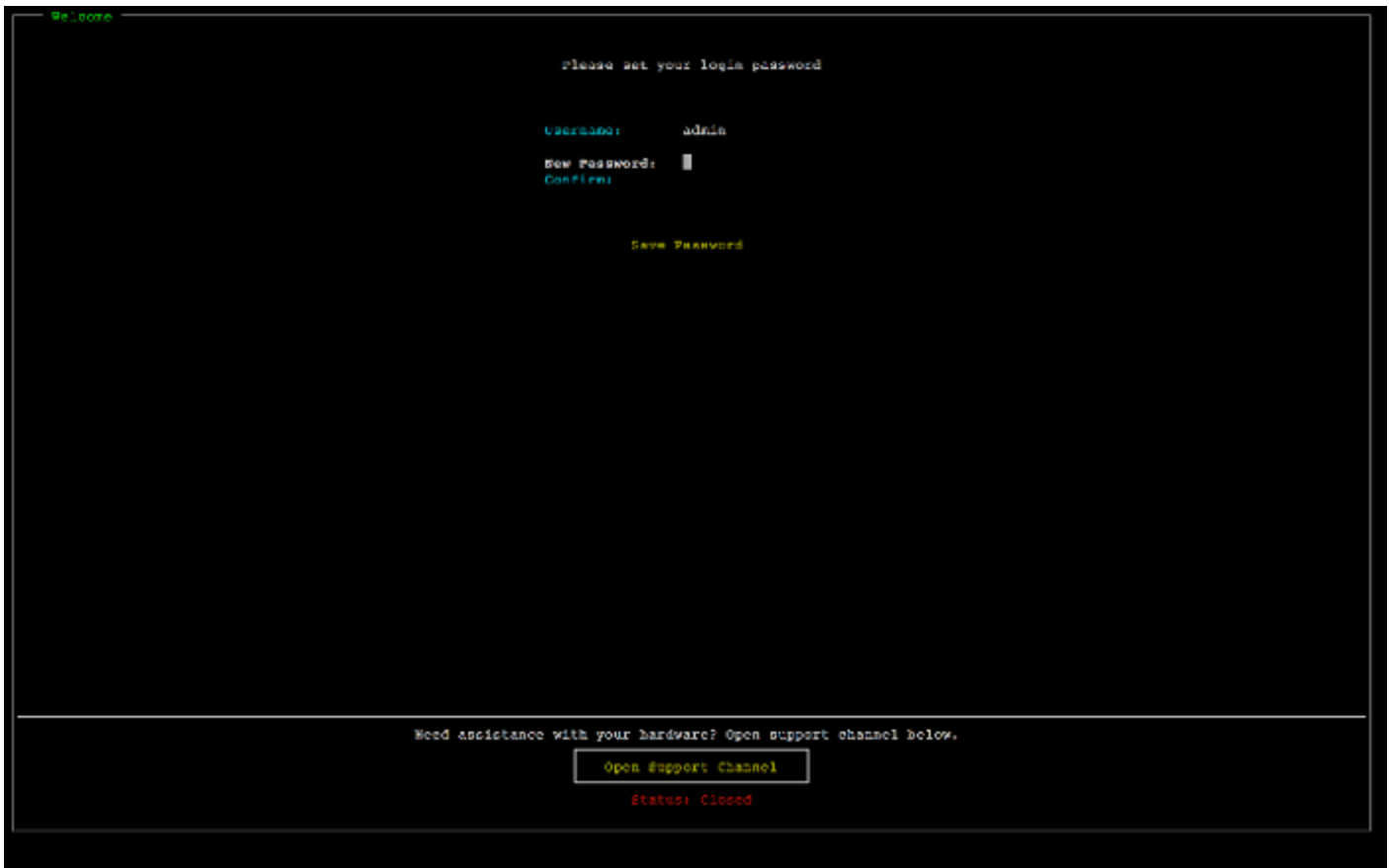
Nach dem Starten des Servers wird die Hardwarekonsole auf dem Monitor angezeigt. Die Hardwarekonsole bietet eine für spezifische Benutzeroberfläche AWS , mit der Sie anfängliche Netzwerkparameter konfigurieren können. Sie konfigurieren diese Parameter, um die Appliance mit AWS zu verbinden und einen Supportkanal zu öffnen, um eine Problembeseitigung 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 Bildschirm 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 Porteeinstellungen.

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 Hardwareseite 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 unterstützen 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.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

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.

```
AWS Storage Gateway Network Configuration
1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: View DNS Configuration
7: View Routes

Press "x" to exit

Enter command: _
```

Seite „Netzwerkconfiguration“ 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 `Ctrl+]` (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 Volume 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 Bestätigungsdiaologfeld 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 Volume 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

eingrichtet 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 Volume Gateways

In diesem Abschnitt finden Sie Anweisungen zum Erstellen und Nutzen eines Volume Gateways.

Themen

- [Erstellen eines Gateways](#)
- [Erstellen eines Volumes](#)
- [Verwenden des Volumes](#)
- [Sichern von Volumes](#)

Erstellen eines Gateways

In diesem Abschnitt finden Sie Anweisungen zum Herunterladen, Bereitstellen und Aktivieren eines Volume Gateways.

Themen

- [Einrichten eines Volume Gateways](#)
- [Verbinden Ihres Tape Gateways mit AWS](#)
- [Überprüfen von Einstellungen und Aktivieren Ihres Volume Gateways](#)
- [Konfigurieren Ihres Volume Gateways](#)

Einrichten eines Volume Gateways

Einrichten eines neuen Volume Gateways

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 Volume Gateway und dann den Volume-Typ aus, den Ihr Gateway verwenden soll. Sie können aus den folgenden Optionen auswählen:
 - Zwischengespeicherte Volumes – Speichert Ihre Primärdaten in Amazon S3 und behält häufig aufgerufene Daten lokal im Cache für einen schnelleren Zugriff.
 - Gespeicherte Volumes – Speichert alle Ihre Daten lokal und sichert sie gleichzeitig asynchron auf Amazon S3. Gateways, die diesen Volume-Typ verwenden, können nicht auf Amazon EC2 bereitgestellt werden.
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-Konsole, 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 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 Volume Gateways mit AWS](#).

Verbinden Ihres Tape Gateways mit AWS

So verbinden Sie ein neues Volume Gateway mit AWS

1. Führen Sie das unter [Einrichten eines Volume-Gateways](#) beschriebene Verfahren aus, falls Sie dies noch nicht getan haben. 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 sich Ihr Gateway mit verbinden soll AWS, müssen Sie das Gateway aktivieren. Anweisungen finden Sie unter [Überprüfen von Einstellungen und Aktivieren Ihres Volume Gateways](#).

Überprüfen von Einstellungen und Aktivieren Ihres Volume Gateways

So aktivieren Sie ein neues Volume Gateway

1. Führen Sie die in den folgenden Themen beschriebenen Verfahren durch, falls Sie dies noch nicht getan haben:
 - [Einrichten eines Volume Gateways](#)
 - [Verbinden Ihres Volume Gateways 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 erstellt 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 Volume Gateways](#).

Konfigurieren Ihres Volume Gateways


So führen Sie die Erstkonfiguration auf einem neuen Volume Gateway durch

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

- [Einrichten eines Volume Gateways](#)
- [Verbinden Ihres Volume Gateways mit AWS](#)
- [Überprüfen von Einstellungen und Aktivieren Ihres Volume 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 deaktivieren
 - `cloudwatch:EnableAlarmActions` – Alarmaktionen aktivieren
 - `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 ein Volume erstellen, damit es verwendet werden kann. Detaillierte Anweisungen finden Sie unter [Erstellen eines Volumes](#).

Erstellen eines Volumes

Zuvor haben Sie lokale Festplatten zugewiesen und dem VM-Cache-Speicher und Upload-Puffer hinzugefügt. Jetzt erstellen Sie ein Speicher-Volume, in dem Ihre Anwendungen Daten lesen und schreiben. Das Gateway verwaltet die Volume-Daten, auf die zuletzt zugegriffen wurde, lokal im Cache-Speicher und überträgt Daten asynchron an Amazon S3. Für gespeicherte Volumes haben Sie lokale Festplatten zugewiesen und dem VM-Upload-Puffer und Ihren Anwendungsdaten hinzugefügt.

Note

Sie können AWS Key Management Service (AWS KMS) verwenden, um Daten zu verschlüsseln, die auf ein zwischengespeichertes Volume geschrieben wurden, das in Amazon S3 gespeichert ist. Derzeit können Sie dies mithilfe der API-Referenz für AWS Storage Gateway durchführen. Weitere Informationen finden Sie unter [CreateCachediSCSIVolume](#) oder [create-cached-iscsi-volume](#).

So erstellen Sie ein Volume

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie in der Storage-Gateway-Konsole Volume erstellen aus.
3. Wählen Sie im Dialogfeld Create volume (Volume erstellen) einen Gateway für Gateway (Gateway) aus.
4. Geben Sie die Kapazität für die Cached-Volumes in Kapazität ein.

Wählen Sie für gespeicherte Volumes einen Wert für Disk ID (Datenträger-ID) aus der Liste aus.

5. Welche Optionen für Volume-Inhalt verfügbar sind, hängt vom Typ des Gateways ab, für den Sie das Volume erstellen.

Für zwischengespeicherte Volumes haben Sie die folgenden Optionen:

- Neues leeres Volume erstellen.
- Erstellen Sie ein Volume basierend auf einen Amazon EBS-Snapshot. Wenn Sie diese Option auswählen, müssen Sie einen Wert für die EBS-Snapshot-ID angeben.

Note

Das Erstellen zwischengespeicherter Volumes von Snapshots von AWS Marketplace - Volumes wird von Storage Gateway nicht unterstützt.

- Clone from last volume recovery point (Vom letzten Volume-Wiederherstellungspunkt klonen). Wenn Sie diese Option auswählen, müssen Sie eine Volume-ID für Source volume (Quell-Volume) auswählen. Wenn keine Volumes in der Region vorhanden sind, wird diese Option nicht angezeigt.

Für gespeicherte Volumes haben Sie die folgenden Optionen:

- Neues leeres Volume erstellen.
- Create a volume based on a snapshot (Volume auf der Basis eines Snapshots erstellen).
Wenn Sie diese Option auswählen, müssen Sie einen Wert für die EBS-Snapshot-ID angeben.
- Preserve existing data on the disk (Auf dem Datenträger vorhandene Daten beibehalten)


6. Geben Sie in iSCSI-Zielname einen Namen ein.

Der Zielname kann Kleinbuchstaben, Zahlen, Punkte (.) und Bindestriche (-) enthalten. iSCSI target nodeDieser Zielname wird als der Name des iSCSI target node (iSCSI-Zielknoten) auf der Registerkarte Targets (Ziele) in der Benutzeroberfläche von iSCSI Microsoft Initiator angezeigt. Beispielsweise wird der Name target1 als `iqn.1007-05.com.amazon:target1` angezeigt. Stellen Sie sicher, dass der Zielname global innerhalb Ihres Storage Area Network (SAN) eindeutig ist.

7. Überprüfen Sie, ob für die Einstellung Network interface (Netzwerkschnittstelle) die IP-Adresse ausgewählt ist, oder wählen Sie eine IP-Adresse für Network interface (Netzwerk Schnittstelle) aus. In Network interface (Netzwerkschnittstelle) wird für jeden Adapter, der für die Gateway-VM konfiguriert ist, eine einzelne IP-Adresse angezeigt. Wenn die Gateway-VM nur für einen Netzwerkadapter konfiguriert ist, wird die Dropdown-Liste Network interface (Netzwerkschnittstelle) nicht angezeigt, da nur eine IP-Adresse vorhanden ist.

Ihr iSCSI-Ziel steht auf dem von Ihnen gewählten Netzwerkadapter zur Verfügung.

Wenn Sie Ihr Gateway für die Verwendung von mehreren Netzwerkadaptern definiert haben, wählen Sie die IP-Adresse aus, die Ihre Speicheranwendungen für den Zugriff auf das Volume verwenden sollen. Weitere Informationen zum Konfigurieren von mehreren Netzwerkadaptern finden Sie unter [Konfigurieren Ihres Gateways für mehrere NICs](#).

 Note

Nachdem Sie einen Netzwerkadapter ausgewählt haben, können Sie diese Einstellung nicht ändern.

8. (Optional) Geben Sie unter Tags einen Schlüssel und einen Wert ein, um Ihrem Volume Tags hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen Ihrer Volumes erleichtert.

9. Wählen Sie Create Volume (Volume erstellen) aus.

Wenn Sie zuvor Volumes in dieser Region erstellt haben, werden diese in der Storage-Gateway-Konsole aufgelistet.

Anschließend wird das Dialogfeld Configure CHAP Authentication (CHAP-Authentifizierung konfigurieren) geöffnet. Sie können an dieser Stelle das Challenge-Handshake Authentication Protocol (CHAP) für Ihr Volume konfigurieren oder Abbrechen auswählen und CHAP später konfigurieren. Weitere Informationen zur CHAP-Einrichtung finden Sie unter [Konfigurieren der CHAP-Authentifizierung für Ihre Volumes](#).

The screenshot shows the AWS Storage Gateway console interface. At the top, there is a 'Create volume' button and an 'Actions' dropdown menu. Below this is a search bar with the text 'Filter by ID, type, or other volume attributes.' A table lists several volumes with columns for Volume ID, Status, Type, Used, Size, and Gateway. The volume 'vol-0e0eb15a2996b3094' is selected, and its details are shown below. The 'Used' field in the details is highlighted with a red box, showing '14.895 GiB'.

Volume ID	Status	Type	Used	Size	Gateway
vol-0020a0ecea492c714	Gateway offline	Cached	-	50 GiB	
vol-013c985f1fa00a284	Available	Cached	0%	30 GiB	
vol-0ba4f299e5a12f9b1	Available	Cached	3%	100 GiB	
vol-0e0eb15a2996b3094	Available	Cached	74%	20 GiB	
vol-0518ba25750e1ddb6	Working stor...	Stored	14.895 GiB	150 GiB	

Details		Tags	
Volume ID	vol-0e0eb15a2996b3094 (Cached)	Status	Available
Gateway		Used	14.895 GiB
CHAP authentication	No	Size	20 GiB
Target name	iqn.1997-05.com.amazon:wsdg-test-2	Monitoring	Cloudwatch
Initiator	10.0.0.10:10.0.0.10	Host IP	
		Host port	3260
		Snapshot schedule	-
		Created	9/26/2017, 8:57:34 PM

Wenn Sie CHAP nicht konfigurieren möchten, beginnen Sie mit der Verwendung Ihres Volumes. Weitere Informationen finden Sie unter [Verwenden des Volumes](#).

Konfigurieren der CHAP-Authentifizierung für Ihre Volumes

CHAP bietet Schutz vor Playback-Angriffen, indem für den Zugriff auf Ihre Speicher-Volume-Ziele eine Authentifizierung erforderlich gemacht wird. Im Dialogfeld Configure CHAP Authentication (CHAP-Authentifizierung konfigurieren) stellen Sie Informationen für die Konfiguration von CHAP für Ihre Volumes bereit.

So konfigurieren Sie CHAP

1. Wählen Sie das Volume aus, für das Sie CHAP konfigurieren möchten.
2. Klicken Sie im Menü Aktionen auf CHAP-Authentifizierung konfigurieren.
3. Geben Sie unter Initiatorname den Namen Ihres Initiators ein.

4. Geben Sie unter Initiatorgeheimnis den geheimen Begriff ein, den Sie zum Authentifizieren Ihres iSCSI-Initiators verwendet haben.
5. Geben Sie unter Zielgeheimnis den geheimen Begriff ein, den Sie zum Authentifizieren Ihres Ziels für die gegenseitige CHAP-Authentifizierung verwendet haben.
6. Wählen Sie Speichern aus, um Ihre Einträge zu speichern.

Weitere Informationen zum Einrichten der CHAP-Authentifizierung finden Sie unter [Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele](#).

Nächster Schritt

[Verwenden des Volumes](#)

Verwenden des Volumes

Im Folgenden finden Sie Anweisungen zum Verwenden Ihres Volumes. Um Ihren Volume verwenden zu können, müssen Sie ihn zunächst als iSCSI-Ziel mit dem Client verbinden, initialisieren und formatieren.

Themen

- [Verbinden Ihrer Volumes mit Ihrem Client](#)
- [Initialisieren und Formatieren eines Volumes](#)
- [Testen Ihres Gateways](#)
- [Wie geht es weiter?](#)

Verbinden Ihrer Volumes mit Ihrem Client

Sie verwenden den iSCSI-Initiator in Ihrem Client zum Herstellen einer Verbindung mit Ihren Volumes. Am Ende des folgenden Verfahrens stehen Ihre Volumes als lokale Geräte auf dem Client zur Verfügung.

Important

Mit Storage Gateway können mehrere Hosts mit demselben Volume verbunden werden, wenn die Hosts den Zugriff über Windows Server Failover Clustering (WSFC) koordinieren.

Ohne WSFC ist es nicht möglich, mehrere Hosts mit dem gleichen Volume zu verbinden (z. B. durch Freigabe eines nicht geclusterten NTFS/ext4-Dateisystems).

Themen

- [Herstellen einer Verbindung mit einem Microsoft Windows-Client](#)
- [Herstellen einer Verbindung mit Red Hat Enterprise Linux-Client](#)

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. Weitere Informationen finden Sie unter [Verbinden von iSCSI-Initiatoren](#).

So stellen Sie eine Verbindung mit einem Windows-Client her

1. Starten Sie „iscsicpl.exe“.
2. Wechseln Sie im Dialogfeld iSCSI Initiator Properties (iSCSI Initiator-Eigenschaften) zur Registerkarte Discovery (Ermittlung) und wählen Sie dann Discovery Portal (Ermittlungsportal) aus.
3. Geben Sie im Dialogfeld Discover Target Portal (Zielportal ermitteln) die IP-Adresse Ihres iSCSI-Ziels als IP-Adresse oder DNS-Name ein.
4. Verbinden Sie das neue Zielportal mit dem Speicher-Volume-Ziel auf dem Gateway.
5. Wählen Sie das Ziel und dann Connect (Verbinden) aus.
6. Überprüfen Sie auf der Registerkarte Targets (Ziele), ob der Zielstatus den Wert Connected (Verbunden) hat (d. h. ob eine Verbindung zum Ziel besteht), und wählen Sie dann OK (OK) aus.

Herstellen einer Verbindung mit Red Hat Enterprise Linux-Client

Das folgende Verfahren zeigt eine Zusammenfassung der Schritte, die Sie zum Verbinden mit einem Red Hat Enterprise Linux (RHEL)-Client ausführen. Weitere Informationen finden Sie unter [Verbinden von iSCSI-Initiatoren](#).

So verbinden Sie einen Linux-Client mit iSCSI-Zielen

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

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 sollte der folgenden Beispielausgabe gleichen.

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
```

Wir empfehlen Ihnen dringend, nach der Einrichtung des Initiators Ihre iSCSI-Einstellungen wie unter [Anpassen Ihrer Linux iSCSI-Einstellungen](#) beschrieben anzupassen.

Initialisieren und Formatieren eines Volumes

Nachdem Sie den Client mithilfe des iSCSI-Initiators mit Ihren Volumes verbunden haben, initialisieren und formatieren Sie Ihr Volume.

Themen

- [Initialisieren und Formatieren von Volumes unter Microsoft Windows](#)
- [Initialisieren und Formatieren von Volumes unter Red Hat Enterprise Linux](#)

Initialisieren und Formatieren von Volumes unter Microsoft Windows

Führen Sie die folgenden Schritte aus, um ein Volume unter Windows zu initialisieren und zu formatieren.

So initialisieren und formatieren Sie Ihr Speicher-Volume

1. Starten Sie **diskmgmt.msc**, um die Konsole Disk Management (Datenträgerverwaltung) zu öffnen.
2. Initialisieren Sie im Dialogfeld Initialize Disk (Datenträger initialisieren) das Volume als MBR (Master Boot Record) (Master-Bootdatensatz)-Partition. Wenn Sie den Partitionsstil auswählen, sollten Sie den Typ des Volumes berücksichtigen, mit dem Sie eine Verbindung herstellen – Cached oder Stored. Dies wird in der folgenden Tabelle gezeigt.

Partitionsstil	Unter folgenden Bedingungen verwenden
MBR (Master Boot Record, Master-Bootdatensatz)	<ul style="list-style-type: none"> • Wenn Ihr Gateway ein Stored-Volume ist und das Speicher-Volume auf eine Größe von 1 TiB begrenzt ist. • Wenn Ihr Gateway ein Cached-Volume ist und das Speicher-Volume eine Größe von weniger als 2 TiB aufweist.

Partitionsstil	Unter folgenden Bedingungen verwenden
GPT (GUID Partition Table, GUID-Partitionstabelle)	Wenn das Speicher-Volumen des Gateways eine Größe von 2 TiB oder mehr aufweist.

3. Erstellen Sie ein einfaches Volumen:

- a. Schalten Sie das Volumen online, um es zu initialisieren. Alle verfügbaren Volumina werden in der Disk Management-Konsole angezeigt.
- b. Öffnen Sie das Kontextmenü (Rechtsklick) für den Datenträger und wählen Sie dann New Simple Volume (Neues einfaches Volumen) aus.

Wichtig

Achten Sie darauf, dass Sie nicht die falsche Festplatte formatieren. Prüfen Sie, ob der Datenträger, den Sie formatieren, mit der Größe des lokalen Datenträgers übereinstimmt, den Sie der Gateway-VM zugeordnet haben, und ob ihr Status Unallocated (Nicht zugeordnet) ist.

- c. Geben Sie die maximale Festplattengröße an.
- d. Weisen Sie dem Volumen einen Laufwerksbuchstaben oder -pfad zu und formatieren Sie das Volumen durch Auswählen von Perform a quick format (Schnellformatierung ausführen).

Wichtig

Es wird nachdrücklich empfohlen, für zwischengespeicherte Volumina Perform a quick format (Schnellformatierung ausführen) auszuwählen. Dies führt zu weniger E/A-Initialisierung, einer kleineren anfänglichen Snapshot-Größe und der schnellstmöglichen Herstellung eines betriebsfähigen Volumens. Gleichzeitig wird eine Cached-Volume-Nutzung für die vollständige Formatierung verhindert.

Note

Die erforderliche Zeit zum Formatieren des Volumes hängt von der Größe des Volumes ab. Der Vorgang kann mehrere Minuten in Anspruch nehmen.

Initialisieren und Formatieren von Volumes unter Red Hat Enterprise Linux

Führen Sie die folgenden Schritte aus, um ein Volume unter Red Hat Enterprise Linux (RHEL) zu initialisieren und zu formatieren.

So initialisieren und formatieren Sie Ihr Speicher-Volume

1. Ändern Sie das Verzeichnis in den Ordner `/dev`.
2. Führen Sie den Befehl `sudo cfdisk` aus.
3. Mit folgendem Befehl identifizieren Sie Ihr neues Volume. Um neue Volumes zu finden, können Sie das Partitionslayout der Volumes aufführen.

```
$ lsblk
```

Ein Fehler wegen nicht erkannter Volume-Bezeichnung für das neue unpartitionierte Volume wird angezeigt.

4. Initialisieren Sie das neue Volume. Wenn Sie den Partitionsstil auswählen, sollten Sie den Typ und die Größe des Volumes berücksichtigen, mit dem Sie eine Verbindung herstellen – `Cached` oder `Stored`. Dies wird in der folgenden Tabelle gezeigt.

Partitionsstil	Unter folgenden Bedingungen verwenden
MBR (Master Boot Record, Master-Bootdatensatz)	<ul style="list-style-type: none"> • Wenn Ihr Gateway ein <code>Stored</code>-Volume ist und das Speicher-Volume auf eine Größe von 1 TiB begrenzt ist. • Wenn Ihr Gateway ein <code>Cached</code>-Volume ist und das Speicher-Volume eine Größe von weniger als 2 TiB aufweist.
GPT (GUID Partition Table,	Wenn das Speicher-Volume des Gateways eine Größe von 2 TiB oder mehr aufweist.

Partitionsstil	Unter folgenden Bedingungen verwenden
GUID-Partitionstabelle)	

Verwenden Sie für eine MBR-Partition den nachfolgenden Befehl: `sudo parted /dev/your volume mklabel msdos`

Verwenden Sie für eine GPT-Partition den nachfolgenden Befehl: `sudo parted /dev/your volume mklabel gpt`

- Erstellen Sie mit dem folgenden Befehl eine Partition.

```
sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
```

- Weisen Sie mit folgendem Befehl der Partition einen Laufwerksbuchstaben zu und erstellen Sie ein Dateisystem.

```
sudo mkfs -L datapartition /dev/your volume
```

- Mounten Sie das Dateisystem mit dem folgenden Befehl.

```
sudo mount -o defaults /dev/your volume /mnt/your directory
```

Testen Ihres Gateways

Sie testen Ihre Volume Gateway-Einrichtung, indem Sie die folgenden Aufgaben ausführen:

- Schreiben Sie Daten auf das Volume.
- Nehmen Sie einen Snapshot auf.
- Stellen Sie die Snapshots auf einem anderen Volume wieder her.

Sie überprüfen die Einrichtung für ein Gateway, indem Sie ein Snapshot-Backup Ihres Volumes erstellen und den Snapshot in speichern AWS. Sie stellen dann den Snapshot auf einem neuen Volume wieder her. Ihr Gateway kopiert die Daten aus dem angegebenen Snapshot in AWS auf das neue Volume.

 Note

Das Wiederherstellen von Amazon Elastic Block Store (Amazon EBS)-Volumes, die verschlüsselt werden, wird nicht unterstützt.

So erstellen Sie einen Amazon EBS-Snapshot eines Speicher-Volumes in Microsoft Windows

1. Kopieren Sie einige Daten auf dem zugeordneten Speicher-Volume auf Ihrem Windows Computer.

Die kopierte Datenmenge ist unerheblich, für diese Demonstration. Eine kleine Datei ist ausreichend für die Demonstration des Wiederherstellungsprozesses.

2. Wählen Sie im Navigationsbereich der Storage Gateway-Konsole Sie Option Volumes aus.
3. Wählen Sie den Speicher-Volume aus, den Sie für das Gateway erstellt haben.

Dieses Gateway sollte nur ein Speicher-Volume enthalten. Wenn Sie das Volume auswählen, werden die zugehörigen Eigenschaften angezeigt.

4. Wählen Sie unter Actions (Aktionen) die Option Create EBS Snapshot (EBS-Snapshot erstellen) aus, um einen Snapshot des Volumes zu erstellen.

Abhängig von der Menge der Daten auf dem Datenträger und die Upload-Bandbreite, kann es einige Sekunden dauern bis der Snapshot erstellt ist. Beachten Sie die Volume-ID für das Volume, von dem Sie einen Snapshot erstellen. Sie verwenden die Snapshot-ID, um den Snapshot zu finden.

5. Geben Sie im Dialogfeld Create EBS Snapshot (EBS-Snapshot erstellen) eine Beschreibung für Ihren Snapshot ein.
6. (Optional) Geben Sie unter Tags einen Schlüssel und Wert ein, um Tags zum Snapshot hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen Ihrer Snapshots erleichtert.
7. Wählen Sie Create Snapshot (Snapshot erstellen) aus. Ihre Snapshot ist als Amazon EBS-Snapshot gespeichert. Notieren Sie sich Ihre Snapshot-ID. Die Anzahl der Snapshots, die für Ihr Volume erstellt wurde, wird in der Snapshot-Spalte angezeigt.
8. Wählen Sie in der Spalte EBS-Snapshots den Link für das Volume aus, für das Sie den Snapshot erstellt haben, um den EBS-Snapshot in der Amazon EC2-Konsole anzuzeigen.

So stellen Sie einen Snapshot auf einem anderen Volume wieder her

Siehe [Erstellen eines Volumes](#).

Wie geht es weiter?

In den vorhergehenden Abschnitten haben Sie ein Gateway erstellt und bereitgestellt und dann Ihren Host mit dem Speicher-Volume des Gateways verbunden. Sie haben Daten zum iSCSI-Volume des Gateways hinzugefügt, einen Snapshot des Volumes erstellt und es in einem neuen Volume wiederhergestellt. Dann haben Sie eine Verbindung zu dem neuen Volume hergestellt und verifiziert, dass die Daten darauf angezeigt wurden.

Nachdem Sie die Übung abgeschlossen haben, sollten Sie Folgendes beachten:

- Wenn Sie Ihr Gateway weiter nutzen möchten, sollten Sie die Informationen über die bessere Dimensionierung des Upload-Puffers für reale Workloads lesen. Weitere Informationen finden Sie unter [Bestimmen der Größe des Volume Gateway-Speichers für reale Workloads](#).
- Wenn Sie Ihr Gateway nicht weiter nutzen möchten, sollten Sie das Gateway löschen, um anfallende Gebühren zu vermeiden. Weitere Informationen finden Sie unter [Bereinigen nicht benötigter Ressourcen](#).

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

- Weitere Informationen zu Speicher-Volumes und deren Verwaltung finden Sie unter [Verwalten von Gateways](#).
- Informationen zum Beheben von Gateway-Problemen finden Sie unter [Fehlerbehebung bei Ihrem Gateway](#).
- Informationen zum Optimieren Ihres Gateways finden Sie unter [Optimieren der Gateway-Leistung](#).
- Informationen zu Storage Gateway-Metriken und dazu, wie Sie die Leistung Ihres Gateways überwachen können, finden Sie unter [Überwachen von Storage Gateway](#).
- Weitere Informationen zum Konfigurieren der iSCSI-Ziele Ihres Gateways zum Speichern von Daten finden Sie unter [Verbinden eines Windows-Clients mit Volumes](#).

Weitere Informationen über die Dimensionierung des Speichers Ihrer Volume Gateway-Instance für reale Arbeitslasten und zum Bereinigen nicht benötigter Ressourcen finden Sie in den folgenden Abschnitten.

Bestimmen der Größe des Volume Gateway-Speichers für reale Workloads

An diesem Punkt verfügen Sie über ein einfaches, funktionierendes Gateway. Die Annahmen zur Erstellung des Gateways sind jedoch nicht für reale Workloads geeignet. Wenn Sie das Gateway für reale Workloads verwenden möchten, müssen Sie zwei Dinge tun:

1. Bestimmen Sie die angemessene Größe Ihres Upload-Puffers.
2. Richten Sie die Überwachung für Ihren Upload-Puffer ein, falls Sie dies nicht bereits getan haben.

Im Folgenden erfahren Sie, wie Sie diese Aufgaben ausführen. Wenn Sie ein Gateway für Cached Volumes aktiviert haben, müssen Sie auch die Größe Ihres Cache-Speichers für reale Workloads auslegen.

So bestimmen Sie die Größe des Upload-Puffers und des Cache-Speichers für ein Gateway-Cached-Setup

- Verwenden Sie die Formel [Bestimmen der Größe des zuzuordnenden Upload-Puffers](#) für die Dimensionierung des Upload-Puffers. Es wird dringend empfohlen, für den Upload-Puffer mindestens 150 GiB zuzuweisen. Wenn die Formel für den Upload-Puffer einen Wert von weniger als 150 GiB ergibt, verwenden Sie 150 GiB als zugewiesenen Upload-Puffer.

Die Upload-Pufferformel berücksichtigt den Unterschied zwischen dem Durchsatz von Ihrer Anwendung zu Ihrem Gateway und dem Durchsatz von Ihrem Gateway zu AWS, multipliziert mit der voraussichtlichen Schreibdauer von Daten. Beispiel: Ihre Anwendungen 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 gibt die Formel an, dass Sie etwa 675 GiB Upload-Puffer-Speicherplatz zuweisen müssen.

So bestimmen Sie die Größe des Upload-Puffers für eine gespeicherte Einrichtung

- Verwenden Sie die Formel aus [Bestimmen der Größe des zuzuordnenden Upload-Puffers](#). Es wird dringend empfohlen, für Ihren Upload-Puffer mindestens 150 GiB zuzuweisen. Wenn die Formel für den Upload-Puffer einen Wert von weniger als 150 GiB ergibt, verwenden Sie 150 GiB als zugewiesenen Upload-Puffer.

Die Upload-Pufferformel berücksichtigt den Unterschied zwischen dem Durchsatz von Ihrer Anwendung zu Ihrem Gateway und dem Durchsatz von Ihrem Gateway zu AWS, multipliziert mit

der voraussichtlichen Schreibdauer von Daten. Beispiel: Ihre Anwendungen 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 gibt die Formel an, dass Sie etwa 675 GiB Upload-Puffer-Speicherplatz zuweisen müssen.

So überwachen Sie den Upload-Puffer

1. Öffnen Sie die Storage Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie die Registerkarte Gateway und dann die Registerkarte Details. Suchen Sie das Feld Upload Buffer Used (Verwendeter Upload-Puffer), um den aktuellen Upload-Puffer Ihres Gateways anzuzeigen.
3. Legen Sie einen oder mehrere Alarme fest, die Sie über die Nutzung des Upload-Puffers benachrichtigen.

Wir empfehlen dringend, einen oder mehrere Upload-Pufferalarme in der Amazon- CloudWatch Konsole zu erstellen. Sie können beispielsweise einen Alarm für eine Nutzungsstufe festlegen, bei der Sie gewarnt werden möchten, und einen Alarm für eine Nutzungsstufe, deren Überschreitung eine Aktion auslöst. Die Aktion kann beispielsweise im Hinzufügen weiteren Upload-Pufferspeichers bestehen. Weitere Informationen finden Sie unter [So richten Sie einen Obergrenzenalarm für den Gateway-Upload-Puffer ein](#).

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.

So bereinigen Sie nicht benötigte Ressourcen

1. Löschen Sie alle Snapshots. Anweisungen finden Sie unter [Löschen eines Snapshots](#).
2. Falls Sie das Gateway nicht weiterhin verwenden möchten, löschen Sie es. Weitere Informationen finden Sie unter [Löschen des Gateways über die AWS Storage Gateway -Konsole und Bereinigen zugehöriger Ressourcen](#).
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.

Sichern von Volumes

Mithilfe von Storage Gateway können Sie Ihre On-Premises-Geschäftsanwendungen schützen, die Storage Gateway-Volumes für cloudbasierten Speicher verwenden. Sie können Ihre On-Premises-Storage Gateway-Volumes über den nativen Snapshot-Planer in Storage Gateway oder AWS Backup sichern. In beiden Fällen werden Storage Gateway-Volume-Sicherungen als Amazon EBS-Snapshots in Amazon Web Services gespeichert.

Themen

- [Verwenden von Storage Gateway zum Sichern Ihrer Volumes](#)
- [Verwenden von AWS Backup zum Sichern Ihrer Volumes](#)

Verwenden von Storage Gateway zum Sichern Ihrer Volumes

Sie können zum Sichern Ihrer Volumes die Storage Gateway-Managementkonsole verwenden, indem Sie Amazon EBS-Snapshots erstellen und die Snapshots in Amazon Web Services speichern. Sie können entweder einen einmaligen Snapshot erstellen oder einen Snapshot-Zeitplan einrichten, der von Storage Gateway verwaltet wird. Sie können den Snapshot später dann auf einem neuen Volume über die Storage-Gateway-Konsole wiederherstellen. Informationen zum Sichern und Verwalten Ihrer Sicherung über Storage Gateway finden Sie in den folgenden Themen:

- [Testen Ihres Gateways](#)
- [Erstellen eines einmaligen Snapshots](#)
- [Klonen einer Volume](#)

Verwenden von AWS Backup zum Sichern Ihrer Volumes

AWS Backup ist ein zentralisierter Backup-Service, der es Ihnen leicht und kostengünstig macht, Ihre Anwendungsdaten über - AWS Services hinweg sowohl in der Amazon Web Services Cloud als auch On-Premises zu sichern. Auf diese Weise können Sie Ihre geschäftlichen und gesetzlichen Anforderungen an die Einhaltung von Backups erfüllen. AWS Backup macht den Schutz Ihrer AWS Speicher-Volumes, Datenbanken und Dateisysteme einfach, indem es einen zentralen Ort bietet, an dem Sie Folgendes tun können:

- Konfigurieren und prüfen Sie die AWS Ressourcen, die Sie sichern möchten.
- Automatisieren geplanter Sicherungen

- Festlegen von Aufbewahrungsrichtlinien
- Überwachen der letzten Sicherungs- und Wiederherstellungsaktivitäten

Da Storage Gateway integriert ist AWS Backup, können Kunden verwenden, AWS Backup um On-Premises-Geschäftsanwendungen zu sichern, die Storage Gateway-Volumes für Cloud-gestützten Speicher verwenden. AWS Backup unterstützt Backup und Wiederherstellung sowohl zwischengespeicherter als auch gespeicherter Volumes. Weitere Informationen zu finden Sie AWS Backup in der - AWS Backup Dokumentation. Weitere Informationen zu AWS Backup finden Sie unter [Was ist AWS Backup?](#) im AWS Backup -Benutzerhandbuch.

Sie können die Backup- und Wiederherstellungsvorgänge von Storage Gateway-Volumes mit AWS Backup verwalten und vermeiden, dass Sie benutzerdefinierte Skripts erstellen oder point-in-time Backups manuell verwalten müssen. Mit können AWS Backup Sie auch Ihre On-Premises-Volume-Backups zusammen mit Ihren In-Cloud- AWS Ressourcen von einem einzigen AWS Backup Dashboard aus überwachen. Sie können verwenden AWS Backup , um entweder ein einmaliges On-Demand-Backup zu erstellen oder einen Backup-Plan zu definieren, der in verwaltet wird AWS Backup.

Storage Gateway-Volume-Backups, die von erstellt wurden, AWS Backup werden in Amazon S3 als Amazon-EBS-Snapshots gespeichert. Sie können die Storage Gateway-Volume-Backups über die AWS Backup Konsole oder die Amazon-EBS-Konsole anzeigen.

Sie können Storage Gateway-Volumes, die über verwaltet werden, einfach AWS Backup auf jedem On-Premises-Gateway oder In-Cloud-Gateway wiederherstellen. Sie können ein solches Volume auch auf einem Amazon EBS-Volume wiederherstellen, das Sie mit EC2-Instances verwenden können.

Vorteile der Verwendung von AWS Backup zum Sichern von Storage Gateway-Volumes

Der Vorteil der Verwendung von AWS Backup zum Sichern von Storage Gateway-Volumes besteht darin, dass Sie Compliance-Anforderungen erfüllen, Betriebsaufwand vermeiden und das Backup-Management zentralisieren können. AWS Backup ermöglicht Ihnen Folgendes:

- Festlegen anpassbarer geplanter Sicherungsrichtlinien, die Ihre Sicherungsanforderungen erfüllen
- Legen Sie Regeln für die Aufbewahrung und den Ablauf von Backups fest, damit Sie keine benutzerdefinierten Skripts mehr entwickeln oder die point-in-time Backups Ihrer Volumes manuell verwalten müssen.

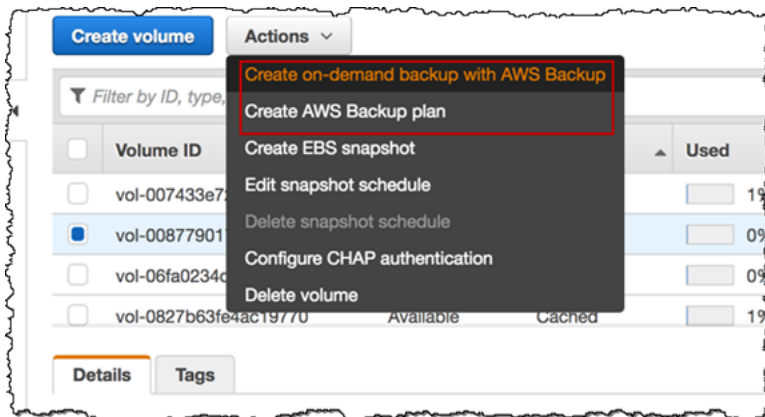
- Verwalten und überwachen Sie Backups über mehrere Gateways hinweg und andere - AWS Ressourcen aus einer zentralen Ansicht.

So verwenden Sie AWS Backup , um Backups Ihrer Volumes zu erstellen

Note

AWS Backup erfordert, dass Sie eine AWS Identity and Access Management (IAM)-Rolle auswählen, die AWS Backup verwendet. Sie müssen diese Rolle erstellen, da sie AWS Backup nicht für Sie erstellt. Sie müssen auch eine Vertrauensstellung zwischen AWS Backup und dieser IAM-Rolle erstellen. Weitere Informationen dazu finden Sie im AWS Backup -Benutzerhandbuch. Weitere Informationen dazu finden Sie unter [Erstellen eines Sicherungsplans](#) im AWS Backup -Benutzerhandbuch.

1. Öffnen Sie die Storage-Gateway-Konsole und wählen Sie im linken Navigationsbereich Volumes aus.
2. Wählen Sie für Aktionen die Option On-Demand-Backup erstellen mit AWS Backup oder AWS Backup-Plan erstellen aus.



Wenn Sie ein On-Demand-Backup des Storage Gateway-Volumes erstellen möchten, wählen Sie On-Demand-Backup mit erstellen aus AWS Backup. Sie werden zur AWS Backup Konsole weitergeleitet.

Create on-demand backup

Settings

Resource
Specify the AWS resource that you want to backup

Resource type: Volume ID:

Backup window

Create Backup now
 Customize backup window

Lifecycle
Specify when this backup is transitioned to cold storage or is expired [Info](#)

Move to cold date
N/A

Expire

Backup Vault

Wenn Sie einen neuen AWS Backup Plan erstellen möchten, wählen Sie **AWS Backup-Plan erstellen** aus. Sie werden zur **AWS Backup Konsole** weitergeleitet.

Create backup plan

Start options

Choose how you want to begin. [Info](#)

Build a new plan
Enter configuration details to create a new backup plan.

Start from an existing plan
Create a new backup plan based on an existing backup plan, including plans created by AWS.

Define a plan using JSON [Info](#)

Backup plan name

Backup plan name is case sensitive. Must contain from 1 to 63 alphanumeric characters or hyphens.

In der AWS Backup Konsole können Sie einen Backup-Plan erstellen, dem Backup-Plan ein Storage Gateway-Volume zuweisen und ein Backup erstellen. Sie können auch laufende Sicherungsverwaltungsaufgaben durchführen.

Suchen und Wiederherstellen Ihrer Volumes von AWS Backup aus

Sie können Ihre Storage Gateway-Sicherungs-Volumes über die AWS Backup Konsole suchen und wiederherstellen. Weitere Informationen finden Sie im AWS Backup -Benutzerhandbuch. Weitere Informationen finden Sie unter [Wiederherstellungspunkte](#) im AWS Backup -Benutzerhandbuch.

So finden Sie Ihre Volumes und stellen sie wieder her

1. Öffnen Sie die - AWS Backup Konsole und suchen Sie das Storage Gateway-Volume-Backup, das Sie wiederherstellen möchten. Sie können das Storage Gateway-Volume-Backup auf einem Amazon EBS-Volume oder auf einem Storage Gateway-Volume wiederherstellen. Wählen Sie die geeignete Option für Ihre Anforderungen aus.
2. Wählen Sie unter Wiederherstellungstyp ein gespeichertes oder zwischengespeichertes Storage Gateway-Volume aus und geben Sie die erforderlichen Informationen ein:
 - Geben Sie für gespeicherte Volumes Informationen zu Gateway name (Gateway-Name), Disk ID (Datenträger-ID) und iSCSI target name (iSCSI-Zielname) ein.

Restore backup

Settings

Snapshot ID
snap-068e1ef065c6f2704

Resource type
Specify the type of AWS resource to create when restoring this backup

EBS volume

Storage Gateway volume

Gateway
temp [dropdown arrow]

iSCSI target name
[input field]

1 to 200 characters including a-z, 0-9, and "-,"

- Geben Sie für zwischengespeicherte Volumes Informationen zu Gateway name (Gateway-Name), Capacity (Kapazität) und iSCSI target name (iSCSI-Zielname) ein.

Restore backup

Settings

Snapshot ID
snap-068e1ef065c6f2704

Resource type
Specify the type of AWS resource to create when restoring this backup

EBS volume

Storage Gateway volume

Gateway
v-thinstaller-centos-1

Capacity
TiB

iSCSI target name
1 to 200 characters including a-z, 0-9, and "-;"

3. Wählen Sie Restore resource (Ressource wiederherstellen) aus, um Ihr Volume wiederherzustellen.

Note

Sie können die Amazon-EBS-Konsole nicht verwenden, um einen Snapshot zu löschen, der von erstellt wurde AWS Backup.

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 an 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 [Ihr Volume Gateway mit zu verbinden 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](#)

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 `Endpoint 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 Ihres Volume Gateways](#)
- [Verschieben Ihrer Daten auf ein neues Gateway](#)

Verwalten Ihres Volume Gateways


In den folgenden Abschnitten erhalten Sie Informationen zum Verwalten der Volume-Gateway-Ressourcen.

Zwischengespeicherte Volumes sind Volumes in Amazon Simple Storage Service (Amazon S3), die als iSCSI-Ziele, auf denen Sie Ihre Anwendungsdaten speichern können, zur Verfügung gestellt werden. Hier finden Sie Informationen zum Hinzufügen und Löschen von Volumes für eine Cached-Konfiguration. Sie können auch lernen, wie Sie Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes in Amazon-EC2-Gateways hinzufügen und daraus entfernen.

Themen

- [Bearbeiten grundlegender Gateway-Informationen](#)
- [Hinzufügen einer Volume](#)
- [Die Größe einer Volume erweitern](#)
- [Klonen einer Volume](#)

- [Anzeigen von Volume-Nutzung](#)
- [Reduzieren des für ein Volume fakturierten Speichers](#)
- [Löschen eines Volumes](#)
- [Verschieben Ihrer Volumes zu einem anderen Gateway](#)
- [Erstellen eines einmaligen Snapshots](#)
- [Bearbeiten Sie einen Snapshot-Zeitplan](#)
- [Löschen eines Snapshots](#)
- [Grundlagen zu Status und Übergängen bei Volumes](#)

 **Important**

Wenn ein zwischengespeichertes Volume Ihre primären Daten in Amazon S3 speichert, sollten Sie Prozesse vermeiden, die Daten auf das gesamte Volumen schreiben und lesen. Wir empfehlen Ihnen nicht, Virenschutzsoftware, die Scans die den gesamten Cached-Volume zu verwenden. Ein solcher Scan, unabhängig davon, ob er bei Anforderung oder geplante durchgeführt wird, sorgt dafür, dass alle Daten in Amazon S3 zum Scannen lokal heruntergeladen werden, sodass viel Bandbreite verbraucht wird. Anstatt einen vollständigen Festplatten-Scann durchzuführen, können Sie einen Echtzeit-Virenschutz verwenden, da dieser von der Cached-Volume gelesen oder geschrieben wird.

Ändern der Größe eines Volumes wird nicht unterstützt. Wenn Sie die Größe eines Volumes ändern möchten, erstellen Sie einen Snapshot des Volumes, und erstellen Sie anschließend aus dem Snapshot eine neue Cached-Volume Die neue Lautstärke ist größer als das Volume, aus der der Snapshot erstellt wurde. Die Schritte zum Entfernen eines Volumes, finden Sie unter [So löschen Sie ein Volume](#). Die Schritte zum Hinzufügen einer Volume und zum Beibehalten von vorhandenen Daten, finden Sie unter [Löschen eines Volumes](#).

Alle Daten von zwischengespeicherten Volumes und Snapshots sind in Amazon S3 gespeichert und werden im Ruhezustand mit serverseitiger Verschlüsselung (SSE) verschlüsselt. Sie können jedoch nicht mithilfe der Amazon S3-API oder anderen Tools wie beispielsweise der Amazon-S3-Managementkonsole auf diese Daten zugreifen.

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 Alarmer getrennt, die zur Überwachung des Gateways eingerichtet wurden. Um die Alarmer erneut zu verbinden, aktualisieren Sie für GatewayName jeden Alarm in der CloudWatch Konsole.

Hinzufügen einer Volume

Bei steigenden Anwendungsanforderungen, müssen Sie möglicherweise weitere Volumes zu Ihrem Gateway hinzufügen. Wenn Sie mehrere Volumes hinzufügen, müssen Sie die Größe des Cache-Speicher und des Upload-Speicher, der dem Gateway zugeordnet ist berücksichtigen. Das Gateway muss über genügend Puffer und Cache-Speicherplatz für neue Volumes verfügen. Weitere Informationen finden Sie unter [Bestimmen der Größe des zuzuordnenden Upload-Puffers](#).

Sie können Volumes mithilfe der Storage-Gateway-Konsole oder der Storage Gateway-API hinzufügen. Informationen zur Verwendung der Storage Gateway-API zum Hinzufügen von Volumes finden Sie unter [CreateCachediSCSIVolume](#). Informationen zum Hinzufügen von Volumes mithilfe der Storage-Gateway-Konsole finden Sie unter [Erstellen eines Volumes](#).

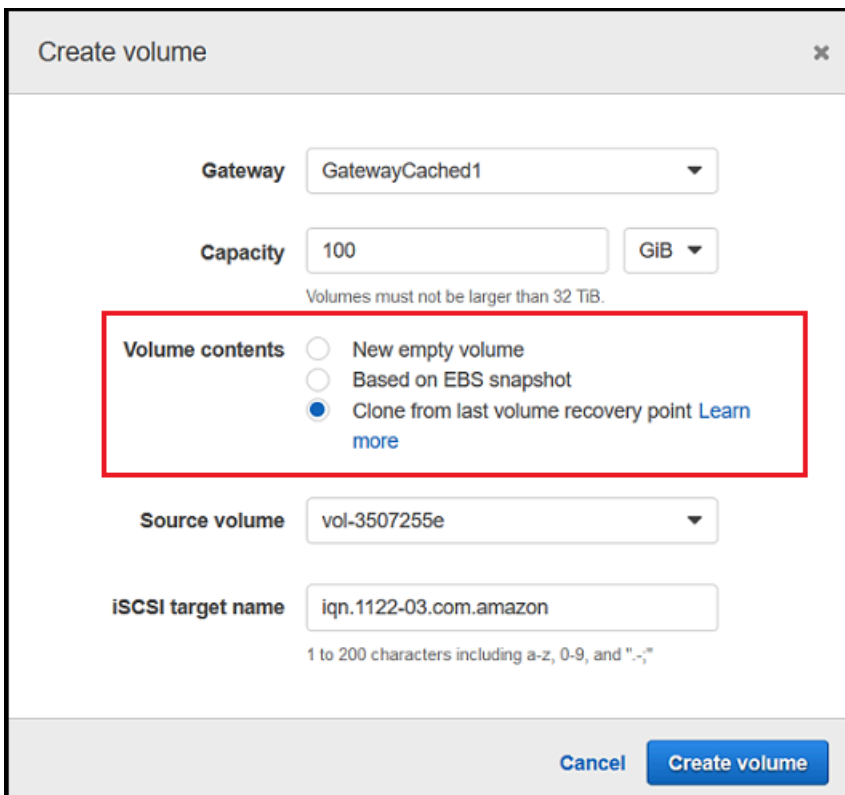
Die Größe einer Volume erweitern

Bei steigenden Anwendungsanforderungen, können Sie Ihre Volume erweitern anstatt mehr Volumes Ihrem Gateway hinzuzufügen. In diesem Fall, können Sie einen der folgenden Schritte ausführen:

- Erstellen Sie einen Snapshot der Volume, die Sie erweitern möchten und verwenden Sie dann diesen Snapshot um eine größere Volume zu erstellen. Weitere Informationen, wie Sie einen Snapshot erstellen, finden Sie unter [Erstellen eines einmaligen Snapshots](#). Weitere Informationen, wie Sie einen Snapshot verwenden um eine neue Volume zu erstellen, finden Sie unter [Erstellen eines Volumes](#).
- Verwenden Sie die Cached-Volume die Sie erweitern möchten um eine neue, größere Volume zu klonen. Weitere Informationen, wie Sie eine Volume klonen können, finden Sie unter [Klonen einer Volume](#). Weitere Informationen, wie Sie eine Volume erstellen können, finden Sie unter [Erstellen eines Volumes](#).

Klonen einer Volume

Sie können ein neues Volume aus jedem vorhandenen zwischengespeicherten Volume in derselben AWS Region erstellen. Das neue Volume wird ab dem letzten Wiederherstellungspunkt der ausgewählten Volume erstellt. Ein Volume-Wiederherstellungspunkt ist ein Zeitpunkt, zu dem alle Daten des Volumes konsistent sind. Um Volumes zu klonen, wählen Sie die Option (Clone from last recovery point) Klonen aus dem letzten Wiederherstellungspunkt im Dialogfeld Create volume (Volume erstellen), und wählen Sie dann das Volume, das als Quelle verwendet werden soll. Der folgende Screenshot zeigt das Dialogfeld Create volume (Volume erstellen).



The screenshot shows a 'Create volume' dialog box with the following fields and options:

- Gateway:** GatewayCached1
- Capacity:** 100 GIB
- Volume contents:** New empty volume, Based on EBS snapshot, Clone from last volume recovery point [Learn more](#)
- Source volume:** vol-3507255e
- iSCSI target name:** iqn.1122-03.com.amazon

Additional text: 'Volumes must not be larger than 32 TiB.' and '1 to 200 characters including a-z, 0-9, and "-,"'.

Das Klonen eines Volumes ist schneller und kostengünstiger als das Erstellen eines Amazon EBS-Snapshots. Beim Klonen werden Ihre Daten von dem Quell-Volume auf das neue Volume byte-to-byte kopiert, wobei der letzte Wiederherstellungspunkt vom Quell-Volume verwendet wird. Storage Gateway erstellt automatisch Wiederherstellungspunkte für Ihre Cached-Volumes. Um zu sehen, wann der letzte Wiederherstellungspunkt erstellt wurde, überprüfen Sie die `-TimeSinceLastRecoveryPoint` Metrik in Amazon CloudWatch.

Das geklonte Volume ist unabhängig von der Quell-Volume. Das bedeutet, dass Änderungen, die an jeder Volume nach dem Klonen vorgenommen wurden keinen Effekt auf die jeweils andere haben. Wenn Sie beispielsweise die Quell-Volume löschen, hat das keine Auswirkungen auf das geklonte Volume. Sie können auch eine Quell-Volume klonen während die Initiator verbunden werden und sie aktiv genutzt werden. Auf diese Weise wird die Leistung des Quell-Volumes nicht beeinträchtigt. Weitere Informationen, wie Sie eine Volume klonen können, finden Sie unter [Erstellen eines Volumes](#).

Sie können auch den Klon-Prozess in Wiederherstellungssituationen verwenden. Weitere Informationen finden Sie unter [Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen](#).

Klonen von einem Volume-Wiederherstellungspunkt aus

Das folgende Verfahren zeigt, wie Sie ein Volume von einem Volume-Wiederherstellungspunkt klonen und dieses Volume dann nutzen können.

Das Klonen und die Verwendung von einem unerreichbarem Gateway aus.

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie in der Storage-Gateway-Konsole Volume erstellen aus.
3. Wählen Sie im Dialogfeld Create volume (Volume erstellen) einen Gateway für Gateway (Gateway) aus.
4. Geben Sie unter Capacity (Kapazität) die Kapazität für das Volume ein. Die Kapazität muss mindestens dieselbe Größe wie die Quell-Volume sein.
5. Wählen Sie Clone from last recovery point (Klonen vom letzten Wiederherstellungspunkt) und wählen Sie eine Volume-ID für Source volume (Quell-Volume) aus. Das Quell-Volume kann ein beliebiges zwischengespeichertes Volume in der ausgewählten AWS Region sein.

The screenshot shows the 'Create volume' dialog box in the AWS Storage Gateway console. The dialog has a title bar with 'Create volume' and a close button. The main content area contains several fields and options:

- Gateway:** A dropdown menu with 'GatewayCached1' selected.
- Capacity:** A text input field with '100' and a unit dropdown with 'GiB' selected. Below this, a note states 'Volumes must not be larger than 32 TiB.'
- Volume contents:** A section with three radio button options: 'New empty volume', 'Based on EBS snapshot', and 'Clone from last volume recovery point'. The 'Clone from last volume recovery point' option is selected and highlighted with a red box. A 'Learn more' link is next to it.
- Source volume:** A dropdown menu with 'vol-3507255e' selected.
- iSCSI target name:** A text input field with 'iqn.1122-03.com.amazon' entered. Below it, a note states '1 to 200 characters including a-z, 0-9, and ".-,"'.

At the bottom of the dialog, there are two buttons: 'Cancel' and 'Create volume'.

6. Geben Sie in iSCSI target name (iSCSI-Zielname) einen Namen ein.

Der Zielname kann Kleinbuchstaben, Zahlen, Punkte (.) und Bindestriche (-) enthalten. iSCSI target nodeDieser Zielname wird als der Name des iSCSI target node (iSCSI-Zielknoten) auf der Registerkarte Targets (Ziele) in der Benutzeroberfläche von iSCSI Microsoft Initiator angezeigt. Beispielsweise wird der Name target1 als iqn.1007-05.com.amazon:target1 angezeigt. Stellen Sie sicher, dass der Zielname global innerhalb Ihres Storage Area Network (SAN) eindeutig ist.

7. Überprüfen Sie, dass für die Einstellung zu Network interface (Netzwerkschnittstelle) die IP-Adresse des Gateways ausgewählt ist, oder wählen Sie eine IP-Adresse für Network interface (Netzwerkschnittstelle).

Wenn Sie das Gateway für die Verwendung von mehreren Netzwerkadaptern definiert haben, wählen Sie die IP-Adresse aus, die Speicheranwendungen für den Zugriff auf das Volume verwenden sollen. Jeder für ein Gateway definierter Netzwerkadapter stellt eine IP-Adresse dar, die Sie auswählen können.

Wenn die Gateway-VM für mehr als einen Netzwerkadapter konfiguriert ist, zeigt das Dialogfeld Create volume (Volume erstellen) eine Liste für Network interface (Netzwerkschnittstelle) an. In dieser Liste wird für jeden für die Gateway-VM konfigurierten Adapter eine IP-Adresse angezeigt. Wenn die Gateway-VM für nur einen Netzwerkadapter konfiguriert ist, wird keine Liste angezeigt, weil nur eine IP-Adresse existiert.

8. Wählen Sie Create Volume (Volume erstellen) aus. Anschließend wird das Dialogfeld Configure CHAP Authentication (CHAP-Authentifizierung konfigurieren) geöffnet. Sie können Ihre CHAP später konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele](#).

Der nächste Schritt ist Ihr Volume mit Ihrem Client zu verbinden. Weitere Informationen finden Sie unter [Verbinden Ihrer Volumes mit Ihrem Client](#).

Erstellen eines Wiederherstellungs-Snapshots

Das folgende Verfahren zeigt, wie Sie einen Snapshot von einem Volume-Wiederherstellungspunkt erstellen können und diesen Snapshot verwenden können. Sie können Snapshots auf einer einmaligen, Ad-hoc Basis erstellen oder einen Snapshot-Zeitplan für das Volume einstellen.

So erstellen und verwenden Sie eine Wiederherstellung eines Snapshot einer Volume von einem nicht erreichbarem Gateway.

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie im Navigationsbereich Gateways aus.
3. Wählen Sie das nicht erreichbare Gateway und dann die Registerkarte Details.

Eine Wiederhergestellte-Snapshot-Nachricht wird in der Registerkarte angezeigt.



4. Wählen Sie Create recovery snapshot (Wiederherstellungs-Snapshot erstellen), um das Dialogfeld Create recovery snapshot (Wiederherstellungs-Snapshot erstellen) zu öffnen.
5. Wählen Sie in der angezeigten Liste mit Volumes das Volume, das sie wiederherstellen möchten, und dann Create snapshots (Snapshots erstellen).

Storage Gateway initiiert den Snapshot-Prozess.

6. Finden und Wiederherstellung des Snapshots.

Anzeigen von Volume-Nutzung

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

So bestimmen Sie, wie viele Daten auf ein Volume geschrieben werden

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.

2. Wählen Sie im Navigationsbereich Volumes und wählen Sie das gewünschte Volume.
3. Wählen Sie die Registerkarte Details.

Die folgenden Felder enthalten Informationen über das Volume:

- Size (Größe): Die Gesamtkapazität des ausgewählten Volumes.
- Used (Genutzt): Die Größe der gespeicherten Daten auf dem Volume.

Note

Diese Werte sind für Volumes, die vor dem 13. Mai 2015 erstellt wurden, nicht verfügbar, bis Sie Daten auf den Volumes speichern.

Reduzieren des für ein Volume fakturierten Speichers

Durch das Löschen von Dateien aus Ihrem Dateisystem werden nicht zwangsläufig Daten vom zugrunde liegenden Blockgerät gelöscht. Auch die Menge der in Ihrem Volume gespeicherten Daten wird nicht unbedingt reduziert. Wenn Sie den kostenpflichtigen Speicher in Ihrem Volume reduzieren möchten, sollten Sie Ihre Dateien mit Nullen überschreiben, um den Speicher auf eine vernachlässigbare Menge an tatsächlichem Speicher zu komprimieren. Storage Gateway berechnet die Speichernutzung für das Volume auf Basis des belegten komprimierten Speichers.

Note

Wenn Sie ein Löschtool verwenden, das die Daten auf dem Volume mit zufälligen Daten überschreibt, wird die Speichernutzung nicht reduziert. Dies liegt daran, dass die zufälligen Daten nicht komprimiert werden können.

Löschen eines Volumes

Möglicherweise müssen Sie ein Volume löschen, da an Ihrer Anwendung Änderungen vorgenommen werden müssen – z. B., wenn Sie Ihre Anwendung für die Verwendung eines größeren Speicher-Volumes migrieren. Bevor Sie diese Volume löschen, stellen Sie sicher, dass derzeit keine Anwendungen auf die Gateway-Volumes schreiben. Stellen Sie darüber hinaus sicher, dass sich keine Snapshots in Bearbeitung für das Volume befinden. Wenn ein Snapshot-Zeitplan für das Volume definiert ist, können Sie diesen auf der Registerkarte Snapshot-Zeitpläne der Storage-

Gateway-Konsole überprüfen. Weitere Informationen finden Sie unter [Bearbeiten Sie einen Snapshot-Zeitplan](#).

Sie können Volumes mit der Storage-Gateway-Konsole oder der Storage-Gateway-API löschen. Weitere Informationen zum Entfernen von Volumes mithilfe der Storage-Gateway-API finden Sie unter [Volume löschen](#). Die folgende Anleitung veranschaulicht Verwendung der Konsole:

Bevor Sie ein Volume löschen, sichern Sie die Daten oder erstellen Sie einen Snapshot der wichtigen Daten. Für Stored-Volumes werden die lokalen Laufwerke nicht gelöscht. Nachdem Sie ein Volume gelöscht haben, können Sie es nicht wiederherstellen.

So löschen Sie ein Volume

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie Volumes und anschließend mindestens ein Volume zum Löschen aus.
3. Klicken Sie unter Aktionen auf Löschen. Ein Bestätigungsdialogfeld wird angezeigt.
4. Vergewissern Sie sich, dass Sie die angegebenen Volumes löschen möchten, geben Sie dann das Wort Löschen in das Bestätigungsfeld ein und wählen Sie Löschen.

Verschieben Ihrer Volumes zu einem anderen Gateway

Wenn Ihr Datenvolumen und Ihre Leistungsanforderungen steigen, möchten Sie Ihre Volumes möglicherweise zu einem anderen Volume-Gateway verschieben. Dazu können Sie ein Volume mithilfe der Storage-Gateway-Konsole oder der API trennen und anfügen.


Durch Trennen und Anfügen eines Volumes können Sie folgende Aktionen ausführen:

- Verschieben Ihrer Volumes zu besseren Host-Plattformen oder neueren Amazon-EC2-Instances
- Aktualisieren der zugrunde liegenden Hardware für Ihren Server
- Verschieben Ihrer Volumes zwischen Hypervisor-Typen

Wenn Sie ein Volume trennen, lädt das Gateway die Volume-Daten und -Metadaten zum Storage Gateway-Service in AWS hoch und speichert diese. Sie können ein getrenntes Volume auch einfach später einem Gateway auf jeder unterstützten Host-Plattform anfügen.

 Note

Ein getrenntes Volume wird zum Standardsatz für Volumespeicher abgerechnet, bis Sie es löschen. Informationen dazu, wie Sie Kosten sparen können, finden Sie unter [Reduzieren des für ein Volume fakturierten Speichers](#).

 Note


Für das Anfügen und Trennen von Volumes gelten folgende Einschränkungen:

- Das Trennen eines Volumes kann viel Zeit in Anspruch nehmen. Wenn Sie ein Volume trennen, lädt das Gateway alle Daten auf dem Volume in hoch, AWS bevor das Volume getrennt wird. Wie viel Zeit dieser Upload dauert, hängt davon ab, wie viele Daten hochgeladen werden müssen und wie leistungsstark Ihre Netzwerkverbindung in AWS ist.
- Wenn Sie ein zwischengespeichertes Volume trennen, können Sie es nicht als gespeichertes Volume wieder anfügen.
- Wenn Sie ein gespeichertes Volume trennen, können Sie es nicht als zwischengespeichertes Volume wieder anfügen.
- Ein getrenntes Volume kann erst verwendet werden, wenn es an ein Gateway angefügt wurde.
- Wenn Sie ein gespeichertes Volume anfügen, muss es vollständig wiederhergestellt sein, bevor Sie es an ein Gateway anfügen können.
- Wenn Sie damit beginnen, ein Volume anzufügen oder zu trennen, müssen Sie warten, bis der Vorgang abgeschlossen ist, bevor Sie das Volume verwenden können.
- Das zwangsweise Löschen eines Volumes wird derzeit nur in der API unterstützt.
- Wenn Sie ein Gateway löschen, während Ihr Volume von diesem Gateway getrennt wird, führt dies zu Datenverlusten. Warten Sie, bis der Trennvorgang abgeschlossen ist, bevor Sie das Gateway löschen.
- Wenn sich ein gespeichertes Gateway im Wiederherstellungsstatus befindet, können Sie kein Volume davon trennen.

Die folgenden Schritte zeigen, wie Sie ein Volume über die Storage-Gateway-Konsole trennen und anfügen. Weitere Informationen zur Verwendung der API finden Sie unter [DetachVolume](#) oder [AttachVolume](#) in der AWS Storage Gateway -API-Referenz.

So trennen Sie ein Volume von einem Gateway

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie Volumes und dann ein oder mehrere Volumes aus, die getrennt werden sollen.
3. Wählen Sie Actions (Aktionen) und Detach volume (Volume trennen) aus. Das Bestätigungsdiaologfeld wird angezeigt.
4. Vergewissern Sie sich, dass Sie die angegebenen Volumes trennen möchten, geben Sie dann das Wort trennen in das Bestätigungsfeld ein und wählen Sie Trennen aus.

 Note

Wenn ein Volume, das Sie trennen möchten, viele Daten umfasst, geht es vom Status Attached (Angefügt) zum Status Detaching (Wird getrennt) über, bis alle Daten hochgeladen wurden. Anschließend ändert sich der Status in Detached (Getrennt). Bei kleinen Datenmengen wird der Status Detaching (Wird getrennt) möglicherweise nicht angezeigt. Wenn das Volume keine Daten enthält, ändert sich der Status von Attached (Angefügt) in Detached (Getrennt).

Sie können das Volume nun an ein anderes Gateway anfügen.

So fügen Sie ein Volume an ein Gateway an

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie im Navigationsbereich Volumes aus. Als Status der einzelnen Volumes, die getrennt wurden, wird Detached (Getrennt) angezeigt.
3. Wählen Sie aus der Liste der getrennten Volumes das Volume aus, das Sie anfügen möchten. Sie können nur jeweils ein Volume anfügen.
4. Wählen Sie unter Actions (Aktionen) die Option Attach volume (Volume anfügen) aus.

5. Wählen Sie im Dialogfeld **Attach Volume** (Volume anfügen) das Gateway aus, an das Sie das Volume anfügen möchten, und geben Sie dann das iSCSI-Ziel ein, mit dem das Volume verbunden werden soll.

Geben Sie beim Anfügen eines gespeicherten Volumes die Datenträger-ID unter **Disk ID** (Datenträger-ID) ein.

6. Wählen Sie **Attach volume** (Volume anfügen) aus. Wenn ein Volume, das Sie anfügen möchten, viele Daten umfasst, geht es vom Status **Detached** (Getrennt) in den Status **Attached** (Angefügt) über, wenn die **AttachVolume**-Operation erfolgreich war.
7. Geben Sie im Assistenten zum Konfigurieren der CHAP-Authentifizierung in den Feldern **Initiator name** (Initiatorname), **Initiator secret** (Initiatorgeheimnis) und **Target secret** (Zielgeheimnis) die entsprechenden Angaben ein und wählen Sie **Save** (Speichern) aus. Weitere Informationen zum Arbeiten mit der CHAP-Authentifizierung (Challenge-Handshake Authentication Protocol) finden Sie unter [Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele](#).

Erstellen eines einmaligen Snapshots

Zusätzlich zu geplanten Snapshots können Sie für Volume-Gateways einmalige Ad-hoc-Snapshots erstellen. Dadurch können Sie Ihre Speicher-Volume sofort, ohne Wartezeit, für den nächsten geplanten Snapshot speichern.

Aufnehmen eines einmaligen Snapshot Ihrer Speicher-Volume

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie im Navigationsbereich erst **Volumes** und anschließend das Volume, von dem Sie Ihren Snapshot erstellen möchten.
3. Wählen Sie für Aktionen **Snapshot erstellen** aus.
4. Geben Sie im Dialogfeld **Create Snapshot** (Snapshot erstellen) die Beschreibung des Snapshots ein und wählen Sie anschließend **Create Snapshot** (Snapshot erstellen).

Ob der Snapshot erstellt wurde, können Sie durch die Verwendung der Konsole überprüfen.

Ihr Snapshot ist unter **Snapshots** in der gleichen Zeile aufgelistet, in der sich das Volume befindet.

Bearbeiten Sie einen Snapshot-Zeitplan

Für gespeicherte Volumes AWS Storage Gateway erstellt einen Standard-Snapshot-Zeitplan von einmal täglich.

Note

Sie können den Standard-Snapshot-Zeitplan nicht entfernen. Gespeicherte Volumes erfordern mindestens einen Snapshot-Zeitplan. Sie können einen Snapshot-Zeitplan jedoch ändern, indem Sie entweder den Zeitpunkt der täglichen Snapshot-Erstellung oder das Intervall (alle 1, 2, 4, 8, 12 oder 24 Stunden) oder beides angeben.

Für zwischengespeicherte Volumes erstellt keinen Standard- AWS Storage Gateway Snapshot-Zeitplan. Es wird kein Snapshot-Standardzeitplan erstellt, weil die Daten in Amazon S3 gespeichert werden, Sie also keine Snapshots und keinen Snapshot-Zeitplan für die Notfallwiederherstellung benötigen. Sie können jedoch jederzeit, wann immer Sie möchten, einen Snapshot-Zeitplan einrichten. Erstellen von Snapshots für Ihre Cached-Volume bietet eine zusätzliche Möglichkeit zum Wiederherstellen Ihrer Daten, falls notwendig.

Wenn Sie die folgenden Schritte ausführen, können Sie den Snapshot-Zeitplan für ein Volume bearbeiten.

Bearbeitung eines Snapshot-Zeitplans für eine Volume

1. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
2. Wählen Sie im Navigationsbereich erst Volumes und anschließend das Volume aus, von dem der Snapshot erstellt wurde.
3. Wählen Sie unter Actions (Aktionen) die Option Edit snapshot schedule (Snapshot-Zeitplan bearbeiten) aus.
4. Ändern Sie den Zeitplan im Dialogfeld Edit snapshot schedule (Snapshot-Zeitplan bearbeiten) und wählen Sie anschließend Save (Speichern).

Löschen eines Snapshots

Sie können einen Snapshot des Speichervolumens löschen. Dies kann beispielsweise sinnvoll sein, wenn Sie im Lauf der Zeit Snapshots eines Speichervolumens erstellt haben und die älteren

Snapshots nicht mehr benötigen. Da es sich bei Snapshots um inkrementelle Sicherungen handelt, werden nur die Daten gelöscht, die nicht in anderen Snapshots benötigt werden, wenn Sie diese löschen.

Themen

- [Das Löschen von Snapshots unter Verwendung von AWS SDK für Java](#)
- [Löschen von Snapshots unter Verwendung von AWS SDK für .NET](#)
- [Löschen von Snapshots unter Verwendung der AWS Tools for Windows PowerShell](#)

Auf der Amazon-EBS-Konsole können Sie jeden Snapshot einzeln löschen. Informationen zum Löschen von Snapshots mithilfe der Amazon-EBS-Konsole finden Sie unter [Löschen eines Amazon-EBS-Snapshots](#) im Amazon-EC2-Benutzerhandbuch.

Um mehrere Snapshots gleichzeitig zu löschen, können Sie eines der - AWS SDKs verwenden, die Storage Gateway-Operationen unterstützen. Beispiele finden Sie unter [Das Löschen von Snapshots unter Verwendung von AWS SDK für Java](#), [Löschen von Snapshots unter Verwendung von AWS SDK für .NET](#) und [Löschen von Snapshots unter Verwendung der AWS Tools for Windows PowerShell](#).

Das Löschen von Snapshots unter Verwendung von AWS SDK für Java

Um so viele Snapshots im Zusammenhang mit einem Volume zu löschen, können Sie eine programmatische Herangehensweise verwenden. Im folgenden Beispiel wird gezeigt, wie Sie mit dem AWS SDK für Java Snapshots löschen. Wenn Sie den Beispielcode verwenden möchten, sollten Sie mit der Ausführung einer Java-Konsolenanwendung vertraut sein. Weitere Informationen finden Sie unter [Erste Schritte](#) im AWS SDK für Java- Entwicklerhandbuch. Falls Sie nur einige Snapshots löschen möchten, verwenden Sie die Konsole, wie hier beschrieben [Löschen eines Snapshots](#).

Example : Löschen von Snapshots mit dem AWS SDK for Java

Das folgende Java-Codebeispiel listet die Snapshots für jedes Volume einer Gateway auf und ob die Snapshot-Startzeit vor oder nach einem bestimmten Datum liegt. Es verwendet die AWS SDK for Java API für Storage Gateway und Amazon EC2. Die Amazon-EC2-API beinhaltet Operationen für das Arbeiten mit Snapshots.

Aktualisieren Sie den Code, um den Service-Endpunkt, den Amazon-Ressourcennamen (ARN) des Gateways sowie die Anzahl der zurückliegenden Tage anzugeben, für die Snapshots gespeichert werden sollen. Snapshots, die vor diesem Zeitlimit aufgenommen wurden, werden gelöscht. Sie

müssen außerdem den Booleschen Wert angeben `viewOnly`, der anzeigt, ob Sie den zu löschenden Snapshot ansehen möchten oder die eigentliche Löschung der Snapshots ausführen möchten.

Führen Sie den Code zunächst nur mit der Ansichtsoption aus (weisen Sie also `viewOnly` den Wert `true` zu), um zu prüfen, was der Code löschen wird. 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 java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

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

    // The number of days back you want to save snapshots. Snapshots before this cutoff
    are deleted
    // if viewOnly = false.
    public static int daysBack = 10;
```

```
// true = show what will be deleted; false = actually delete snapshots that meet
the daysBack criteria
public static boolean viewOnly = true;

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

    // Create a Storage Gateway and amazon ec2 client
    sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

    sgClient.setEndpoint(serviceURLSG);

    ec2Client = new AmazonEC2Client(new PropertiesCredentials(
ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
    ec2Client.setEndpoint(serviceURLEC2);

    List<VolumeInfo> volumes = ListVolumesForGateway();
    DeleteSnapshotsForVolumes(volumes, daysBack);

}
public static List<VolumeInfo> ListVolumesForGateway()
{
    List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

    String marker = null;
    do {
        ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
        ListVolumesResult result = sgClient.listVolumes(request);
        marker = result.getMarker();

        for (VolumeInfo vi : result.getVolumeInfos())
        {
            volumes.add(vi);
            System.out.println(OutputVolumeInfo(vi));
        }
    } while (marker != null);

    return volumes;
}
private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
int daysBack2) {
```

```

// Find snapshots and delete for each volume
for (VolumeInfo vi : volumes) {

    String volumeARN = vi.getVolumeARN();
    String volumeId =
volumeARN.substring(volumeARN.lastIndexOf("/") + 1).toLowerCase();
    Collection<Filter> filters = new ArrayList<Filter>();
    Filter filter = new Filter().withName("volume-id").withValues(volumeId);
    filters.add(filter);

    DescribeSnapshotsRequest describeSnapshotsRequest =
        new DescribeSnapshotsRequest().withFilters(filters);
    DescribeSnapshotsResult describeSnapshotsResult =
        ec2Client.describeSnapshots(describeSnapshotsRequest);

    List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
    System.out.println("volume-id = " + volumeId);
    for (Snapshot s : snapshots){
        StringBuilder sb = new StringBuilder();
        boolean meetsCriteria = !CompareDates(daysBack, s.getStartTime());
        sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

        sb.append(", meets criteria for delete? " + meetsCriteria);
        sb.append(", deleted? ");
        if (!viewOnly & meetsCriteria) {
            sb.append("yes");
            DeleteSnapshotRequest deleteSnapshotRequest =
                new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
            ec2Client.deleteSnapshot(deleteSnapshotRequest);
        }
        else {
            sb.append("no");
        }
        System.out.println(sb.toString());
    }
}

private static String OutputVolumeInfo(VolumeInfo vi) {

    String volumeInfo = String.format(
        "Volume Info:\n" +
        "  ARN: %s\n" +

```

```
        " Type: %s\n",
        vi.getVolumeARN(),
        vi.getVolumeType());
    return volumeInfo;
}

// Returns the date in two formats as a list
public static boolean CompareDates(int daysBack, Date snapshotDate) {
    Date today = new Date();
    Calendar cal = new GregorianCalendar();
    cal.setTime(today);
    cal.add(Calendar.DAY_OF_MONTH, -daysBack);
    Date cutoffDate = cal.getTime();
    return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
}
}
```

Löschen von Snapshots unter Verwendung von AWS SDK für .NET

Um so viele Snapshots im Zusammenhang mit einem Volume zu löschen, können Sie eine programmatische Herangehensweise verwenden. Im folgenden Beispiel wird gezeigt, wie Sie mit der AWS SDK für .NET Version 2 und 3 Snapshots löschen. Wenn Sie den Beispielcode verwenden möchten, sollten Sie mit der Ausführung einer .NET-Konsolenanwendung vertraut sein. Weitere Informationen finden Sie unter [Erste Schritte](#) im AWS SDK für .NET Entwicklerhandbuch. Falls Sie nur einige Snapshots löschen möchten, verwenden Sie die Konsole, wie hier beschrieben [Löschen eines Snapshots](#).

Example : Löschen von Snapshots mit dem AWS SDK for .NET

Im folgenden C#-Codebeispiel kann ein - AWS Identity and Access Management Benutzer die Snapshots für jedes Volume eines Gateways auflisten. Der Benutzer kann dann bestimmen, ob die Snapshot-Startzeit vor oder nach einem bestimmten Datum (Aufbewahrungszeitraum) liegt, und Snapshots löschen, deren Aufbewahrungszeitraum überschritten ist. Im Beispiel kommt die AWS SDK für .NET-API für Storage Gateway und Amazon EC2 zum Einsatz. Die Amazon-EC2-API beinhaltet Operationen für das Arbeiten mit Snapshots.

Im folgenden Codebeispiel wird das AWS SDK für .NET Version 2 und 3 verwendet. Sie können ältere Versionen von .NET auf die neue Version migrieren. Weitere Informationen finden Sie unter [Migrieren Ihres Codes zur neuesten Version des AWS SDK for .NET](#).

Aktualisieren Sie den Code, um den Service-Endpunkt, den Amazon-Ressourcennamen (ARN) des Gateways sowie die Anzahl der zurückliegenden Tage anzugeben, für die Snapshots gespeichert werden sollen. Snapshots, die vor diesem Zeitlimit aufgenommen wurden, werden gelöscht. Sie müssen außerdem den Booleschen Wert angeben `viewOnly`, der anzeigt, ob Sie den zu löschenden Snapshot ansehen möchten oder die eigentliche Löschung der Snapshots ausführen möchten. Führen Sie den Code zunächst nur mit der Ansichtsoption aus (weisen Sie also `viewOnly` den Wert `true` zu), um zu prüfen, was der Code löschen wird. 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.

Zuerst erstellen Sie einen Benutzer und fügen die minimale IAM-Richtlinie zu dem IAM-Benutzer hinzu. Anschließend planen Sie automatische Snapshots für Ihr Gateway.

Die folgende Codes erstellen die minimale Richtlinie, die einem Benutzer erlauben Snapshots zu löschen. In diesem Beispiel heißt die Richtlinie **sgw-delete-snapshot**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "StmtEC2Snapshots",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "StmtSgwListVolumes",
      "Effect": "Allow",
      "Action": [
        "storagegateway:ListVolumes"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```
}
```

Der folgende C#-Code sucht alle Snapshots im angegebenen Gateway, die den Volumes und dem angegebenen Unterbrechungszeitraum entsprechen an und löscht sie dann.

```
using System;
using System.Collections.Generic;
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
    class Program
    {
        /*
         * Replace the variables below to match your environment.
         */

        /* IAM AccessKey */
        static String AwsAccessKey = "AKIA.....";

        /* IAM SecretKey */
        static String AwsSecretKey = "*****";

        /* Account number, 12 digits, no hyphen */
        static String OwnerID = "123456789012";

        /* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXX* */
        static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXX";

        /* Snapshot status: "completed", "pending", "error" */

        static String SnapshotStatus = "completed";

        /* Region where your gateway is activated */
        static String AwsRegion = "ap-southeast-2";

        /* Minimum age of snapshots before they are deleted (retention policy) */
        static int daysBack = 30;
    }
}
```

```
/*
 * Do not modify the four lines below.
 */
static AmazonEC2Config ec2Config;
static AmazonEC2Client ec2Client;
static AmazonStorageGatewayClient sgClient;
static AmazonStorageGatewayConfig sgConfig;

static void Main(string[] args)
{
    // Create an EC2 client.
    ec2Config = new AmazonEC2Config();
    ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
    ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);

    // Create a Storage Gateway client.
    sgConfig = new AmazonStorageGatewayConfig();
    sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
".amazonaws.com";
    sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
sgConfig);

    List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
    List<Snapshot> StorageGatewaySnapshots =
ListSnapshotsForVolumes(StorageGatewayVolumes,
                        daysBack);
    DeleteSnapshots(StorageGatewaySnapshots);
}

/*
 * List all volumes for your gateway
 * returns: A list of VolumeInfos, or null.
 */
private static List<VolumeInfo> ListVolumesForGateway()
{
    ListVolumesResponse response = new ListVolumesResponse();
    try
    {
        ListVolumesRequest request = new ListVolumesRequest();
        request.GatewayARN = GatewayARN;
        response = sgClient.ListVolumes(request);

        foreach (VolumeInfo vi in response.VolumeInfos)
```



```
        {
            Console.WriteLine(OutputVolumeInfo(vi));
        }
    }
    catch (AmazonStorageGatewayException ex)
    {
        Console.WriteLine(ex.Message);
    }
    return response.VolumeInfos;
}

/*
 * Gets the list of snapshots that match the requested volumes
 * and cutoff period.
 */
private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
{
    List<Snapshot> SelectedSnapshots = new List<Snapshot>();
    try
    {
        foreach (VolumeInfo vi in volumes)
        {
            String volumeARN = vi.VolumeARN;
            String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

            DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

            Filter ownerFilter = new Filter();
            List<String> ownerValues = new List<String>();
            ownerValues.Add(OwnerID);
            ownerFilter.Name = "owner-id";
            ownerFilter.Values = ownerValues;
            describeSnapshotsRequest.Filters.Add(ownerFilter);

            Filter statusFilter = new Filter();
            List<String> statusValues = new List<String>();
            statusValues.Add(SnapshotStatus);
            statusFilter.Name = "status";
            statusFilter.Values = statusValues;
            describeSnapshotsRequest.Filters.Add(statusFilter);
```

```
        Filter volumeFilter = new Filter();
        List<String> volumeValues = new List<String>();
        volumeValues.Add(volumeID);
        volumeFilter.Name = "volume-id";
        volumeFilter.Values = volumeValues;
        describeSnapshotsRequest.Filters.Add(volumeFilter);

        DescribeSnapshotsResponse describeSnapshotsResponse =
            ec2Client.DescribeSnapshots(describeSnapshotsRequest);

        List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
        Console.WriteLine("volume-id = " + volumeID);
        foreach (Snapshot s in snapshots)
        {
            if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
            {
                Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                    " + s.StartTime + ", " + s.Description);
                SelectedSnapshots.Add(s);
            }
        }
    }
}
catch (AmazonEC2Exception ex)
{
    Console.WriteLine(ex.Message);
}
return SelectedSnapshots;
}

/*
 * Deletes a list of snapshots.
 */
private static void DeleteSnapshots(List<Snapshot> snapshots)
{
    try
    {
        foreach (Snapshot s in snapshots)
        {

            DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
            DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
```

```
        Console.WriteLine("Volume: " +
            s.VolumeId +
            " => Snapshot: " +
            s.SnapshotId +
            " Response: "
            + response.HttpStatusCode.ToString());
    }
}
catch (AmazonEC2Exception ex)
{
    Console.WriteLine(ex.Message);
}
}

/*
 * Checks if the snapshot creation date is past the retention period.
 */
private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
snapshotDate)
{
    DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
    return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
}

/*
 * Displays information related to a volume.
 */
private static String OutputVolumeInfo(VolumeInfo vi)
{
    String volumeInfo = String.Format(
        "Volume Info:\n" +
        "  ARN: {0}\n" +
        "  Type: {1}\n",
        vi.VolumeARN,
        vi.VolumeType);
    return volumeInfo;
}
}
}
```

Löschen von Snapshots unter Verwendung der AWS Tools for Windows PowerShell

Um so viele Snapshots im Zusammenhang mit einem Volume zu löschen, können Sie eine programmatische Herangehensweise verwenden. Im folgenden Beispiel wird gezeigt, wie Sie mit den AWS Tools for Windows PowerShell Snapshots löschen. Um das Beispielskript verwenden zu können, sollten Sie mit der Ausführung eines PowerShell Skripts vertraut sein. Weitere Informationen finden Sie unter [Erste Schritte](#) im AWS Tools for Windows PowerShell. Falls Sie nur einige Snapshots löschen möchten, verwenden Sie die Konsole, wie hier beschrieben [Löschen eines Snapshots](#).

Example : Löschen von Snapshots mithilfe der AWS Tools for Windows PowerShell

Das folgende PowerShell Skriptbeispiel listet die Snapshots für jedes Volume eines Gateways auf und ob die Snapshot-Startzeit vor oder nach einem bestimmten Datum liegt. Es verwendet die AWS Tools for Windows PowerShell Cmdlets für Storage Gateway und Amazon EC2. Die Amazon-EC2-API beinhaltet Operationen für das Arbeiten mit Snapshots.

Sie müssen das Skript aktualisieren und den Amazon-Ressourcennamen (ARN) des Gateways sowie die Anzahl der zurückliegenden Tage angeben, für die Snapshots gespeichert werden sollen. Snapshots, die vor diesem Zeitlimit aufgenommen wurden, werden gelöscht. Sie müssen außerdem den Booleschen Wert angeben `viewOnly`, der anzeigt, ob Sie den zu löschenden Snapshot ansehen möchten oder die eigentliche Löschung der Snapshots ausführen möchten. Führen Sie den Code zunächst nur mit der Ansichtsoption aus (weisen Sie also `viewOnly` den Wert `true` zu), um zu prüfen, was der Code löschen wird.

```
<#
.DESCRIPTION
    Delete snapshots of a specified volume that match given criteria.

.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS 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_DeleteSnapshots.ps1
#>

# Criteria to use to filter the results returned.
```

```
$daysBack = 18
$gatewayARN = "**** provide gateway ARN ****"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volume in $volumesResult)
{
    Write-Output("`nVolume Info:")
    Write-Output("ARN: " + $volume.VolumeARN)
    Write-Output("Type: " + $volume.VolumeType)
}

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
{
    $volumeARN = $volume.VolumeARN

    $volumeId = ($volumeARN-split"/")[3].ToLower()

    $filter = New-Object Amazon.EC2.Model.Filter
    $filter.Name = "volume-id"
    $filter.Value.Add($volumeId)

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
        $d = ([DateTime]::Now).AddDays(-$daysBack)
        $meetsCriteria = $false
        if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
        {
            $meetsCriteria = $true
        }

        $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
        $meetsCriteria
        if (!$viewOnly -AND $meetsCriteria)
        {
            $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
            #Can get RequestId from response for troubleshooting.
            $sb = $sb + ", deleted? yes"
        }
    }
}
```

```
    else {  
        $sb = $sb + ", deleted? no"  
    }  
    Write-Output($sb)  
}  
}
```

Grundlagen zu Status und Übergängen bei Volumes

Jeder Volume verfügt über einen zugeordneten Status, aus dem sich auf einen Blick der Zustand des Volumes ersehen lässt. In den meisten Fällen gibt der Status an, dass der Volume ordnungsgemäß funktioniert und Sie keine Aktion durchzuführen brauchen. In einigen Fällen gibt der Status ein Problem mit dem Volume an, das eventuell eine Aktion Ihrerseits erforderlich macht. Die folgenden Informationen können Sie bei der Entscheidung unterstützen, ob Sie handeln müssen. Sie können den Volume-Status in der Storage Gateway-Konsole oder mithilfe einer der Storage Gateway-API-Operationen anzeigen, z. B. [DescribeCachediSCSIVolumes](#) oder [DescribeStorediSCSIVolumes](#).

Themen

- [Grundlagen zum Volume Status](#)
- [Grundlegendes zum Anfügestatus](#)
- [Grundlagen zu Statusübergängen bei Cached-Volumes](#)
- [Grundlagen zu Statusübergängen bei Stored-Volumes](#)

Grundlagen zum Volume Status

Die folgende Tabelle zeigt den Status des Volumes in der Storage-Gateway-Konsole. Der Status des Volumes wird in der Spalte Status für jedes Speichervolume im Gateway angezeigt. Ein Volume, das ordnungsgemäß funktioniert, hat den Status Available (Verfügbar).

In der folgenden Tabelle finden Sie eine Beschreibung aller Speichervolumestatus sowie Hinweise, ob statusspezifisch Maßnahmen ergriffen werden müssen. Der Status Available (Verfügbar) ist der normale Status eines Volumes. Ein Volume sollte diesen Status während des Großteils seiner Nutzungszeit aufweisen.

Status	Bedeutung
Verfügbar	Der Volume ist zur Verwendung verfügbar. Dieser Status ist der normalen Ausführungsstatus eines Volumes.

Status	Bedeutung
	<p>Wenn eine Bootstrapping-Phase abgeschlossen ist, erhält das Volume wieder den Status Available (Verfügbar). Das bedeutet, dass das Gateway alle am Volume vorgenommenen Änderungen synchronisiert hat, seitdem es den Status Pass Through erhalten hat.</p>
Bootstrapping	<p>Das Gateway synchronisiert Daten lokal mit einer Kopie der in gespeicherten Daten AWS. In der Regel müssen Sie bei diesem Status keine Maßnahmen ergreifen, weil das Speichervolume den Status Available (Verfügbar) in den meisten Fällen automatisch erkennt.</p> <p>Die folgenden Szenarien gelten, wenn ein Volume den Status Bootstrapping besitzt:</p> <ul style="list-style-type: none">• Ein Gateway ist unerwartet heruntergefahren.• Ein Gateway-Upload-Puffer wurde überschritten. In diesem Szenario tritt Bootstrapping auf, wenn Ihr Volume den Status Pass Through besitzt und die Menge des kostenlosen Upload-Puffers ausreichend erhöht wird. Sie können zusätzlichen Upload-Pufferspeicherplatz als eine Möglichkeit zur Erhöhung des Prozentsatzes der kostenlosen Upload-Pufferspeicher schaffen. In diesem Szenario ändert sich der Status des Speichervolumens von Pass Through in Bootstrapping in Available. Sie können dieses Volume während des Bootstrapping Zeitraums weiterhin verwenden. Sie können jedoch zu diesem Zeitpunkt keine Snapshots des Volumens erstellen.• Sie erstellen ein Gateway für gespeicherte Volumes und behalten die vorhandenen lokalen Festplattendaten bei. In diesem Szenario beginnt Ihr Gateway mit dem Hochladen aller Daten in AWS. Das Volume hat den Status Bootstrapping, bis alle Daten von der lokalen Festplatte nach kopiert wurden AWS. Sie können dieses Volume während des Bootstrapping Zeitraums weiterhin verwenden. Sie können jedoch zu diesem Zeitpunkt keine Snapshots des Volumens erstellen.

Status	Bedeutung
Erstellen	Das Volume wird derzeit erstellt und kann noch nicht verwendet werden. Der Status Creating (Wird erstellt) ist vorübergehend. Es ist keine Aktion erforderlich.
Wird gelöscht	Der Volume wird gerade gelöscht. Der Status Deleting (Wird gelöscht) ist vorübergehend. Es ist keine Aktion erforderlich.
Irrecoverable (Nicht wiederherstellbar)	Ein Fehler ist aufgetreten, aus dem das Volume nicht wiederhergestellt werden kann. Weitere Informationen, zu den Maßnahmen, die in dieser Situation möglich sind, finden Sie unter Fehlerbehebung bei Volume-Problemen .

Status	Bedeutung
Pass Through	<p>Daten, die lokal verwaltet werden, sind nicht synchron mit Daten, die in gespeichert sind AWS. Daten, die auf ein Volume geschrieben werden, während das Volume sich im Status Pass Through befindet, verbleiben im Cache, bis der Volume-Status Bootstrapping lautet. Diese Daten werden in hochgeladen, AWS wenn der Bootstrapping-Status beginnt.</p> <p>Der Status Pass Through kann aus verschiedenen Gründen auftreten, darunter z. B.:</p> <ul style="list-style-type: none">• Der Status Pass Through tritt auf, wenn Ihr Gateway keinen Upload-Pufferspeicher mehr hat. Während die Volumes den Status Pass Through haben, können Ihre Anwendungen weiterhin Daten von Ihren Speichervolumen lesen und Daten auf Speichervolumen schreiben. Jedoch schreibt das Gateway keine Volume-Daten in den Upload-Puffer oder lädt diese Daten auch nicht in AWS hoch. <p>Das Gateway lädt weiterhin alle Daten hoch, die auf das Volume geschrieben wurden, bevor das Volume den Status Pass Through angenommen hat. Alle ausstehenden oder geplanten Snapshots eines Speichervolumen schlagen fehl, während das Volume im Status Pass Through ist. Weitere Informationen darüber, welche Aktion durchzuführen ist, wenn das Speichervolumen den Status Pass Through erreicht, weil der Upload-Puffer erschöpft ist, finden Sie unter Fehlerbehebung bei Volume-Problemen.</p> <p>Um zum Status ACTIVE (AKTIV) zurückzukehren, muss ein Volume im Status Pass Through die Bootstrapping-Phase beenden. Während des Bootstrappings richtet das Volume die Synchronisation innerhalb von wieder ein AWS, sodass es den Datensatz (Protokoll) von Änderungen am Volume fortsetzen und die CreateSnapshot Funktionalität aktivieren kann. Beim Bootstrapping werden Schreibvorgänge auf das Volume im Upload-Puffer erfasst.</p> <ul style="list-style-type: none">• Der Status Pass Through tritt auf, wenn sich mehr als ein Speichervolumen im Bootstrapping befindet. Es kann nur jeweils ein Gateway-S

Status	Bedeutung
	<p>peichervolume zur gleichen Zeit Bootstrappen. Beispiel: Sie erstellen zwei Speichervolumes und wollen die vorhandenen Daten auf beiden beibehalten. In diesem Fall behält das zweite Speichervolume den Status Pass Through, bis das erste Speichervolume das Bootstrapping beendet hat. In diesem Szenario müssen Sie keine Maßnahmen ergreifen. Jedes Speichervolume wechselt automatisch in den Status Verfügbar, sobald seine Erstellung abgeschlossen ist. Sie können die Lese- und Schreibvorgänge zum Speichervolume fortsetzen, während es im Status Pass Through oder Bootstrapping ist.</p> <ul style="list-style-type: none"><li data-bbox="472 653 1511 856">• In seltenen Fällen gibt der Status Pass Through an, dass eine Festplatte, die einem Upload-Puffer zugeordnet wurde, fehlgeschlagen ist. Weitere Informationen, welche Aktionen in diesem Fall auszuführen sind, finden Sie unter Fehlerbehebung bei Volume-Problemen.<li data-bbox="472 884 1463 1136">• Der Status Pass Through kann auftreten, wenn ein Volume den Zustand Active (Aktiv) oder Bootstrapping aufweist. In diesem Fall empfängt das Volume eine Schreiboperation, die Kapazität des Upload-Puffers reicht aber nicht mehr aus, um die Schreiboperation aufzuzeichnen (zu protokollieren).<li data-bbox="472 1163 1503 1465">• Der Status Pass Through tritt bei beliebigem Status des Volumes auf, wenn das Gateway nicht ordnungsgemäß heruntergefahren wird. Zu einem nicht ordnungsgemäßen Herunterfahren kann es kommen, wenn die Software abstürzt oder die VM ausgeschaltet wird. In diesem Fall wird ein Volume, egal in welchem Zustand es sich befindet, in den Status Pass Through übergehen.

Status	Bedeutung
Restoring (Wiederherstellung läuft)	<p>Das Volume wird von einem vorhandenen Snapshot wiederhergestellt. Dieser Status gilt nur für gespeicherte Volumes. Weitere Informationen finden Sie unter So funktioniert Volume Gateway (Architektur).</p> <p>Wenn Sie gleichzeitig zwei Speichervolumes wiederherstellen, geben beide Speichervolumes den Status Restoring (Wird wiederhergestellt) an. Jedes Speichervolume wechselt automatisch in den Status Verfügbar, sobald seine Erstellung abgeschlossen ist. Sie können Lese- und Schreibvorgänge zu einem Speichervolume durchführen und einen Snapshot aufnehmen, während es sich im Status Restoring (Wird wiederhergestellt) befindet.</p>

Status	Bedeutung
Restoring Pass Through (Pass Through wird wiederhergestellt)	<p>Das Volume wird von einem vorhandenen Snapshot wiederhergestellt und hat ein Problem mit dem Upload-Puffer. Dieser Status gilt nur für gespeicherte Volumes. Weitere Informationen finden Sie unter So funktioniert Volume Gateway (Architektur).</p> <p>Einer der Gründe, die zum Status Restoring Pass Through (Pass Through wird wiederhergestellt) führen, ist, wenn Ihr Gateway keinen Upload-Pufferspeicher mehr hat. Ihre Anwendungen können weiterhin Daten von Ihren Speichervolumes lesen und Daten auf Ihre Speichervolumes schreiben, während diese den Status Restoring Pass Through (Pass Through wird wiederhergestellt) haben. Während der Status Restoring Pass Through (Pass Through wird wiederhergestellt) aktiv ist, können jedoch keine Snapshots eines Speichervolumes erstellt werden. Weitere Informationen darüber, welche Aktion durchgeführt werden muss, wenn Ihr Speichervolume im Status Restoring Pass Through (Pass Through wird wiederhergestellt) ist, da die Upload-Puffer Kapazität überschritten wurde, finden Sie unter Fehlerbehebung bei Volume-Problemen.</p> <p>In seltenen Fällen weist der Status Restoring Pass Through (Pass Through wird wiederhergestellt) darauf hin, dass eine Festplatte, die einem Upload-Puffer zugeordnet wurde, fehlgeschlagen ist. Weitere Informationen, welche Aktionen in diesem Fall auszuführen sind, finden Sie unter Fehlerbehebung bei Volume-Problemen.</p>
Upload Buffer Not Configured (Upload-Puffer nicht konfiguriert)	<p>Sie können das Volume nicht erstellen oder verwenden, weil für das Gateway kein Upload-Puffer konfiguriert ist. Weitere Informationen zum Hinzufügen von Upload-Puffer-Kapazität für Volumes in einer Cached-Volumes-Konfiguration finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers. Weitere Informationen zum Hinzufügen von Upload-Puffer-Kapazität für Volumes in einer Stored-Volumes-Konfiguration finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.</p>

Grundlegendes zum Anfügestatus

Sie können ein Volume mithilfe der Storage Gateway-Konsole oder API von einem Gateway trennen bzw. an ein Gateway anfügen. Die folgende Tabelle zeigt den Anfügestatus des Volumes in der Storage-Gateway-Konsole. Der Anfügestatus des Volumes wird in der Spalte Attachment status (Anfügestatus) für jedes Speichervolume im Gateway angezeigt. Beispiel: Ein Volume, das von einem Gateway getrennt ist, hat den Status Detached (Getrennt). Weitere Informationen dazu, wie Sie ein Volume trennen und anfügen können, finden Sie unter [Verschieben Ihrer Volumes zu einem anderen Gateway](#).

Status	Bedeutung
Attached (Angefügt)	Das Volume ist an ein Gateway angefügt.
Detached (Getrennt)	Das Volume ist von einem Gateway getrennt.
Detaching (Wird getrennt)	Das Volume wird von einem Gateway getrennt. Wenn Sie ein Volume trennen und das Volume keine Daten enthält, wird dieser Status möglicherweise nicht angezeigt.

Grundlagen zu Statusübergängen bei Cached-Volumes

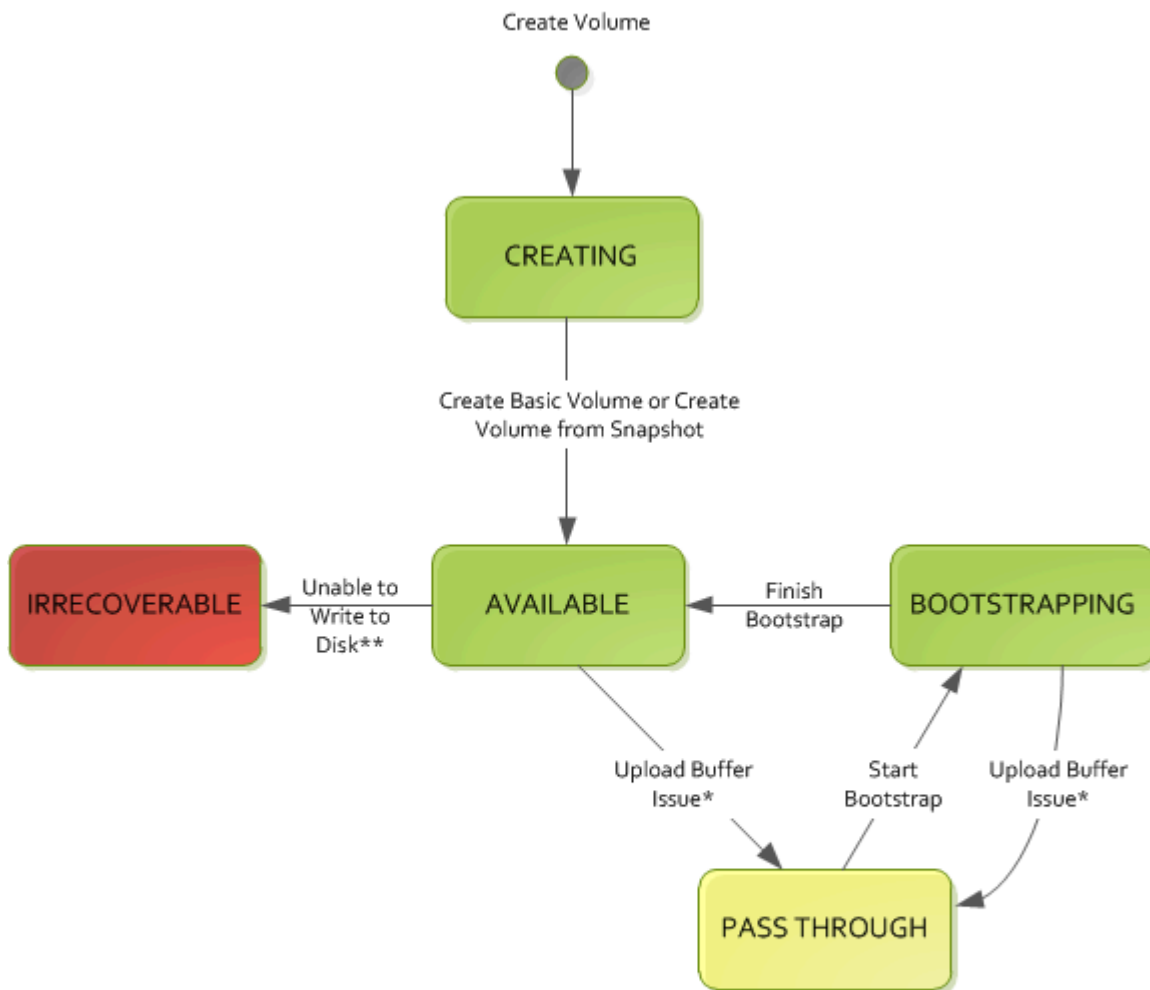
Das folgende Statusdiagramm beschreibt die gängigsten Statusübergänge für Volumes in Cached-Gateways. Sie müssen das Diagramm nicht im Detail verstehen, um Ihr Gateway effektiv zu verwenden. Die Abbildung bietet detaillierte Information, wenn Sie mehr darüber erfahren möchten, wie Volume Gateways funktionieren.

Das Diagramm zeigt weder den Status Upload-Puffer nicht konfiguriert noch den Status Wird gelöscht an. Volume-Status werden im Diagramm als grüne, gelbe und rote Felder dargestellt. Sie können die Farben mithilfe der folgenden Informationen interpretieren.

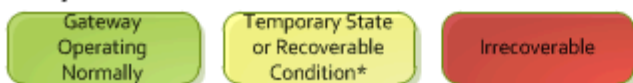
Farbe	Volume-Status
Grün	Das Gateway funktioniert normal. Der Volume-Status lautet Verfügbar bzw. wird irgendwann zu Verfügbar.

Farbe	Volume-Status
Gelb	<p>Das Volume hat den Status Pass Through, der angibt, dass ein potenzielles Problem mit dem Speichervolume vorliegt. Wenn dieser Status angezeigt wird, weil der Upload-Pufferspeicher voll ist, wird in einigen Fällen Pufferspeicherplatz wieder verfügbar werden. Zu diesem Zeitpunkt korrigiert das Speichervolume sich selbst in den Status Verfügbar. In anderen Fällen müssen Sie möglicherweise mehr Upload-Pufferspeicher für Ihr Gateway hinzufügen, damit das Speichervolume den Status Available (Verfügbar) erreicht. Weitere Informationen zur Fehlerbehebung, wenn die Upload-Puffer-Kapazität überschritten wurde, finden Sie unter Fehlerbehebung bei Volume-Problemen. Weitere Informationen zum Hinzufügen von Upload-Puffer-Kapazität, finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.</p>
Rot	<p>Das Speichervolume hat den Status Nicht wiederherstellbar. In diesem Fall sollten Sie das Volume löschen. Weitere Informationen hierzu finden Sie unter So löschen Sie ein Volume.</p>

Ein Übergang zwischen zwei Zuständen wird im Diagramm durch eine markierte Zeile dargestellt. So wird der Übergang vom Status Creating (Wird erstellt) zum Status Available (Verfügbar) als Create Basic Volume or Create Volume from Snapshot (Erstelle Basic Volume oder erstelle Volume aus Snapshot) bezeichnet. Dieser Übergang repräsentiert die Erstellung eines Cached-Volumes. Weitere Informationen zur Erstellung eines Speicher Volumes, finden Sie unter [Hinzufügen einer Volume](#).



Key



* e.g. run out of upload buffer

** e.g. lost connectivity

Note

Der Volume-Status Pass Through wird in diesem Diagramm gelb dargestellt. Dies entspricht jedoch nicht der Farbe des Statussymbols im Feld Status der Storage-Gateway-Konsole.

Grundlagen zu Statusübergängen bei Stored-Volumes

Das folgende Statusdiagramm beschreibt die gängigsten Statusübergänge für Volumes in Stored-Gateways. Sie müssen das Diagramm nicht im Detail verstehen, um Ihr Gateway effektiv zu

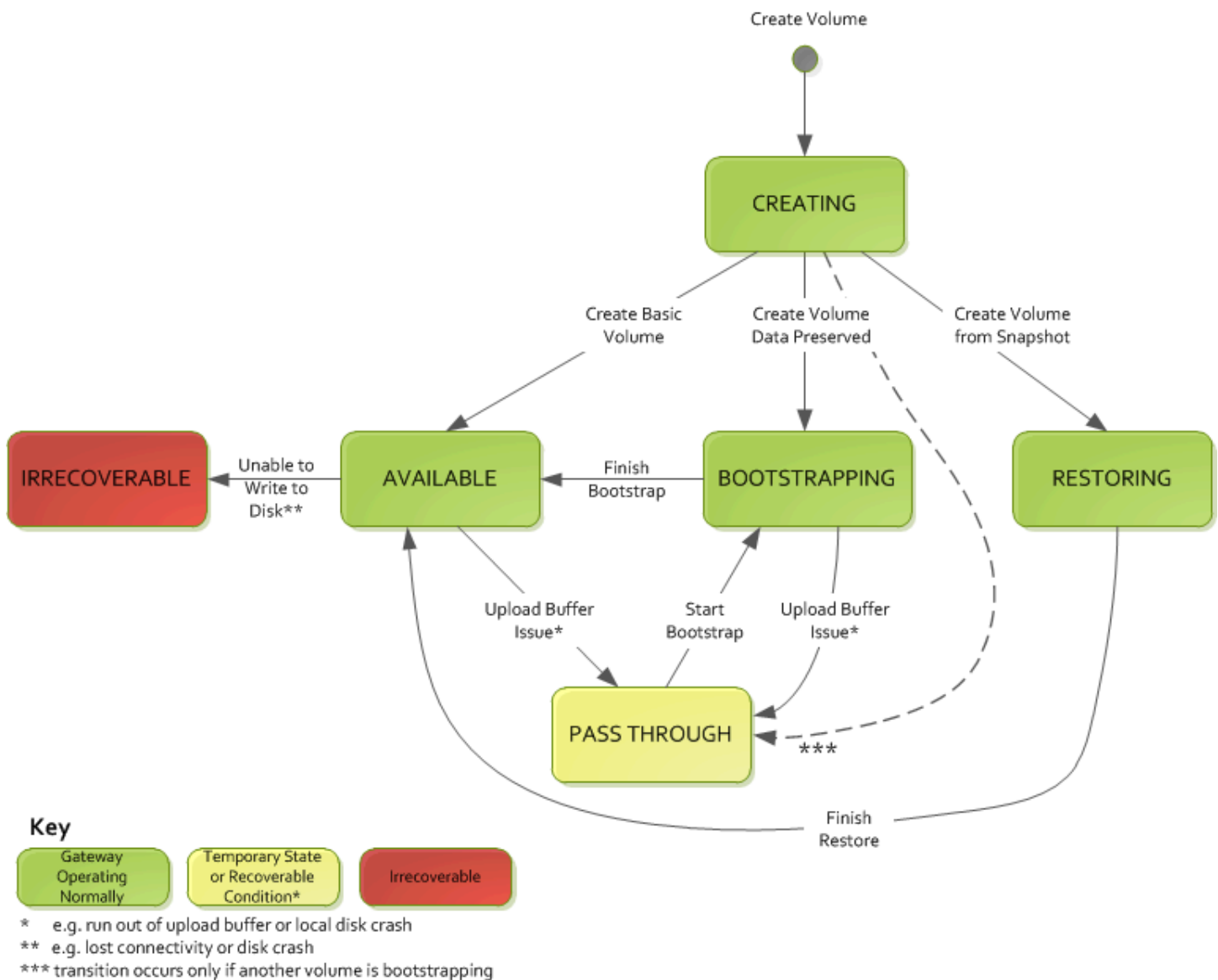
verwenden. Die Abbildung bietet detaillierte Information, wenn Sie Interesse haben mehr darüber zu erfahren, wie Volume Gateways funktionieren.

Das Diagramm zeigt weder den Status Upload-Puffer nicht konfiguriert noch den Status Wird gelöscht an. Volume-Status werden im Diagramm als grüne, gelbe und rote Felder dargestellt. Sie können die Farben mithilfe der folgenden Informationen interpretieren.

Farbe	Volume-Status
Grün	Das Gateway funktioniert normal. Der Volume-Status lautet Verfügbar bzw. wird irgendwann zu Verfügbar.
Gelb	Wenn Sie ein Speichervolume erstellen und die Daten beibehalten, dann tritt der Pfad vom Status Creating (Wird erstellt) zum Status Pass Through auf, wenn sich ein anderes Volume im Bootstrapping befindet. In diesem Fall wird das Volume vom Status Pass Through in den Status Bootstrapping übergehen und dann in den Status Available (Verfügbar), sobald das erste Volume das Bootstrapping beendet hat. Abgesehen von dem o. g. spezifischen Szenario gibt die Farbe Gelb (Status Pass Through) an, dass ein potenzielles Problem mit dem Speichervolume vorliegt; das am häufigsten auftretende Problem ist ein Problem mit dem Upload-Puffer. Wenn die Upload-Kapazität erschöpft wurde, wird in einigen Fällen Pufferspeicherplatz wieder verfügbar werden. Zu diesem Zeitpunkt korrigiert das Speichervolume sich selbst in den Status Verfügbar. In anderen Fällen müssen Sie möglicherweise mehr Upload-Pufferspeicher für Ihr Gateway hinzufügen, damit das Speichervolume in den Status Available (Verfügbar) zurückkehren kann. Weitere Informationen zur Fehlerbehebung, wenn die Upload-Puffer-

Farbe	Volume-Status
	Kapazität überschritten wurde, finden Sie unter Fehlerbehebung bei Volume-Problemen . Weitere Informationen zum Hinzufügen von Upload-Puffer-Kapazität, finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers .
Rot	Das Speichervolume hat den Status Nicht wiederherstellbar. In diesem Fall sollten Sie das Volume löschen. Weitere Informationen hierzu finden Sie unter Löschen eines Volumes .

Ein Übergang zwischen zwei Zuständen wird im folgendem Diagramm durch eine markierte Zeile dargestellt. So wird der Übergang vom Status Creating (Wird erstellt) zum Status Available (Verfügbar) als Create Basic Volume (Erstelle Basic Volume) bezeichnet. Dieser Übergang stellt die Erstellung eines Speichervolumens dar, ohne dass die Daten beibehalten oder das Volume aus einem Snapshot erstellt wird.



Note


Der Volume-Status Pass Through wird in diesem Diagramm gelb dargestellt. Dies entspricht jedoch nicht der Farbe des Statussymbols im Feld Status der Storage-Gateway-Konsole.

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 gespeicherter Volumes auf ein neues gespeichertes Volume Gateway

So verschieben Sie Ihr gespeichertes Volume auf ein neues gespeichertes Volume Gateway

1. Beenden Sie alle Anwendungen, die auf das alte gespeicherte Volume Gateway schreiben.
2. Führen Sie die folgenden Schritte aus, um einen Snapshot für Ihr Volume zu erstellen, und warten Sie dann, bis der Snapshot abgeschlossen ist.
 - a. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
 - b. Wählen Sie im Navigationsbereich zunächst Volumes und anschließend das Volume aus, von dem Sie den Snapshot erstellen möchten.
 - c. Wählen Sie für Aktionen Snapshot erstellen aus.
 - d. Geben Sie im Dialogfeld Snapshot erstellen die Beschreibung des Snapshots ein und wählen Sie anschließend Snapshot erstellen.

Ob der Snapshot erstellt wurde, können Sie durch die Verwendung der Konsole überprüfen. Wenn immer noch Daten auf das Volume hochgeladen werden, warten Sie, bis der Upload abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren. Wählen Sie die Snapshot-Links auf den Volumes aus, um den Snapshot-Status anzuzeigen und sich zu vergewissern, dass keine ausstehenden Snapshots vorliegen.

3. Gehen Sie wie folgt vor, um das alte gespeicherte Volume Gateway zu beenden:

- a. Wählen Sie im Navigationsbereich Gateways und anschließend das alte gespeicherte Volume 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 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. Wenn das Gateway heruntergefahren wird, lautet der Status des Gateways Herunterfahren.

- c. Fahren Sie die VM mithilfe der Hypervisor-Steuerelemente herunter.

Weitere Informationen zum Anhalten von Gateways finden Sie unter [Starten und Anhalten von Volume Gateway](#).


4. Trennen Sie die Speicherfestplatten, die Ihren gespeicherten Volumes zugeordnet sind, von der Gateway-VM. Die Stammfestplatte der VM wird hier ausgeschlossen.
5. Aktivieren Sie ein neues gespeichertes Volume Gateway mit einem neuen Hypervisor-VM-Image, das in der Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home> verfügbar ist.
6. Fügen Sie die physischen Speicherfestplatten an, die Sie in Schritt 5 von der alten gespeicherten Volume-Gateway-VM getrennt haben.
7. Gehen Sie wie folgt vor, um gespeicherte Volumes zu erstellen und die vorhandenen Daten auf der Festplatte beizubehalten.
 - a. Wählen Sie in der Storage-Gateway-Konsole Volume erstellen aus.
 - b. Wählen Sie im Dialogfeld Volume erstellen das gespeicherte Volume Gateway aus, das Sie in Schritt 5 erstellt haben.
 - c. Wählen Sie einen Wert für Festplatten-ID aus der Liste aus.
 - d. Für Volume-Inhalt wählen Sie die Option Vorhandene Daten auf der Festplatte beibehalten aus.

Weitere Informationen zur Erstellung von Volumes finden Sie unter [Erstellen eines Volumes](#).

8. (Optional) Geben Sie im Assistenten zum Konfigurieren der CHAP-Authentifizierung in den Feldern Initiatorname, Initiatorgeheimnis und Zielgeheimnis die entsprechenden Angaben ein und wählen Sie Speichern aus.


Weitere Informationen zum Arbeiten mit der CHAP-Authentifizierung (Challenge-Handshake Authentication Protocol) finden Sie unter [Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele](#).

9. Starten Sie die Anwendung, die auf Ihr gespeichertes Volume schreibt.
10. Wenn Sie sich vergewissert haben, dass Ihr neues gespeichertes Volume Gateway ordnungsgemäß funktioniert, können Sie das alte gespeicherte Volume Gateway löschen.

 **Important**

Bevor Sie diesen Schritt ausführen, 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.

Gehen Sie wie folgt vor, um das alte gespeicherte Volume 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 gespeicherte Volume Gateway aus, das Sie löschen möchten.
- b. Wählen Sie für Aktionen die Option Gateway löschen aus.
- c. Aktivieren Sie im Bestätigungsdialogfeld, das angezeigt wird, das Kontrollkästchen zum Bestätigen des Löschvorgangs. Stellen Sie sicher, dass die aufgelistete Gateway-ID das alte gespeicherte Volume Gateway angibt, das Sie löschen möchten, und wählen Sie dann Löschen aus.



11. Löschen Sie die alte Gateway-VM. Informationen zum Löschen einer VM finden Sie in der Dokumentation zu Ihrem Hypervisor.

Verschieben zwischengespeicherter Volumes auf eine neue zwischengespeicherte virtuelle Volume-Gateway-Maschine

So verschieben Sie zwischengespeicherte Volumes auf eine neue zwischengespeicherte virtuelle Volume-Gateway-Maschine (VM)

1. Beenden Sie alle Anwendungen, die auf das alte zwischengespeicherte Volume Gateway schreiben.
2. Trennen Sie die iSCSI-Volumes von allen Clients, die sie verwenden, oder heben Sie die Bereitstellung dieser Volumes auf. Dies trägt dazu bei, dass die Daten auf diesen Volumes konsistent bleiben, indem verhindert wird, dass Clients Daten auf diesen Volumes ändern oder hinzufügen.
3. Führen Sie die folgenden Schritte aus, um einen Snapshot für Ihr Volume zu erstellen, und warten Sie dann, bis der Snapshot abgeschlossen ist.
 - a. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
 - b. Wählen Sie im Navigationsbereich zunächst Volumes und anschließend das Volume aus, von dem Sie den Snapshot erstellen möchten.
 - c. Wählen Sie für Aktionen Snapshot erstellen aus.
 - d. Geben Sie im Dialogfeld Snapshot erstellen die Beschreibung des Snapshots ein und wählen Sie anschließend Snapshot erstellen.

Ob der Snapshot erstellt wurde, können Sie durch die Verwendung der Konsole überprüfen. Wenn immer noch Daten auf das Volume hochgeladen werden, warten Sie, bis der Upload abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren. Wählen Sie die Snapshot-Links auf den Volumes aus, um den Snapshot-Status anzuzeigen und sich zu vergewissern, dass keine ausstehenden Snapshots vorliegen.

Weitere Informationen zum Überprüfen des Volume-Status finden Sie unter [Grundlagen zu Status und Übergängen bei Volumes](#). Informationen zum Status zwischengespeicherter Volumes finden Sie unter [Grundlagen zu Statusübergängen bei Cached-Volumes](#).

4. Führen Sie die folgenden Schritte aus, um das alte zwischengespeicherte Volume Gateway zu beenden:
 - a. Wählen Sie im Navigationsbereich Gateways und anschließend das alte zwischengespeicherte Volume 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. Notieren Sie sich die Gateway-ID, da sie in einem späteren Schritt benötigt wird.

Während das Gateway angehalten wird, sehen Sie möglicherweise eine Meldung mit dem Status des Gateways. Wenn das alte Gateway heruntergefahren wird, werden eine Meldung und die Schaltfläche Gateway starten auf der Registerkarte Details angezeigt. Wenn das Gateway heruntergefahren wird, lautet der Status des Gateways Herunterfahren.

- c. Fahren Sie die alte VM mithilfe der Hypervisor-Steuerelemente herunter. Weitere Informationen zum Herunterfahren einer Amazon-EC2-Instance finden Sie unter [Stoppen und Starten Ihrer Instances](#) im Amazon-EC2-Benutzerhandbuch für Windows-Instances. Weitere Informationen zum Herunterfahren einer KVM-, VMware- oder Hyper-V-VM finden Sie in Ihrer Hypervisor-Dokumentation.

Weitere Informationen zum Anhalten von Gateways finden Sie unter [Starten und Anhalten von Volume Gateway](#).

5. Trennen Sie alle Festplatten, einschließlich der Stammfestplatte, der Cache-Festplatten und der Upload-Pufferfestplatten, von der alten Gateway-VM.

Note

Notieren Sie sich die Volume-ID der Stammfestplatte sowie die Gateway-ID, die dieser Stammfestplatte zugeordnet ist. In einem späteren Schritt trennen Sie diese Festplatte vom neuen Storage-Gateway-Hypervisor. (Siehe Schritt 11.)

Wenn Sie eine Amazon-EC2-Instance als VM für Ihr zwischengespeichertes Volume Gateway verwenden, finden Sie weitere Informationen unter [Trennen eines Amazon-EBS-Volumes von einer Linux-Instance](#) im Amazon-EC2-Benutzerhandbuch für Linux-Instances. Informationen zum Trennen von Festplatten von einer KVM-, VMware- oder Hyper-V-VM finden Sie in der Dokumentation zu Ihrem Hypervisor.

- Erstellen Sie eine neue Storage-Gateway-Hypervisor-VM-Instance, aktivieren Sie sie jedoch nicht als Gateway. Weitere Informationen zum Erstellen einer neuen Storage-Gateway-Hypervisor-VM finden Sie unter [Einrichten eines Volume Gateways](#). Dieses neue Gateway nimmt die Identität des alten Gateways an.

Note

Fügen Sie der neuen VM keine Festplatten für den Cache oder den Upload-Puffer hinzu. Ihre neue VM verwendet dieselben Cache-Festplatten und Upload-Pufferfestplatten, die auch von der alten VM verwendet wurden.

- Ihre neue Storage-Gateway-Hypervisor-VM-Instance sollte dieselbe Netzwerkkonfiguration wie die alte VM verwenden. Die Standard-Netzwerkkonfiguration für das Gateway ist das Dynamic Host Configuration Protocol (DHCP). Mit dem DHCP wird Ihr Gateway automatisch einer IP-Adresse zugewiesen.

Wenn Sie eine statische IP-Adresse für Ihre neue VM manuell konfigurieren müssen, finden Sie weitere Informationen unter [Konfigurieren Ihres Gateway-Netzwerks](#). Wenn Ihr Gateway einen SOCKS5-Proxy (Socket Secure Version 5) verwenden muss, um eine Internetverbindung herzustellen, finden Sie weitere Informationen unter [Weiterleiten Ihres lokalen Gateways über einen Proxy](#).

- Starten Sie die neue VM.
- Fügen Sie die Festplatten, die Sie in Schritt 5 von der alten zwischengespeicherten Volume-Gateway-VM getrennt haben, an das neue zwischengespeicherte Volume Gateway an. Fügen

Sie sie in derselben Reihenfolge an die neue Gateway-VM an, in der sie sich auf der alten Gateway-VM befinden.

Alle Festplatten müssen den Übergang unverändert durchlaufen. Ändern Sie die Volume-Größen nicht, da dadurch die Metadaten inkonsistent werden.

10. Initiieren Sie den Gateway-Migrationsprozess, indem Sie mit einer URL im folgenden Format eine Verbindung mit der neuen VM herstellen.

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

Sie können dieselbe IP-Adresse, die Sie für die alte Gateway-VM verwendet haben, für die neue Gateway-VM wiederverwenden. Ihre URL sollte ähnlich wie das folgende Beispiel aussehen.

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

Verwenden Sie diese URL in einem Browser oder über die Befehlszeile mit `curl`, um den Migrationsprozess zu starten.

Wenn der Gateway-Migrationsprozess erfolgreich initiiert wurde, wird die folgende Meldung angezeigt:

```
Successfully imported Storage Gateway information. Please refer to Storage Gateway documentation to perform the next steps to complete the migration.
```

11. Trennen Sie die Stammfestplatte des alten Gateways, deren Volume-ID Sie in Schritt 5 notiert haben.
12. Starten Sie das Gateway.

Führen Sie die folgenden Schritte aus, um das neue zwischengespeicherte Volume Gateway zu starten:

- a. Öffnen Sie die Storage-Gateway-Konsole unter <https://console.aws.amazon.com/storagegateway/home>.
- b. Wählen Sie im Navigationsbereich Gateways und wählen Sie dann das zu startende Gateway. Der Status des Gateways ist Shutdown (Herunterfahren).
- c. Wählen Sie Details und dann Gateway starten aus.

Weitere Informationen zum Starten von Gateways finden Sie unter [Starten und Anhalten von Volume Gateway](#).

13. Ihre Volumes sollten jetzt für Ihre Anwendungen unter der IP-Adresse der neuen Gateway-VM verfügbar sein.
14. Vergewissern Sie sich, dass Ihre Volumes verfügbar sind, und löschen Sie die alte Gateway-VM. Informationen zum Löschen einer VM finden Sie in der Dokumentation zu Ihrem 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](#)
- [Dimensionen für Storage Gateway-Metriken](#)
- [Überwachen des Upload-Puffers](#)
- [Überwachen des Cache-Speichers](#)
- [Grundlegendes zu CloudWatch Alarmen](#)
- [Erstellen empfohlener CloudWatch Alarme für Ihr Gateway](#)
- [Erstellen eines benutzerdefinierten CloudWatch Alarms für Ihr Gateway](#)
- [Überwachen des Volume Gateways](#)

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-Metriken 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	<p>Anzahl der vom Gateway generierten Zustandsbenachrichtigungen im Zusammenhang mit der Verfügbarkeit.</p> <p>Verwenden Sie diese Metrik zusammen mit der Statistik <code>Sum</code>, um zu beobachten, ob Ereignisse im Zusammenhang mit der Verfügbarkeit im Gateway auftreten.</p> <p>Weitere Informationen zu den Ereignissen finden Sie in Ihrer konfigurierten CloudWatch Protokollgruppe.</p> <p>Einheit: Zahl</p>	

Metrik	Beschreibung	
CacheHitPercent	<p>Prozentsatz der Lesevorgänge einer Anwendung, die aus dem Cache abgearbeitet wurden. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Einheit: Prozent</p>	
CacheUsed	<p>Gesamtanzahl der im Gateway-Cache-Speicher verwendeten Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Einheit: Byte</p>	
IoWaitPercent	<p>Prozentsatz der Zeit, die das Gateway auf eine Antwort vom lokalen Datenträger wartet.</p> <p>Einheit: Prozent</p>	
MemTotalBytes	<p>Menge an RAM, das für die Gateway-VM bereitgestellt wird, in Bytes.</p> <p>Einheit: Byte</p>	
MemUsedBytes	<p>Menge an RAM, das derzeit von der Gateway-VM verwendet wird, in Bytes.</p> <p>Einheit: Byte</p>	

Metrik	Beschreibung	
QueuedWrites	<p>Die Anzahl der Bytes, die darauf warten, in geschrieben zu werden AWS, die am Ende des Benachrichtigungszeitraums für alle Volumes im Gateway erfasst werden. Diese Bytes werden in Ihrem Gateway-Arbeitsspeicher gespeichert.</p> <p>Einheit: Byte</p>	
ReadBytes	<p>Die Gesamtzahl der Bytes, die in Ihren lokalen Anwendungen im Berichtszeitraum für alle Volumes im Gateway gelesen wurden.</p> <p>Verwenden Sie diese Metrik mit der Sum-Statistik, um den Durchsatz zu messen, und mit der Samples-Statistik, um die IOPS-Werte zu messen.</p> <p>Einheit: Byte</p>	

Metrik	Beschreibung	
ReadTime	<p>Die Gesamtzahl der Millisekunden, die für Leseoperationen in Ihren lokalen Anwendungen im Berichtszeitraum für alle Volumes im Gateway aufgewendet wurden.</p> <p>Verwenden Sie diese Metrik mit der Average-Statistik, um die Latenz zu messen.</p> <p>Einheit: Millisekunden</p>	
TimeSinceLastRecoveryPoint	<p>Die Zeit seit dem letzten verfügbaren Wiederherstellungspunkt. Weitere Informationen finden Sie unter Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen.</p> <p>Einheit: Sekunden</p>	
TotalCacheSize	<p>Die Gesamtgröße des Cache in Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Einheit: Byte</p>	
UploadBufferPercentageUsed	<p>Prozentuale Nutzung des Gateway-Upload-Puffers. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Einheit: Prozent</p>	

Metrik	Beschreibung	
UploadBufferUsed	<p>Gesamtanzahl der im Gateway-Upload-Puffer verwendeten Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen</p> <p>.</p> <p>Einheit: Byte</p>	
UserCpuPercent	<p>Prozentsatz der CPU-Zeit, die für die Gateway-Verarbeitung aufgewendet wurde, gemittelt über alle Kerne.</p> <p>Einheit: Prozent</p>	
WorkingStorageFree	<p>Die Gesamtmenge des nicht verwendeten Speicherplatzes im Gateway-Arbeitsspeicher. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Einheit: Byte</p>	
WorkingStoragePercentUsed	<p>Prozentuale Nutzung des Gateway-Upload-Puffers. Die Stichprobe wird am Ende des Berichtszeitraums entnommen</p> <p>.</p> <p>Einheit: Prozent</p>	

Metrik	Beschreibung	
WorkingStorageUsed	<p>Gesamtanzahl der im Gateway-Upload-Puffer verwendeten Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Einheit: Byte</p>	
WriteBytes	<p>Die Gesamtzahl der Byte, die in Ihren lokalen Anwendungen im Berichtszeitraum für alle Volumes im Gateway geschrieben wurden.</p> <p>Verwenden Sie diese Metrik mit der Sum-Statistik, um den Durchsatz zu messen, und mit der Samples-Statistik, um die IOPS-Werte zu messen.</p> <p>Einheit: Byte</p>	
WriteTime	<p>Die Gesamtzahl der Millisekunden, die für Schreiboperationen in Ihren lokalen Anwendungen im Berichtszeitraum für alle Volumes im Gateway aufgewendet wurden.</p> <p>Verwenden Sie diese Metrik mit der Average-Statistik, um die Latenz zu messen.</p> <p>Einheit: Millisekunden</p>	

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	<p>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 .</p> <p>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.</p>
VolumeId	<p>Diese Dimension filtert die angeforderten Daten nach Volume-spezifischen Metriken. Identifizieren Sie ein zu verwenden des Speicher-Volume mithilfe des Werts VolumeId. Weitere Informationen zur Verwendung von Volume-Metriken finden Sie unter Messung der Leistung zwischen Ihrer Anwendung und Ihrem Gateway.</p>

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 Volume Gateway \(Architektur\)](#).

Note

Die Metriken `WorkingStoragePercentUsed`, `WorkingStorageUsed` und `WorkingStorageFree` stellen den Upload-Puffer für gespeicherte Volumes nur bis zur Freigabe des 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 <code>UploadBufferPercentUsed</code> , <code>UploadBufferUsed</code> und <code>UploadBufferFree</code> mit der Statistik <code>Average</code> . Verwenden Sie z. B. <code>UploadBufferUsed</code> mit der <code>Average</code> -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 Alarm erstellen die Dimension `AWS/StorageGateway:GatewayId,GatewayName` 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 Volume Gateway \(Architektur\)](#).

Interessierendes Element	Methode zum Messen
Gesamtnutzung des Caches	<p>Verwenden Sie die Metriken <code>CachePercentUsed</code> und <code>TotalCacheSize</code> mit der Statistik <code>Average</code>. Verwenden Sie z. B. <code>CachePercentUsed</code> mit der <code>Average</code>-Statistik für die Analyse der Cache-Nutzung über einen Zeitraum.</p> <p>Die <code>TotalCacheSize</code> -Metrik ändert sich nur, wenn Sie Cache zum Gateway hinzufügen.</p>
Prozentsatz der aus dem Cache bedienten Leseanfragen	<p>Verwenden Sie die <code>CacheHitPercent</code> -Metrik mit der <code>Average</code>-Statistik.</p> <p>In der Regel soll <code>CacheHitPercent</code> auf einem hohen Wert bleiben.</p>
Prozentsatz des Cache, der nicht mehr aktuell ist, d. h., er enthält Inhalte, die nicht in hochgeladen wurden AWS	<p>Verwenden Sie die <code>CachePercentDirty</code> -Metrik mit der <code>Average</code>-Statistik.</p> <p>In der Regel soll <code>CachePercentDirty</code> auf einem niedrigen Wert bleiben.</p>

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 Metrics` 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 Volume Gateway verwendet werden, finden Sie unter [Grundlegendes zu Gateway-Metriken](#) und [Grundlegendes zu Volume-Metriken](#). 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 verfügbaren 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 Volume 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 deaktivieren
- `cloudwatch:EnableAlarmActions` – Alarmaktionen aktivieren
- `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 verwendet 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 des Volume Gateways

In diesem Abschnitt wird beschrieben, wie Sie ein Gateway in einer Konfiguration mit zwischengespeicherten oder gespeicherten Volumes überwachen, einschließlich der Überwachung der dem Gateway zugeordneten Volumes oder Bänder und der Überwachung des Upload-Puffers. Sie verwenden die AWS Management Console, um Metriken 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. Ausführliche Informationen zu CloudWatch finden Sie im [Amazon- CloudWatch Benutzerhandbuch](#).

Themen

- [Abrufen von Volume Gateway-Zustandsprotokollen mit Amazon CloudWatch Logs](#)
- [Verwenden von Amazon CloudWatch Metrics](#)

- [Messung der Leistung zwischen Ihrer Anwendung und dem Gateway](#)
- [Messung der Leistung zwischen Ihrem Gateway und AWS](#)
- [Grundlagen zu Volumen-Metriken](#)

Abrufen von Volume Gateway-Zustandsprotokollen mit Amazon CloudWatch Logs

Sie können Amazon CloudWatch Logs verwenden, um Informationen über den Zustand Ihres Volume Gateways und verwandter Ressourcen zu erhalten. Sie können diese 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 Cluster bereitgestellt wird, der mit VMware High Availability (HA) aktiviert ist, 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 Volume 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 [Fehlerbehebung bei Volume-Problemen](#).

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 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 linken 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 linken 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 Amazon CloudWatch-Konsole geöffnet.

Verwenden von Amazon CloudWatch Metrics

Sie können Überwachungsdaten für Ihr Gateway entweder über die AWS Management Console oder die CloudWatch API abrufen. Die Konsole zeigt eine Reihe von Diagrammen an, die auf den Rohdaten der CloudWatch API basieren. Sie können die CloudWatch API auch über eines der [AWS Software Development Kits \(SDKs\)](#) oder die [Amazon CloudWatch -API-Tools](#) verwenden. Je nach Anforderungen können Sie entweder die in der Konsole angezeigten oder die mit der API aufgerufenen Graphen verwenden.

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

- Die zu verwendende Metrikdimension. Eine Dimension ist ein Name-Wert-Paar, mit dem Sie eine Metrik eindeutig identifizieren. Die Dimensionen für Storage Gateway sind GatewayId, GatewayName und VolumeId. In der CloudWatch Konsole können Sie die Volume Metrics Ansichten Gateway Metrics und verwenden, um Gateway-spezifische und Volume-spezifische

Dimensionen einfach 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 Typen von Storage-Gateway-Metriken, die Sie verwenden können.

CloudWatch Namespace	Dimension	Beschreibung
AWS/StorageGateway	GatewayId , GatewayName	<p>Diese Dimensionen filtern nach Metrikdaten, die Aspekte des Gateways beschreiben. Sie können ein zu verwendendes Gateway identifizieren, indem Sie die Dimensionen GatewayId und GatewayName angeben.</p> <p>Die Durchsatz- und Latenzdaten eines Gateways basieren auf sämtlichen Volumes im Gateway.</p> <p>Die Daten werden automatisch in 5-Minuten-Intervallen kostenlos zur Verfügung gestellt.</p>
	VolumeId	<p>Diese Dimension filtert nach Metrikdaten, die für ein Volume spezifisch sind. Identifizieren Sie ein zu verwendendes Volume mithilfe seiner VolumeId-Dimension.</p> <p>Die Daten werden automatisch in 5-Minuten-Intervallen kostenlos zur Verfügung gestellt.</p>

Das Arbeiten mit Gateway- und Volume-Metriken 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](#)

Messung der Leistung zwischen Ihrer Anwendung und dem Gateway

Datendurchsatz, Datenlatenz und Operationen pro Sekunde sind drei Maßzahlen, mit denen Sie die Leistung des Anwendungsspeichers, der Ihr Gateway verwendet, beurteilen können. Wenn Sie die richtige Aggregationsstatistik verwenden, können Sie diese Werte mit Storage-Gateway-Metriken messen.

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), die `Sum` -Statistik für den Datendurchsatz (Byte pro Sekunde) 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 Ihren Anwendungen und Gateways messen können.

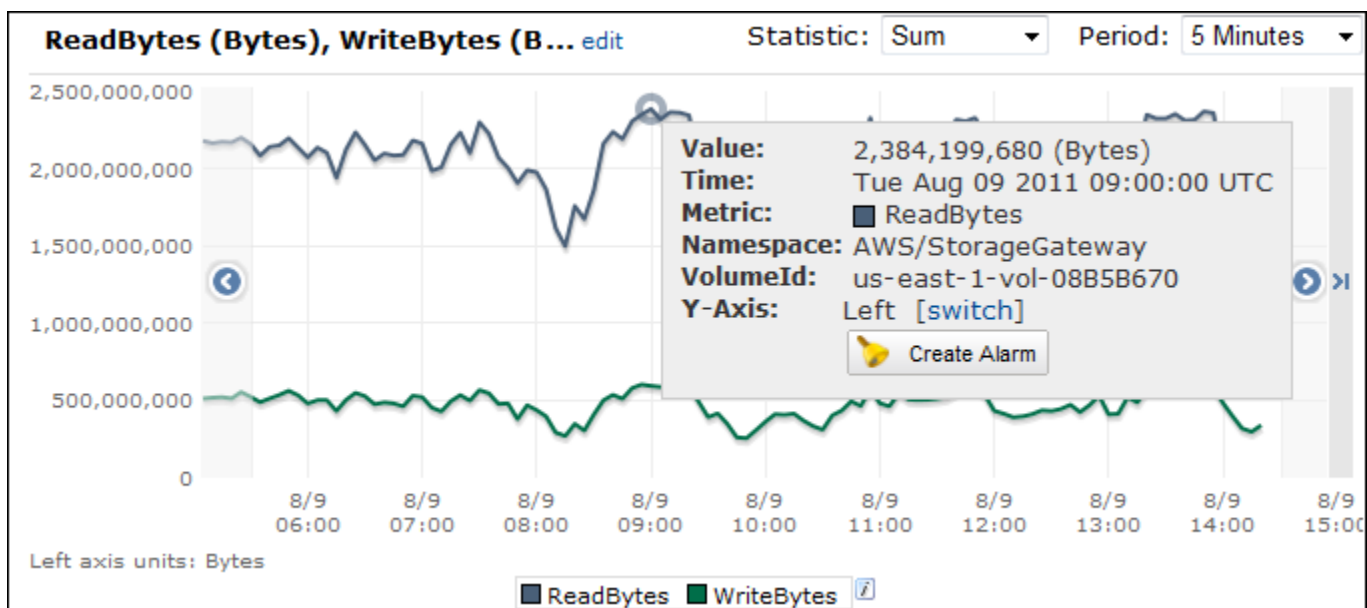
Interessierendes Element	Methode zum Messen
Durchsatz	Verwenden Sie die Metriken <code>ReadBytes</code> und <code>WriteBytes</code> mit der Statistik <code>Sum</code> CloudWatch . Beispiel: Mit dem <code>Sum</code> -Wert der <code>ReadBytes</code> -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie den Durchsatz als Rate in Byte pro Sekunde.
Latency	Verwenden Sie die Metriken <code>ReadTime</code> und <code>WriteTime</code> mit der Statistik <code>Average</code> CloudWatch . Beispiel: Der <code>Average</code> -Wert der <code>ReadTime</code> -Metrik gibt die Latenz pro Operation über den Stichprobenzeitraum an.
IOPS	Verwenden Sie die Metriken <code>ReadBytes</code> und <code>WriteBytes</code> mit der Statistik <code>Samples</code> CloudWatch . Beispiel: Mit dem <code>Samples</code> -Wert der <code>ReadBytes</code> -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie IOPS.

Für die Diagramme der durchschnittlichen Latenz und der durchschnittlichen Größe wird der Durchschnitt über die Gesamtzahl der Operationen (Lese- oder Schreiboperationen, je nachdem, welcher Wert für das Diagramm gilt) berechnet, die während des Zeitraums abgeschlossen wurden.

So messen Sie den Datendurchsatz von einer Anwendung zu einem Volume

1. Öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Volume-Metriken aus und suchen Sie das Volume, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metriken ReadBytes und WriteBytes 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 den resultierenden zeitlich sortierten Gruppen von Datenpunkten (eine für ReadBytes und eine für WriteBytes) jeden Datenpunkt durch den Zeitraum (in Sekunden), um den Durchsatz an dem Stichprobenpunkt zu erhalten. Der gesamte Durchsatz ist die Summe der Durchsätze.

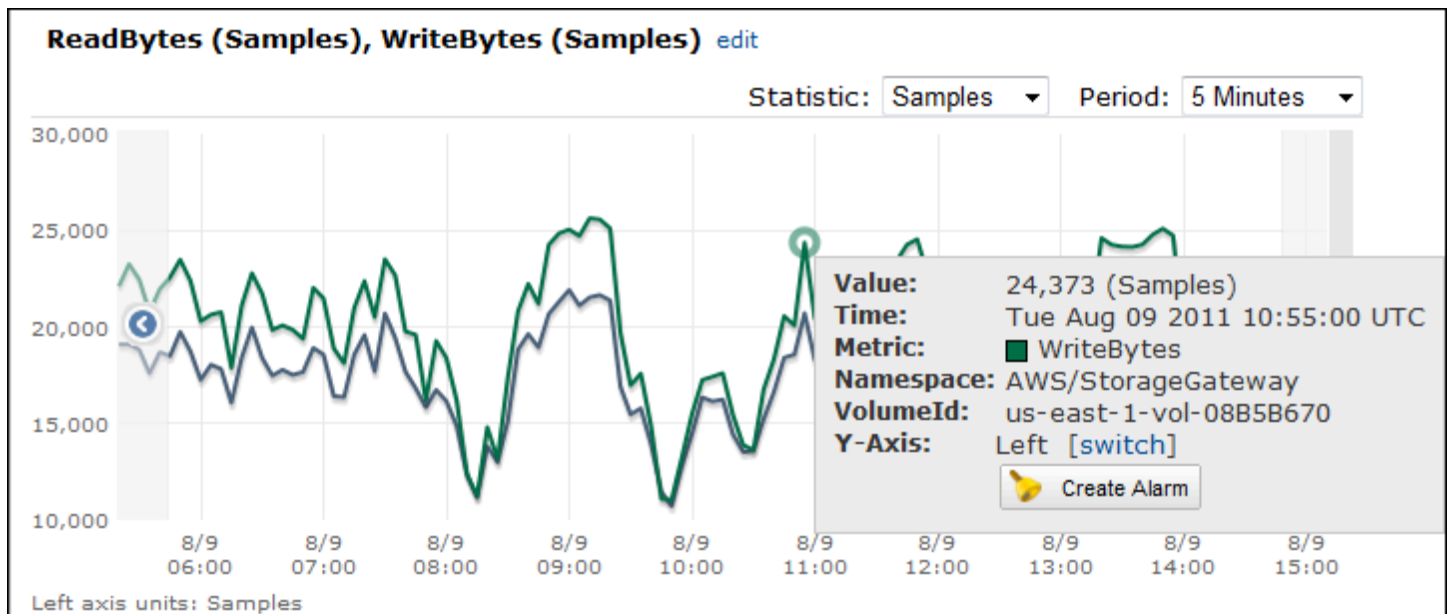
In der folgenden Abbildung sind die Metriken ReadBytes und WriteBytes für ein Volume mit der Sum-Statistik dargestellt. In der Abbildung zeigt der Cursor über einem Datenpunkt Informationen zu dem Datenpunkt wie den Wert und die Anzahl von Bytes an. Teilen Sie den Bytes-Wert durch den Wert für Period (Zeitraum)(5 Minuten), um den Datendurchsatz an diesem Stichprobenpunkt zu erhalten. Für den hervorgehobenen Punkt ist der Lesedurchsatz 2.384.199.680 Byte dividiert durch 300 Sekunden, was 7,6 MB pro Sekunde entspricht.



So messen Sie die Ein-/Ausgabeoperationen von Daten pro Sekunde von einer Anwendung zu einem Volume

1. Öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Volume-Metriken aus und suchen Sie das Volume, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metriken ReadBytes und WriteBytes aus.
5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die Samples-Statistik aus.
7. Wählen Sie für Zeitraum einen Wert von 5 Minuten oder mehr.
8. Dividieren Sie in den resultierenden zeitlich sortierten Gruppen von Datenpunkten (eine für ReadBytes und eine für WriteBytes) jeden Datenpunkt durch den Zeitraum (in Sekunden), um IOPS zu erhalten.

In der folgenden Abbildung sind die Metriken ReadBytes und WriteBytes für ein Speicher-Volume mit der Samples-Statistik dargestellt. In der Abbildung zeigt der Cursor über einem Datenpunkt Informationen zu dem Datenpunkt wie den Wert und die Anzahl von Stichproben an. Teilen Sie den Stichprobenwert durch den Wert für Period (Zeitraum) (5 Minuten), um die Operationen pro Sekunde an diesem Stichprobenpunkt zu erhalten. Für den hervorgehobenen Punkt ist die Anzahl von Schreiboperationen 24.373 Byte dividiert durch 300 Sekunden, was 81 Schreiboperationen pro Sekunde entspricht.



Messung der Leistung zwischen Ihrem Gateway und AWS

Datendurchsatz, Datenlatenz und Operationen pro Sekunde sind drei Maßzahlen, mit denen Sie die Leistung des Anwendungsspeichers, der Storage Gateway verwendet, beurteilen können. Diese drei Werte können mit den Storage-Gateway-Metriken gemessen werden, die für Sie bereitgestellt werden, wenn Sie die richtige Aggregationsstatistik verwenden. In der folgenden Tabelle werden die Metriken und die entsprechenden Statistiken zusammengefasst, mit denen Sie Durchsatz, Latenz und Eingabe-/Ausgabevorgänge pro Sekunde (IOPS) zwischen Ihrem Gateway und AWS messen können.

Interessierendes Element	Methode zum Messen
Durchsatz	Verwenden Sie die Metriken <code>ReadBytes</code> und <code>WriteBytes</code> mit der Statistik <code>Sum</code> CloudWatch . Beispiel: Mit dem <code>Sum</code> -Wert der <code>ReadBytes</code> -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie den Durchsatz als Rate in Byte pro Sekunde.
Latency	Verwenden Sie die Metriken <code>ReadTime</code> und <code>WriteTime</code> mit der Statistik <code>Average</code> CloudWatch . Beispiel: Der <code>Average</code> -Wert der <code>ReadTime</code> -Metrik gibt die Latenz pro Operation über den Stichprobenzeitraum an.
IOPS	Verwenden Sie die Metriken <code>ReadBytes</code> und <code>WriteBytes</code> mit der Statistik <code>Samples</code> CloudWatch . Beispiel: Mit dem <code>Samples</code> -Wert der

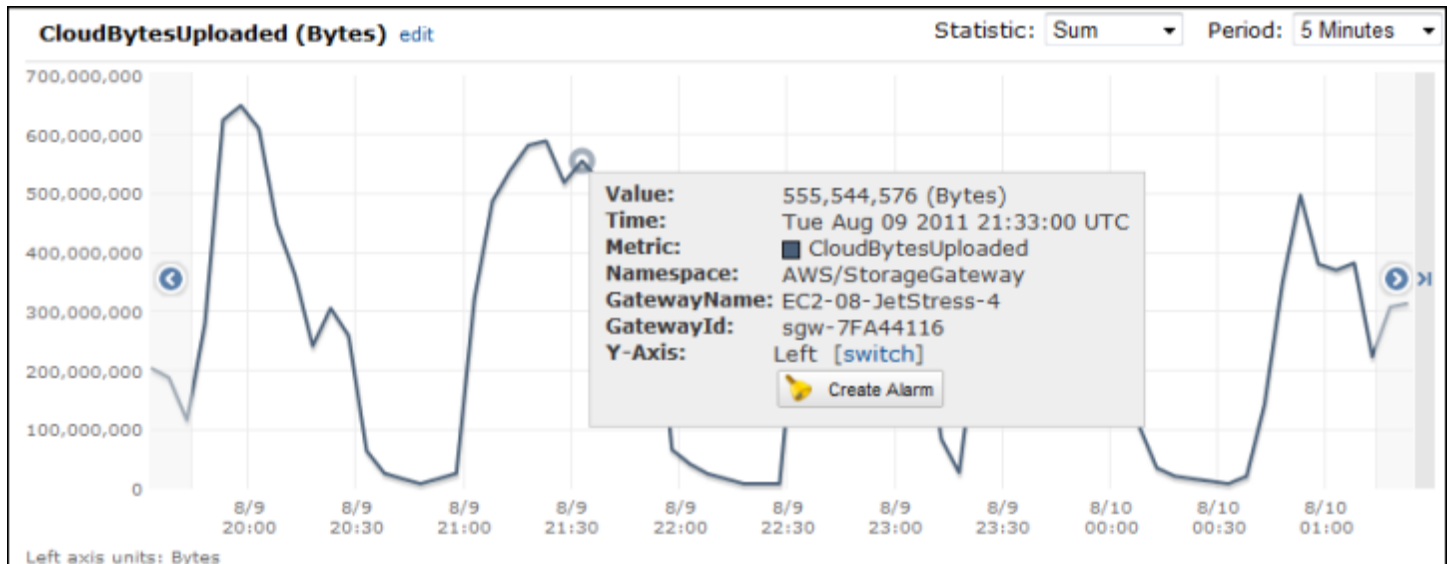
Interessierendes Element	Methode zum Messen
	ReadBytes -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie IOPS.
Durchsatz zu AWS	Verwenden Sie die CloudBytesUploaded Metriken CloudByte sDownloaded und mit der Sum - CloudWatch Statistik. Der Sum Wert der CloudBytesDownloaded Metrik über einen Stichprobenzeitraum von 5 Minuten geteilt durch 300 Sekunden gibt Ihnen beispielsweise den Durchsatz vom AWS zum Gateway als Byte pro Sekunde.
Latenz der Daten in AWS	Verwenden Sie die CloudDownloadLatency -Metrik mit der Average- Statistik. Beispiel: Die Average-Statistik der CloudDownloadLaten cy -Metrik gibt die Latenz pro Operation an.

So messen Sie den Upload-Datendurchsatz von einem Gateway zu AWS

1. Öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Gateway-Metriken aus und suchen Sie das Volume, 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-Volume mit der Statistik Sum dargestellt. In der Abbildung zeigt der Cursor über einem Datenpunkt Informationen zu dem Datenpunkt wie den Wert und die hochgeladenen 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 Gateway zu 555.544.576 Byte geteilt durch 300 Sekunden, was 1,7 Megabyte pro Sekunde entspricht.



So messen Sie die Latenz pro Operation eines Gateways

1. Öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Gateway-Metriken aus und suchen Sie das Volume, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metriken ReadTime und WriteTime 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.
8. Addieren Sie in der resultierenden zeitlich sortierten Gruppe von Punkten (eine für ReadTime und eine für WriteTime) die Datenpunkte der gleichen zeitlichen Stichprobe, um die gesamte Latenz in Millisekunden zu erhalten.

So messen Sie die Datenlatenz von einem Gateway zu AWS

1. Öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Gateway-Metriken aus und suchen Sie das Volume, 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 Gateways auf fest AWS

1. Öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Alarms (Alarmer).
3. Wählen Sie Alarm erstellen, um den Assistenten zum Erstellen von Alarmen zu starten.
4. Wählen Sie die Dimension Storage Gateway aus und suchen Sie das Gateway, mit dem Sie arbeiten möchten.
5. Wählen Sie die Metrik `CloudBytesUploaded` aus.
6. Zum Definieren des Alarms legen Sie den Alarmstatus fest, 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.
7. Konfigurieren Sie die auszuführenden Aktionen für den Alarmstatus. Sie können beispielsweise eine E-Mail-Benachrichtigung an sich selbst senden lassen.
8. 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 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.

Grundlagen zu Volumen-Metriken

Im Folgenden finden Sie Informationen zu den Storage-Gateway-Metriken, die ein Volume eines Gateways betreffen. Jedes Volume eines Gateways verfügt über eine Reihe von zugeordneten Metriken.

Einige Volume-spezifische Metriken haben denselben Namen wie bestimmte Gateway-spezifische Metriken. Diese Metriken stellen die gleichen Messungsarten dar, beziehen sich jedoch statt des Gateways auf das Volume. Geben Sie vor Beginn der Arbeit an, ob Sie mit einer Gateway-Metrik oder einer Volume-Metrik arbeiten möchten. Geben Sie beim Arbeiten mit Volume-Metriken die Volume-ID für das Speicher-Volume 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 Speicher-Volumes verwenden können.

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
AvailabilityNotification	Die Anzahl der vom Volume gesendeten Verfügbarkeitsbenachrichtigungen. Einheiten: Anzahl	Ja	Ja
CacheHitPercent	Prozentsatz der Anwendungsleseoper	Ja	Nein

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
	<p>ationen vom Volume aus dem Cache. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Wenn keine Anwendungsleseoperationen vom Volume vorhanden sind, wird dieser Metrikwert mit 100 % angegeben.</p> <p>Einheiten: Prozent</p>		

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
CachePercentDirty	<p>Der Anteil des Volumes am Gesamtprozentsatz des Gateway-Caches, der nicht für AWS beibehalten wurde. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Verwenden Sie die Metrik CachePercentDirty des Gateways, um den Gesamtprozentsatz des Gateway-Caches anzuzeigen, der nicht dauerhaft in AWS gespeichert wird. Weitere Informationen finden Sie unter Grundlagen zu Gateway-Metriken.</p> <p>Einheiten: Prozent</p>	Ja	Ja

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
CachePercentUsed	<p>Der Anteil des Volumes am Gesamtprozentsatz der Auslastung des Cache-Speichers des Gateways. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.</p> <p>Verwenden Sie die CachePercentUsed -Metrik des Gateways, um den Gesamtprozentsatz der Auslastung des Cache-Speichers des Gateways anzusehen. Weitere Informationen finden Sie unter Grundlagen zu Gateway-Metriken.</p> <p>Einheiten: Prozent</p>	Ja	Nein
CloudBytesDownloaded	<p>Die Anzahl der von der Cloud auf das Volume heruntergeladenen Byte.</p> <p>Einheiten: Byte</p>	Ja	Ja

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
CloudBytesUploaded	Die Anzahl der von der Cloud auf das Volume hochgeladenen Byte. Einheiten: Byte	Ja	Ja
HealthNotification	Die Anzahl der vom Volume gesendeten Zustandsbenachrichtigungen. Einheiten: Anzahl	Ja	Ja
IoWaitPercent	Der Prozentsatz der IoWaitPercent Einheiten, die derzeit vom Volume verwendet werden. Einheiten: Prozent	Ja	Ja
MemTotalBytes	Der Prozentsatz des Gesamtspeichers, der gegenwärtig vom Volume verwendet wird. Einheiten: Prozent	Ja	Nein

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
MemoryUsage	<p>Der Prozentsatz des Speichers, der gegenwärtig vom Volume verwendet wird.</p> <p>Einheiten: Prozent</p>	Ja	Nein
ReadBytes	<p>Die Gesamtzahl in Byte, die in Ihren lokalen Anwendungen im Berichtszeitraum gelesen wurde.</p> <p>Verwenden Sie diese Metrik mit der Sum-Statistik, um den Durchsatz zu messen, und mit der Samples-Statistik, um die IOPS-Werte zu messen.</p> <p>Einheiten: Byte</p>	Ja	Ja

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
ReadTime	<p>Die Gesamtzahl der Millisekunden, die im Berichtszeitraum für Leseoperationen in Ihren On-Premise-Anwendungen aufgewendet wurden.</p> <p>Verwenden Sie diese Metrik mit der Average-Statistik, um die Latenz zu messen.</p> <p>Einheiten: Millisekunden</p>	Ja	Ja
UserCpuPercent	<p>Der Prozentsatz der zugewiesenen CPU-Datenverarbeitungseinheiten, die gegenwärtig vom Volume verwendet werden.</p> <p>Einheiten: Prozent</p>	Ja	Ja

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
WriteBytes	<p>Die Gesamtzahl in Byte, die in Ihren lokalen Anwendungen im Berichtszeitraum geschrieben wurde.</p> <p>Verwenden Sie diese Metrik mit der Sum-Statistik, um den Durchsatz zu messen, und mit der Samples-Statistik, um die IOPS-Werte zu messen.</p> <p>Einheiten: Byte</p>	Ja	Ja
WriteTime	<p>Die Gesamtzahl der Millisekunden, die im Berichtszeitraum für Schreiboperationen in Ihren On-Premise-Anwendungen aufgewendet wurden.</p> <p>Verwenden Sie diese Metrik mit der Average-Statistik, um die Latenz zu messen.</p> <p>Einheiten: Millisekunden</p>	Ja	Ja

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
QueuedWrites	Die Anzahl der Bytes, die darauf warten, in geschrieben zu werden AWS, die am Ende des Benachrichtigungszeitraums erfasst werden. Einheiten: Byte	Ja	Ja

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](#)
- [Verwaltung von lokalen Festplatten für Ihr Storage Gateway](#)
- [Verwaltung der Bandbreite für Ihr Volume Gateway](#)
- [Verwalten von Gateway-Updates über die AWS Storage Gateway -Konsole](#)
- [Ausführen von Wartungsaufgaben in der lokalen Konsole](#)
- [Löschen des Gateways über die AWS Storage Gateway -Konsole und Bereinigen zugehöriger Ressourcen](#)

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 Volume Gateway

So beenden Sie ein Volume 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 Volume 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](#)
- [Bestimmen der Größe des zuzuordnenden Upload-Puffers](#)
- [Bestimmen der Größe des zuzuordnenden Cache-Speichers](#)
- [Konfigurieren zusätzlichen Upload-Puffers oder Cache-Speichers](#)

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:

- Volume Gateways:
 - Gespeicherte Gateways benötigen mindestens eine Festplatte als Upload-Puffer.
 - Cached-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 ermöglichen. 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.

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

Bei Volume Gateways wechselt das Volume in den Status PASS THROUGH, wenn der Upload-Puffer seine Kapazität erreicht. In diesem Status werden neue Daten, die Ihre Anwendung schreibt, lokal beibehalten, aber nicht AWS sofort in hochgeladen. Daher können Sie keine neuen Snapshots aufnehmen. Wenn Kapazität des Upload-Puffers frei wird, wechselt das Volume in den Status BOOTSTRAPPING. In diesem Status werden alle neuen Daten, die lokal beibehalten wurden, in hochgeladen AWS. Schließlich wechselt das Volume wieder zum Status AKTIV zurück. Storage Gateway setzt dann die normale Synchronisation der lokal gespeicherten Daten mit der in gespeicherten Kopie fort AWS und Sie können mit der Erstellung neuer Snapshots beginnen. Weitere Informationen zum Volume-Status finden Sie unter [Grundlagen zu Status und Übergängen bei Volumes](#).

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.

$$\left(\begin{array}{c} \text{Application} \\ \text{Throughput} \\ \text{(MB/s)} \end{array} - \begin{array}{c} \text{Network} \\ \text{Throughput} \\ \text{to AWS (MB/s)} \end{array} \right) \times \begin{array}{c} \text{Compression} \\ \text{Factor} \end{array} \times \begin{array}{c} \text{Duration} \\ \text{of writes} \\ \text{(s)} \end{array} = \begin{array}{c} \text{Upload} \\ \text{Buffer} \\ \text{(MB)} \end{array}$$

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

$$((40 \text{ MB/sec}) - (12 \text{ MB/sec} * 2)) * (12 \text{ hours} * 3600 \text{ seconds/hour}) = 691200 \text{ megabytes}$$

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 Speichieranforderungen 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.

Note

UPLOAD-PUFFER ist die einzige verfügbare Option für die Zuweisung von Festplatten auf Volume Gateways für gespeicherte Volumes.

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

Verwaltung der Bandbreite für Ihr Volume 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 angeben AWS Management Console, indem Sie die verwenden, oder programmgesteuert, indem Sie entweder die Storage Gateway-API (siehe [UpdateBandwidthRateLimit](#)) oder ein AWS Software Development Kit (SDK) verwenden. 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 von Gateway-Bandbreitenlimits 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 bandwidth.\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 bandwidth.\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 verwenden zu können, 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.

- 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-Konsolebefehlen	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	<p>Geben Sie die entsprechende Zahl ein, um SOCKS-Proxy konfigurieren auszuwählen.</p> <p>Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.</p>
Anzeigen der aktuellen SOCKS-Proxy-Konfiguration	<p>Geben Sie die entsprechende Zahl ein, um Aktuelle SOCKS-Proxykonfiguration anzeigen auszuwählen.</p> <p>Wenn kein SOCKS-Proxy konfiguriert ist, wird die Meldung <code>SOCKS Proxy not configured</code> angezeigt. Ist ein SOCKS-Proxy konfiguriert</p>

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	<p>Geben Sie die entsprechende Zahl ein, um Adapter beschreiben auszuwählen.</p> <p>Eine Liste der Adapternamen wird angezeigt, und Sie werden aufgefordert, einen Adapternamen einzugeben, z. B. eth0. Wenn der von Ihnen angegebene Adapter verwendet wird, werden die folgenden Informationen zum Adapter angezeigt:</p> <ul style="list-style-type: none">• Media Access Control-Adresse (MAC)• IP-Adresse• Netzmaske• Gateway-IP-Adresse• DHCP-aktivierter Status <p>Sie verwenden die hier aufgeführten Adapternamen, wenn Sie eine statische IP-Adresse konfigurieren oder den Standardadapter Ihres Gateways festlegen.</p>
Konfigurieren von DHCP	<p>Geben Sie die entsprechende Zahl ein, um DHCP konfigurieren auszuwählen.</p> <p>Sie werden aufgefordert, die Netzwerkschnittstelle für die Verwendung von DHCP zu konfigurieren.</p>

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren einer statischen IP-Adresse für Ihr Gateway	<p>Geben Sie die entsprechende Zahl ein, um Statische IP-Adresse konfigurieren auszuwählen.</p> <p>Sie werden aufgefordert, die folgenden Informationen zur Konfiguration einer statischen IP-Adresse einzugeben:</p> <ul style="list-style-type: none">• Netzwerkadaptername• IP-Adresse• Netzmaske• Standard-Gateway-Adresse• Primary Domain Name Service-Adresse (DNS)• Sekundäre DNS-Adresse <div data-bbox="829 1304 1511 1766" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>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.</p></div>

Zur Ausführung dieser Aufgabe	Vorgehensweise
	<p>Wenn Ihr Gateway mehrere Netzwerkschnittstellen verwendet, müssen Sie alle aktivierten Schnittstellen für die Verwendung von DHCP- oder statischen IP-Adressen einrichten.</p> <p>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.</p> <p>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.</p>

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren eines Hostnamens für Ihr Gateway	<p data-bbox="829 226 1438 310">Geben Sie die entsprechende Zahl ein, um Hostname konfigurieren auszuwählen.</p> <p data-bbox="829 352 1471 583">Sie werden aufgefordert, auszuwählen, ob das Gateway einen von Ihnen angegebenen statischen Hostnamen verwenden oder einen Namen automatisch über DHCP oder rDNS beziehen soll.</p> <div data-bbox="829 621 1507 1031" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p data-bbox="857 659 979 695"> Note</p><p data-bbox="906 716 1463 989">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.</p></div>

Zur Ausführung dieser Aufgabe	Vorgehensweise
Zurücksetzen der Netzwerkkonfiguration Ihres Gateways auf DHCP	<p>Geben Sie die entsprechende Zahl ein, um Alles auf DHCP zurücksetzen auszuwählen.</p> <p>Alle Netzwerkschnittstellen sind für die Verwendung von DHCP eingerichtet.</p> <div data-bbox="829 541 1507 999" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>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.</p></div>
Einrichten des Standard-Routing-Adapters Ihres Gateways	<p>Geben Sie die entsprechende Zahl ein, um Standardadapter festlegen auszuwählen.</p> <p>Die Adapter, die für Ihr Gateway verfügbar sind, werden angezeigt, und Sie werden aufgefordert, einen der Adapter auszuwählen, z. B. eth0.</p>
Anzeigen der DNS-Konfiguration Ihres Gateways	<p>Geben Sie die entsprechende Zahl ein, um DNS-Konfiguration anzeigen auszuwählen.</p> <p>Die IP-Adressen des primären und sekundären DNS-Namensservers werden angezeigt.</p>

Zur Ausführung dieser Aufgabe	Vorgehensweise
Anzeigen von Routing-Tabellen	<p>Geben Sie die entsprechende Zahl ein, um Routen anzeigen auszuwählen.</p> <p>Die Standard-Route Ihres Gateways wird angezeigt.</p>

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. <div data-bbox="834 1325 1507 1780" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>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.</p> </div>

Befehl	Funktion
ip	<p>Routing, Geräte und Tunnel anzeigen/manipulieren.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>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.</p> </div>
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.
tcptracert	Erfassen Sie die Traceroute-Ausgabe des TCP-Datenverkehrs zu einem Ziel.

- 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 Mindestanforderungen. Das Gateways funktioniert möglicherweise nicht ordnungsgemäß. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.

Die Konsole zeigt die Anzahl der Fehler und Warnungen neben der Menüoption für die Ressourcenprüfung an.

Konfigurieren von Networkadaptern für Ihr Gateway

Standardmäßig ist Storage Gateway für die Verwendung eines Networkadapters des Typs E1000 konfiguriert, aber Sie können Ihr Gateway auch für die Verwendung eines Networkadapters 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 Networkadapter.

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-Netzwerkadapertyp 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 Adapertyp 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.

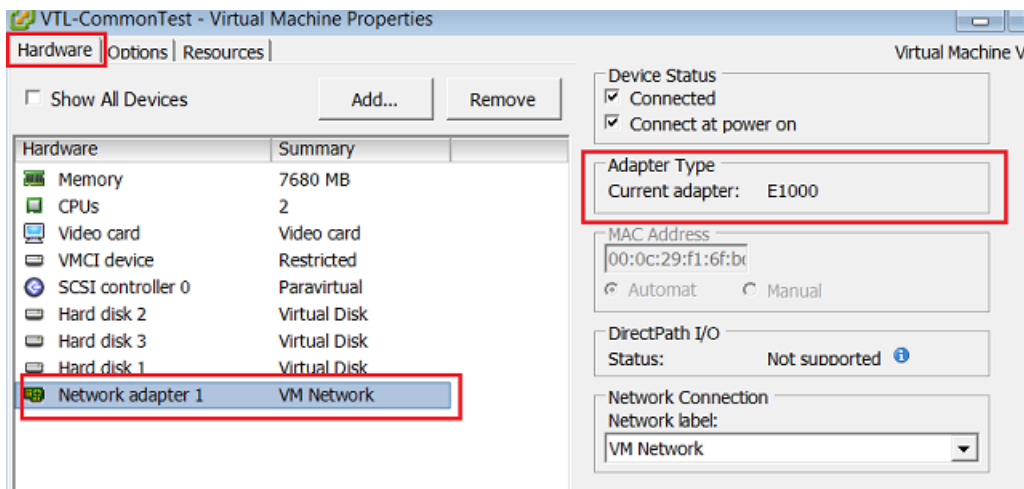
In den folgenden Abschnitten werden die Schritte beschrieben, mit denen Sie Ihr Gateway für die Verwendung eines VMXNET3-Adapter konfigurieren:

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, dass 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](#)
- [Weiterleitung des auf EC2 bereitgestellten Gateways über einen HTTP-Proxy](#)
- [Testen der Netzwerkkonnektivität Ihres Gateways](#)
- [Anzeigen des Gateway-Systemressourcen-Status](#)
- [Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole](#)

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-Konsolebefehlen	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
<code>[PASSED]</code> (<code>[BESTANDEN]</code>)	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 Ressourcenprüfung 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 konfigurieren.

Befehl	Funktion
	<p> Note</p> <p>Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren.</p>
ip	<p>Routing, Geräte und Tunnel anzeigen/manipulieren.</p> <p> Note</p> <p>Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren.</p>
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.

```
[[root@localhost vms]# virsh list
 Id   Name           State
-----
 7    SGW_KVM        running

[[root@localhost vms]# virsh console 7
```

2. Verwenden Sie den folgenden Befehl, um auf die lokale Konsole zuzugreifen.

```
# virsh console VM_Id
```

```
[[root@localhost vms]# virsh console 7
Connected to domain SGW_KVM
Escape character is ^]

AWS Appliance

Login to change your network configuration and other settings.
localhost login: _
```

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.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: 10.0.3.32
#####

1: HTTP/SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: License Information
7: Command Prompt

0: Get activation key

Press "x" to exit session

Enter command: _
```

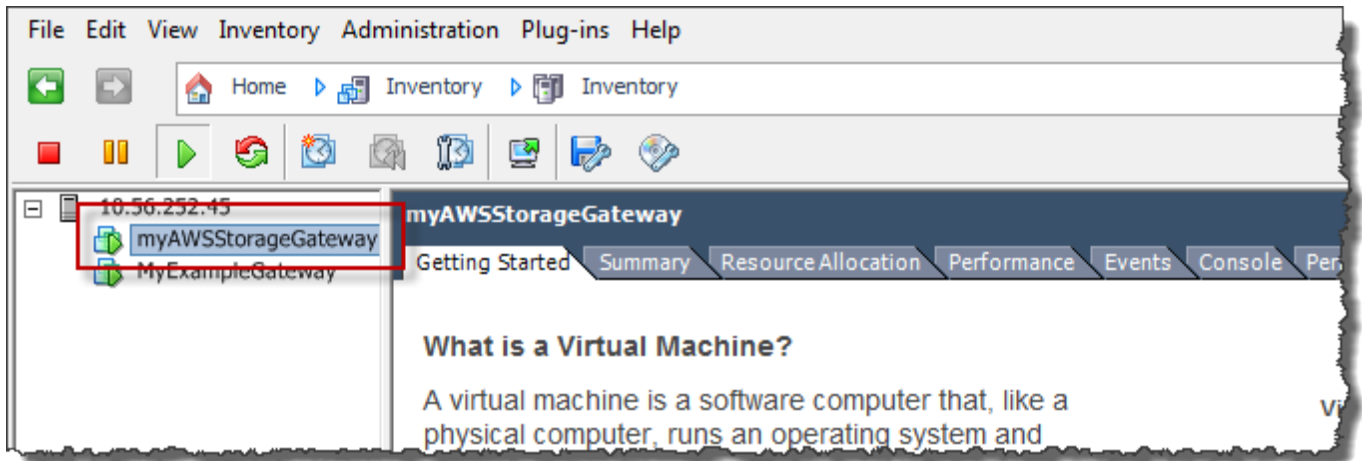
Zugreifen auf die lokale Konsole mit VMware ESXi

So greifen Sie mithilfe von VMware ESXi auf die lokale Konsole des Gateways zu

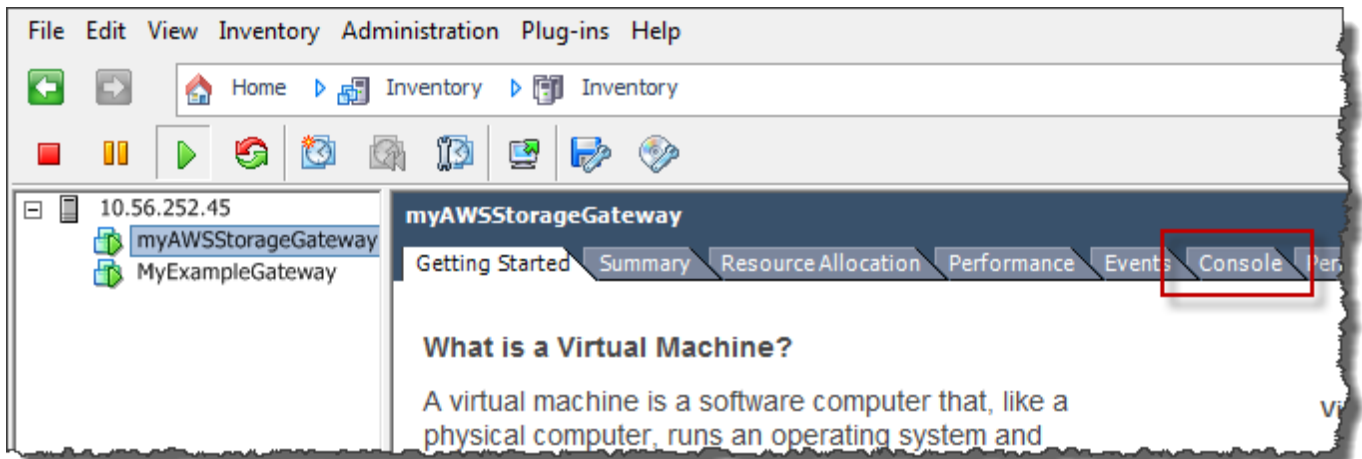
1. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM.
2. Stellen Sie sicher, dass das Gateway aktiviert ist.

Note

Wenn Ihre Gateway-VM aktiviert ist, erscheint wie im folgenden Screenshot dargestellt ein grünes Pfeilsymbol mit dem VM-Symbol. Wenn Ihre Gateway-VM nicht aktiviert ist, wählen Sie das Symbol Power On (Energie ein) im Menü Toolbar (Symbolleiste), um sie zu aktivieren.



3. Wählen Sie die Registerkarte Console (Konsole).



Nach einem kurzen Augenblick können Sie sich an die VM anmelden.

Note

Drücken Sie Ctrl+Alt (Strg+Alt), um den Mauszeiger aus dem Konsolenfenster freizugeben.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

- Um sich mit den Standard-Anmeldeinformationen anzumelden, fahren Sie mit dem Verfahren [Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen](#) fort.

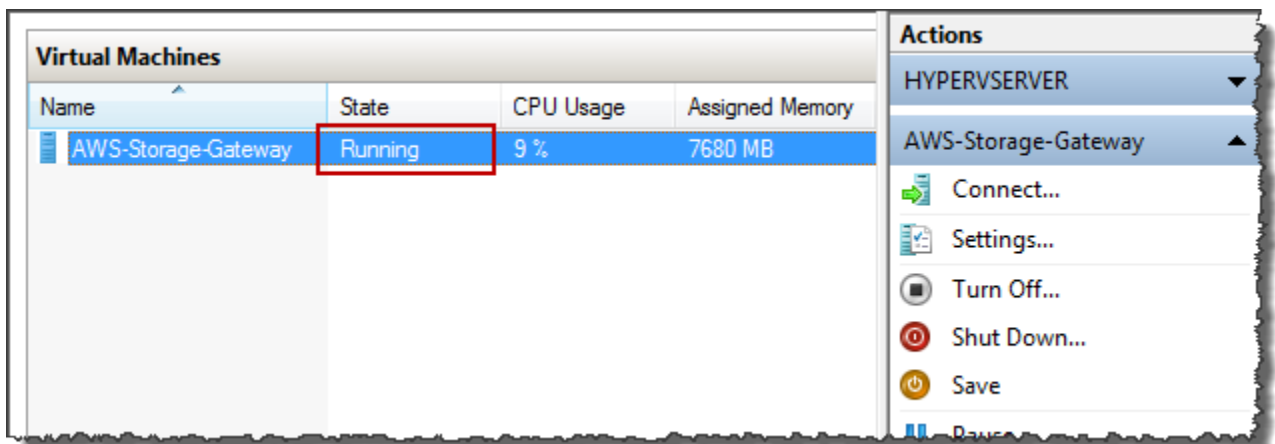
Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V

Zugreifen auf die lokale Gateway-Konsole (Microsoft Hyper-V)

- Wählen Sie in der Liste Virtual Machines (Virtuelle Maschinen) im Microsoft Hyper-V Manager Ihre Gateway-VM aus.
- Stellen Sie sicher, dass das Gateway aktiviert ist.

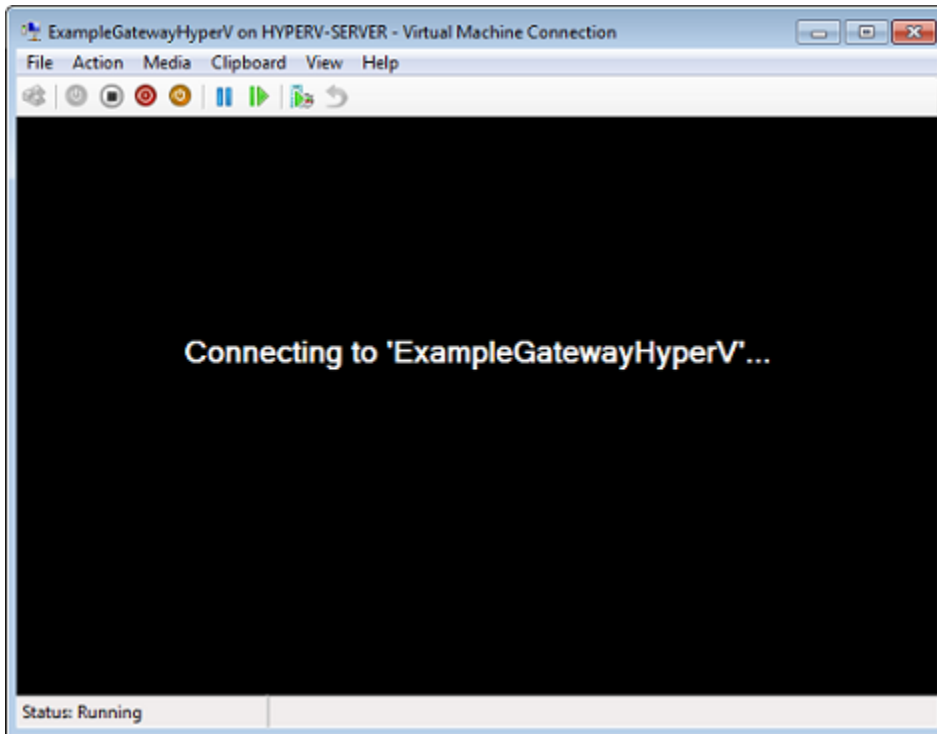
Note

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.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Um sich mit den Standard-Anmeldeinformationen anzumelden, fahren Sie mit dem Verfahren [Anmelden an der lokalen Konsole mit den Standard-Anmeldeinformationen](#) fort.

Konfigurieren von Networkadaptern für Ihr Gateway

In diesem Abschnitt finden Sie Informationen zum Konfigurieren von mehreren Networkadaptern für Ihr Gateway.

Themen

- [Konfigurieren des Gateways für mehrere NICs in einem VMware-ESXi-Host](#)
- [Konfigurieren des Gateways für mehrere NICs in einem Microsoft-Hyper-V-Host](#)

Konfigurieren des Gateways für mehrere NICs in einem VMware-ESXi-Host

Das folgende Verfahren setzt voraus, dass für Ihre Gateway-VM bereits ein Networkadapter definiert wurde und beschreibt, wie Sie einen Adapter unter VMware ESXi hinzufügen.

So konfigurieren Sie das Gateway für einen zusätzlichen Networkadapter 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 Networkadapters.
 - 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](#) .

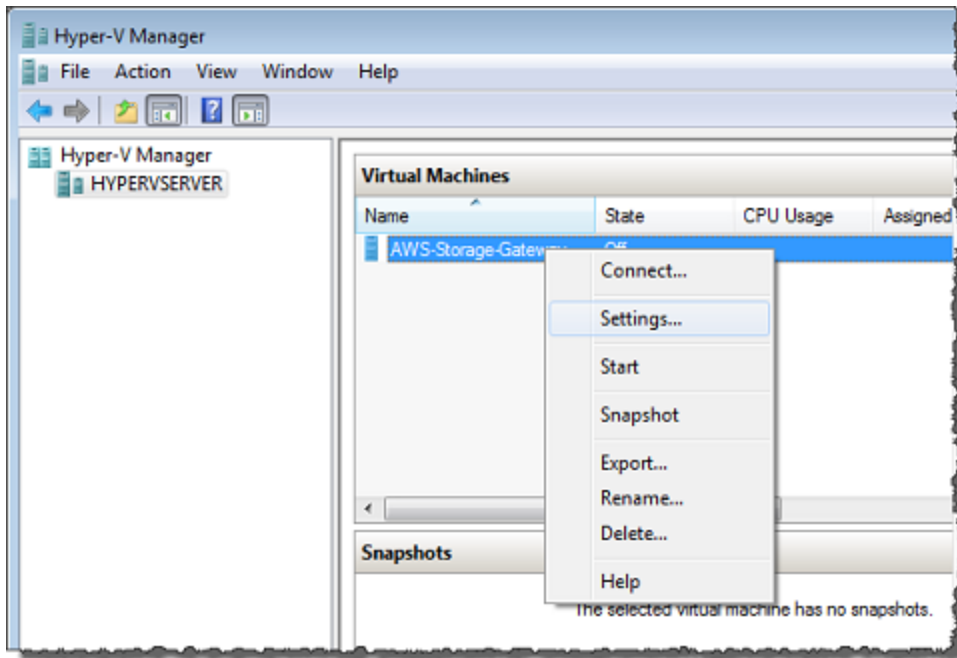
Konfigurieren des Gateways für mehrere NICs in einem Microsoft-Hyper-V-Host

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 gezeigt, wie Sie einen Adapter für einen Microsoft Hyper-V-Host hinzufügen.

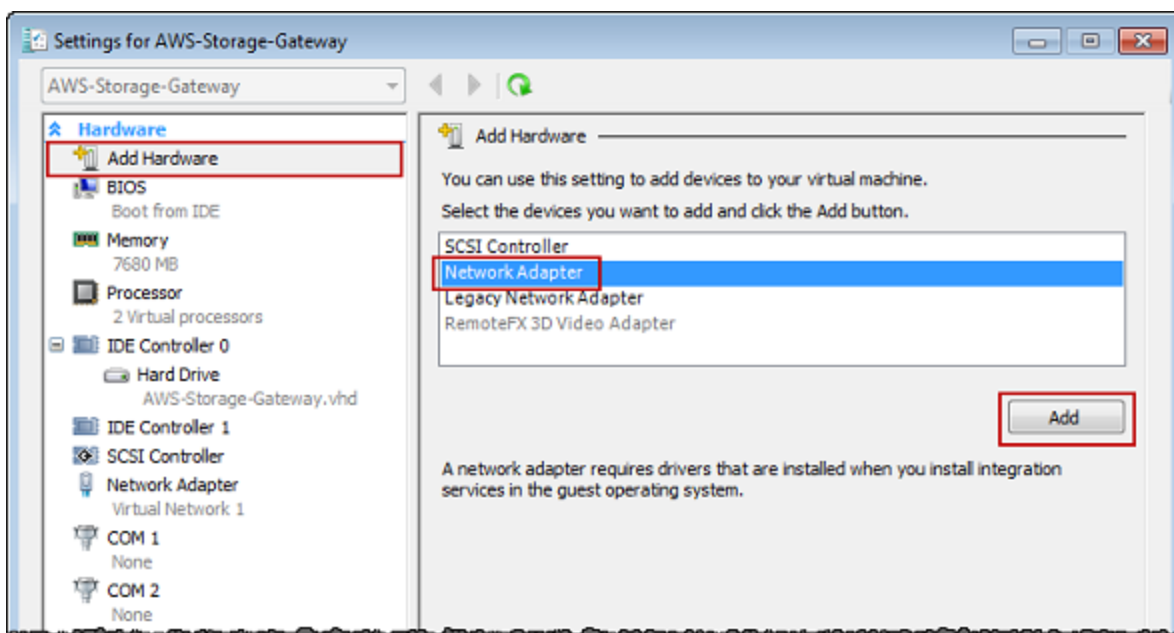
So konfigurieren Sie Ihr Gateway für einen zusätzlichen Netzwerkadapter in einem Microsoft Hyper-V-Host

1. Schalten Sie in der Storage-Gateway-Konsole das Gateway aus. Anweisungen finden Sie unter [So beenden Sie ein Volume Gateway](#).
2. Wählen Sie im Microsoft Hyper-V Manager Ihre 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).

- Öffnen Sie im Client das Kontextmenü für Ihre Gateway-VM und wählen Sie Settings (Einstellungen).

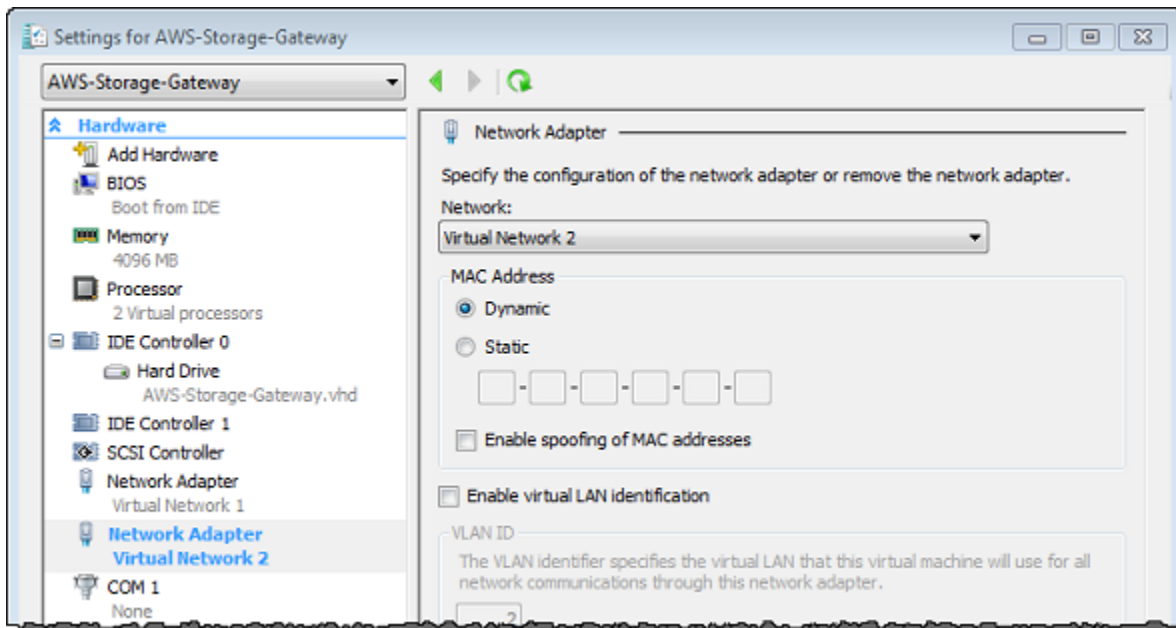


- Wählen Sie im Dialogfeld Settings (Einstellungen) der VM für Hardware die Option Add Hardware (Hardware hinzufügen).
- Wählen Sie im Fenster Add Hardware (Hardware hinzufügen) die Option Network Adapter (Netzwerkadapter) und anschließend Add (Hinzufügen), um ein Gerät hinzuzufügen.



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 Volume 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.

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 Bestätigungsdiaologfeld 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 Volume Gateway

Wenn das Gateway, das Sie löschen möchten, auf einer virtuellen Maschine (VM) bereitgestellt ist, sollten Sie die folgenden Aktionen ausführen, um die Ressourcen zu bereinigen:

- Löschen Sie das Gateway. Anweisungen finden Sie unter [Löschen eines Gateways mithilfe der Storage-Gateway-Konsole](#).
- Löschen Sie alle Amazon EBS-Snapshots, die Sie nicht benötigen. Weitere Informationen finden Sie unter [Löschen eines Amazon-EBS-Snapshots](#) im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

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 aus auf Amazon EC2 bereitgestellten Cached-Volumes

Wenn Sie ein Gateway mit Cached-Volumes auf EC2 bereitgestellt haben, schlagen wir vor, dass Sie die folgenden Schritte ausführen, um das Gateway zu löschen und seine Ressourcen zu bereinigen:

1. Löschen Sie das Gateway in der Storage-Gateway-Konsole wie unter [Löschen eines Gateways mithilfe der Storage-Gateway-Konsole](#) gezeigt.
2. Stoppen Sie in der Amazon-EC2-Konsole die EC2-Instance, wenn Sie die Instance erneut verwenden möchten. Andernfalls beenden Sie die Instance. Wenn Sie das Löschen von Volumes

planen, notieren Sie sich die Blockgeräte, die der Instance zugeordnet sind, sowie die Geräte-IDs, bevor Sie die Instance beenden. Diese benötigen Sie zur Identifizierung der Volumes, die Sie löschen möchten.

3. Entfernen Sie in der Amazon-EC2-Konsole alle Amazon-EBS-Volumes, die der Instance zugeordnet sind, wenn Sie sie nicht erneut verwenden möchten. Weitere Informationen finden Sie unter [Bereinigungen von Instances und Volumes](#) im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Leistung

In diesem Abschnitt wird die Leistung von Storage Gateway beschrieben.

Themen

- [Optimieren der Gateway-Leistung](#)
- [Verwenden von VMware vSphere High Availability mit Storage Gateway](#)

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 24 dedizierte physische CPU-Kerne
- Für ein Volume 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
- Festplatte 1, die wie folgt als Gateway-Cache verwendet werden soll:
 - SSD unter Verwendung eines NVMe Controllers
- Festplatte 2, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
 - SSD unter Verwendung eines NVMe Controllers
- Festplatte 3, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
 - SSD unter Verwendung eines NVMe Controllers
- Netzwerkadapter 1 auf VM Netzwerk 1 konfiguriert:
 - Verwenden Sie VM-Netzwerk 1 und fügen Sie VMXnet3 (10 Gbit/s) zur Verwendung der Aufnahme hinzu.
- Netzwerkadapter 2 auf VM Netzwerk 2 konfiguriert:
 - Verwenden Sie VM-Netzwerk 2 und fügen Sie VMXnet3 (10 Gbit/s) hinzu, um eine Verbindung zu AWS herzustellen.

Hinzufügen von Ressourcen zu Ihrem Gateway

Die folgenden Engpässe können die Leistung Ihres Volume 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. .

 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.

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.

Ändern der Volumes-Konfiguration

Wenn Sie bei Volume Gateways feststellen, dass durch das Hinzufügen weiterer Volumes in einem Gateway der Durchsatz reduziert wird, sollten sie in Erwägung ziehen, die Volumes zu einem separaten Gateway hinzuzufügen. Insbesondere wenn ein Volume für eine Anwendung mit hohem Durchsatz verwendet wird, sollten Sie in Betracht ziehen, eine separate Gateway mit hoher Durchsatzrate für die Anwendung zu erstellen. Jedoch gilt allgemein, Sie sollten nicht nur eine Gateway für alle Ihre Anwendungen mit hohem Durchsatz verwenden und ein anderes Gateway für alle Ihre Anwendungen mit geringem Durchsatz. Um den Durchsatz Ihrer Volume zu messen, verwenden Sie die `ReadBytes` und `WriteBytes` Metriken.

Weitere Informationen zu diesen Metriken finden Sie unter [Messung der Leistung zwischen Ihrer Anwendung und dem Gateway](#).

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.

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 Netzkabel auf, um eine höhere Bandbreite zwischen Ihrem Initiator und dem Gateway zu erreichen.

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..

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](#)
- [Herunterladen des OVA-Image von der Storage-Gateway-Konsole](#)
- [Bereitstellen des Gateways](#)
- [\(Optional\) Hinzufügen von Überschreibungsoptionen für andere VMs auf Ihrem Cluster](#)
- [Aktivieren des Gateways](#)
- [Testen der Konfiguration von VMware High Availability](#)

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.

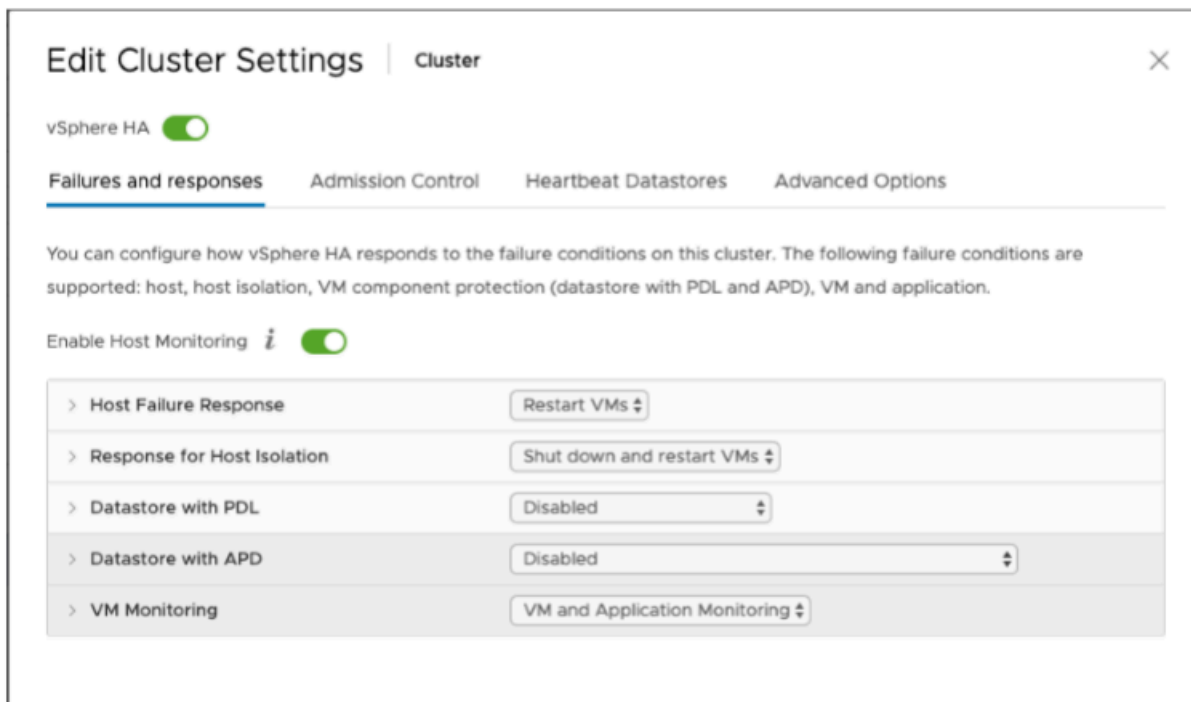
Konfigurieren Sie anschließend Ihren VMware-Cluster für die Arbeit mit Storage Gateway.

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 Volume 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.

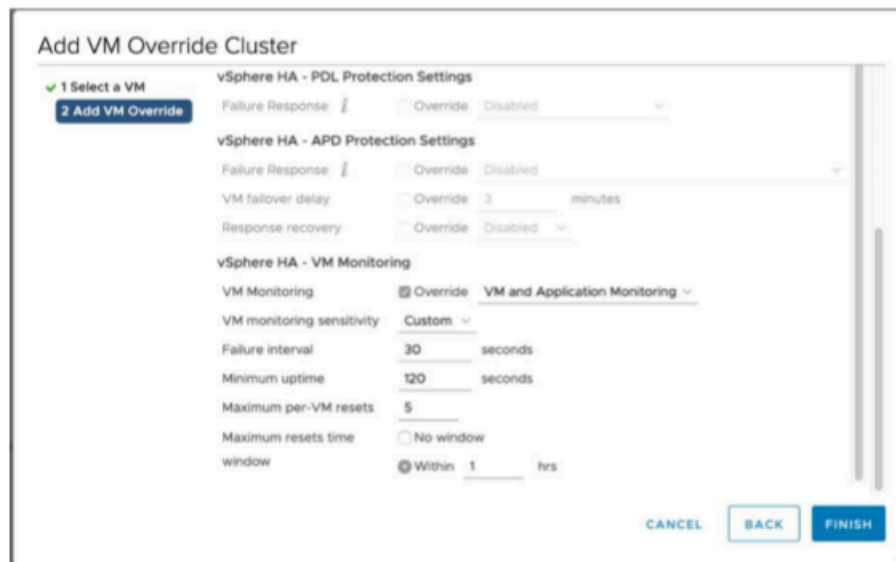
(Optional) Hinzufügen von Überschreibungsoptionen für andere VMs auf Ihrem Cluster

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 Ihres Volume Gateways mit AWS](#)
 - b. [Überprüfen von Einstellungen und Aktivieren Ihres Volume Gateways](#)
 - c. [Konfigurieren von Volume 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 , die [Volume-Gateway-Zustandsprotokolle mit CloudWatch Protokollgruppen abrufen](#).

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](#)
- [Identity and Access Management für AWS Storage Gateway](#)
- [Protokollierung und Überwachung in AWS Storage Gateway](#)
- [Compliance-Validierung für AWS Storage Gateway](#)
- [Ausfallsicherheit in AWS Storage Gateway](#)
- [Infrastruktursicherheit in AWS Storage Gateway](#)
- [AWS Bewährte Methoden für die Sicherheit](#)

Datenschutz in AWS Storage Gateway

Das AWS [Modell der geteilten Verantwortung](#) Modell 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 bei der Verwendung von AWS KMS zur 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 KMS Schlüssel löschen oder deaktivieren oder das Erteilungstoken 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?](#)

Konfigurieren der CHAP-Authentifizierung für Ihre Volumes

In Storage Gateway stellen Ihre iSCSI-Initiatoren eine Verbindung mit Ihren Volumes als iSCSI-Ziele her. Storage Gateway verwendet CHAP (Challenge-Handshake Authentication Protocol) zum Authentifizieren von iSCSI und Initiator-Verbindungen. CHAP bietet Schutz vor Playback-Angriffen, indem für den Zugriff auf Speicher-Volume-Ziele eine Authentifizierung erforderlich gemacht wird. Für jedes Volume-Ziel können Sie CHAP-Anmeldeinformationen oder auch mehrere CHAP-Anmeldeinformationen definieren. Sie können Sie diese Anmeldeinformationen für die verschiedenen Initiatoren im Dialogfeld "Configure CHAP credentials" anzeigen und bearbeiten.

So konfigurieren Sie CHAP-Anmeldeinformationen

1. Wählen Sie in der Storage-Gateway-Konsole Volumes und dann das Volume aus, für das Sie CHAP-Anmeldeinformationen konfigurieren möchten.
2. Klicken Sie im Menü Aktionen auf CHAP-Authentifizierung konfigurieren.
3. Geben Sie unter Initiatorname den Namen Ihres Initiators ein. Der Name muss mindestens 1 Zeichen und darf maximal 255 Zeichen lang sein.
4. Geben Sie in Initiatorgeheimnis den geheimen Begriff ein, den Sie zum Authentifizieren Ihres iSCSI-Initiators verwenden möchten. Der geheime Begriff für den Initiator muss mindestens 12 Zeichen und darf maximal 16 Zeichen lang sein.
5. Geben Sie in Target secret (Zielgeheimnis) den geheimen Begriff ein, den Sie zum Authentifizieren Ihres Ziels für die gegenseitige CHAP-Authentifizierung verwenden möchten. Der geheime Begriff für das Ziel muss mindestens 12 Zeichen und darf maximal 16 Zeichen lang sein.
6. Wählen Sie Speichern aus, um Ihre Einträge zu speichern.

Um CHAP-Anmeldeinformationen anzeigen oder aktualisieren zu können, müssen Sie über die notwendigen IAM-Rollenberechtigungen verfügen, die Ihnen das Ausführen dieses Vorgangs erlauben.

Anzeigen und Bearbeiten von CHAP-Anmeldeinformationen

Sie können CHAP-Anmeldeinformationen für jeden Benutzer hinzufügen, entfernen oder aktualisieren. Zum Anzeigen oder Bearbeiten von CHAP-Anmeldeinformationen müssen Sie über die erforderlichen IAM-Rollenberechtigungen verfügen, die Ihnen ermöglichen, den Vorgang auszuführen, und das Initiatorziel muss einem funktionierenden Gateway angefügt sein.

Configure CHAP authentication

Initiator name	Initiator secret	Target secret
initiator2	*****	*****
initiator1	*****	*****
Add an initiator name.	Add an initiator secret value.	Add a target secret value.

This volume accepts only connections from authenticated iSCSI initiators. [Learn more](#)

Cancel Save

So fügen Sie CHAP-Anmeldeinformationen hinzu

1. Wählen Sie in der Storage-Gateway-Konsole Volumes und dann das Volume aus, dem Sie CHAP-Anmeldeinformationen hinzufügen möchten.
2. Klicken Sie im Menü Aktionen auf CHAP-Authentifizierung konfigurieren.
3. Geben Sie auf der Seite „CHAP konfigurieren“ Initiatorname, Initiatorgeheimnis und Zielgeheimnis in die entsprechenden Felder ein und wählen Sie Speichern aus.

So entfernen Sie CHAP-Anmeldeinformationen

1. Wählen Sie in der Storage-Gateway-Konsole Volumes und dann das Volume aus, für das Sie CHAP-Anmeldeinformationen entfernen möchten.
2. Klicken Sie im Menü Aktionen auf CHAP-Authentifizierung konfigurieren.
3. Klicken Sie auf das X neben den Anmeldeinformationen, die Sie entfernen möchten, und wählen Sie Save (Speichern) aus.

So aktualisieren Sie CHAP-Anmeldeinformationen

1. Wählen Sie in der Storage-Gateway-Konsole Volumes und dann das Volume aus, für das Sie CHAP aktualisieren möchten.
2. Klicken Sie im Menü Aktionen auf CHAP-Authentifizierung konfigurieren.
3. Ändern Sie auf der Seite "Configure CHAP credentials" die Einträge für die Anmeldeinformationen, die Sie aktualisieren möchten.
4. Klicken Sie auf Speichern.

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](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Funktionsweise von AWS Storage Gateway mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Storage Gateway](#)
- [Fehlerbehebung für AWS Storage Gateway-Identität und -Zugriff](#)

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 Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern 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 (servicespezifisch)	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 auch der Prinzipal-Entität (Benutzer oder Rolle) 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 anzugeben, 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 anzugeben, 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 Richtlinienbedingungsschlüssel	Ja
---	----

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, 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 Bedingungs Schlüssel angeben, 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 Bedingungs Schlüssel und servicespezifische Bedingungs Schlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungs Schlüssel finden Sie unter [AWS Globale Bedingungskontextschlüssel](#) im IAM-Benutzerhandbuch.

Eine Liste der AWS SGW-Bedingungs Schlüssel finden Sie unter [Bedingungs Schlüssel für AWS Storage Gateway](#) in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungs Schlüssel 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 an 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 Bedingungelement 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 [Richtlinienuvalidierung 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:ListGroupsWithUser",
      "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 CloudTrail gesammelten 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 CloudTrail finden 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": "AIDAI15AUEPBH2M7JTNVC",
    "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": "cloudtrailgatewayvt1",
    "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": "AIDAI5AUEPBH2M7JTNCV",
      "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": "
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 "
  ]
}

```

```
    " 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 heruntergeladen 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](#).
- Verwenden Sie AWS Backup , um Ihre Volumes zu sichern. Weitere Informationen finden Sie unter [Sichern von Volumes](#).
- Klonen Sie Ihr Volume von einem Wiederherstellungspunkt aus. Weitere Informationen finden Sie unter [Klonen einer Volume](#).

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](#)
- [Fehlerbehebung bei der Einrichtung von Microsoft Hyper-V](#)
- [Fehlerbehebung bei Problemen mit Amazon-EC2-Gateway](#)
- [Fehlerbehebung bei Hardware-Appliance-Problemen](#)
- [Fehlerbehebung bei Volume-Problemen](#)
- [Beheben von Problemen mit Hochverfügbarkeit](#)
- [Bewährte Methoden zum Wiederherstellen Ihrer Daten](#)

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.	<p>Verwenden Sie den Hypervisor-Client zum Herstellen einer Verbindung mit Ihrem Host, um die Gateway-IP-Adresse zu ermitteln.</p> <ul style="list-style-type: none">• 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. <p>Wenn Sie immer noch Probleme haben die Gateway-IP-Adresse zu ermitteln:</p> <ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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,	<ul style="list-style-type: none">• Überprüfen Sie, dass auf die Gateway-VM zugegriffen werden kann, indem Sie die VM Ihres Clients anpingen.

Problem	Maßnahme
<p>wenn Sie in der Storage-Gateway-Managementkonsole auf die Schaltfläche Weiter zur Aktivierung klicken.</p>	<ul style="list-style-type: none">• Stellen Sie sicher, dass Ihre VM eine Netzwerkverbindung zum Internet hat. Andernfalls müssen Sie die Konfiguration eines SOCKS-Proxy vornehmen. Weitere Informationen zur Verfahrensweise 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 automatisch mit einem Network Time Protocol (NTP) Server synchronisiert und dass die Gateway-VM auf die richtige Uhrzeit eingestellt 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-Authentifizierung, 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
<p>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.</p>	<p>Anweisungen zum Entfernen eines Datenträgers, der als Upload-Pufferspeicherplatz zugewiesen ist, finden Sie unter Entfernen von Datenträgern aus dem Gateway.</p>
<p>Sie müssen die Bandbreite zwischen Ihrem Gateway und AWS verbessern.</p>	<p>Sie können die Bandbreite von Ihrem Gateway zu verbessern, AWS indem Sie Ihre Internetverbindung zu AWS auf einem Netzwerkdapter (NIC) einrichten, der von der Verbindung Ihrer Anwendungen und der Gateway-VM getrennt ist. 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 Gateway und AWS. Indem Sie Ihre Internetverbindung verbessern, stellen Sie sicher, dass Ihr Upload-Puffer nicht aufgefüllt wird.</p>

Problem	Maßnahme
Durchsatz zu oder von Ihrem Gateway sinkt auf Null.	<ul style="list-style-type: none">• 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 beschrieben Testen 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 Netzwerkadapter Konfiguration Ihres Gateways anzuzeigen, befolgen Sie die Anweisungen in Konfigurieren Ihres Gateway-Netzwerks und wählen Sie die Option die die Netzwerkkonfiguration Ihres Gateway anzeigt. <p>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 Gateway und AWS.</p>

Problem	Maßnahme
Sie haben Schwierigkeiten 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 Fehlermeldung: „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 AWS öffnen 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 AWS öffnen können. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.

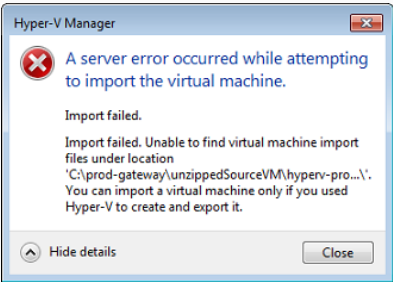
 Note

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.

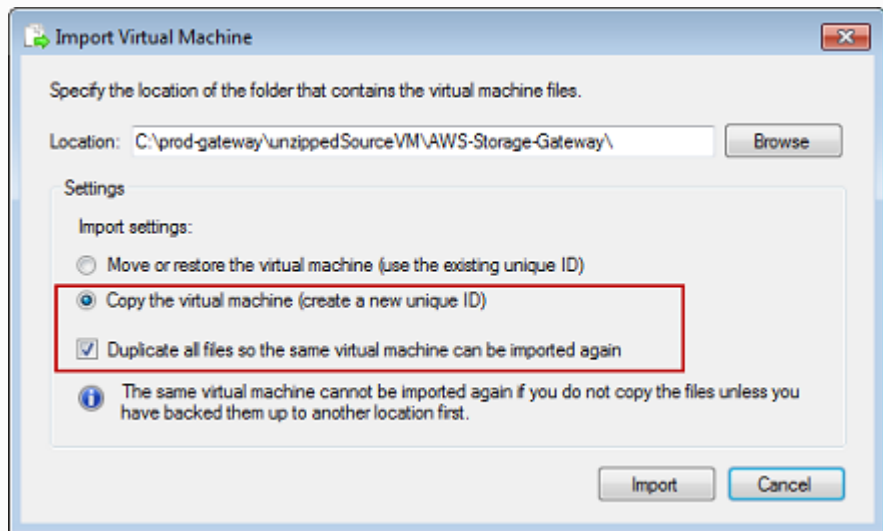
Fehlerbehebung bei der Einrichtung von Microsoft Hyper-V

In der folgenden Tabelle sind typische Probleme aufgeführt, die beim Bereitstellen von Storage Gateway auf der Microsoft Hyper-V-Plattform auftreten können.

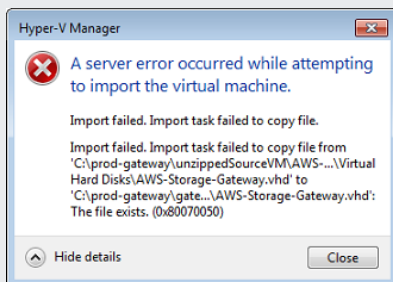
Problem	Maßnahme
<p>Sie versuchen, ein Gateway zu importieren und erhalten die Fehlermeldung: „Import ist fehlgeschlagen. Die Import-Datei der Virtuellen Maschine wird unter Standort nicht gefunden...“.</p> 	<p>Dieser Fehler kann aus folgenden Gründen auftreten:</p> <ul style="list-style-type: none"> • 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 <code>AWS-Storage-Gateway\</code> lauten, wie im folgenden Beispiel dargestellt:  <ul style="list-style-type: none"> • Wenn Sie bereits ein Gateway bereitgestellt haben, die Option Copy the virtual machine (virtuelle Maschine kopieren) nicht ausgewählt ist und Sie die Option Duplicate all files (Alle Dateien duplizieren) im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) markiert haben, dann wurde die VM an dem Speicherort erstellt, an dem Sie die Dateien entpackt haben, und Sie können nicht erneut von dort importieren. Zur Behebung dieses Problems, erwerben Sie eine neue Kopie der entpackten Gateway Quell-Dateien und kopieren Sie diese an einen neuen Speicherort. Verwenden Sie den neuen Speicherort als Importquelle. Das folgende Beispiel zeigt die Optionen, die Sie überprüfen

Problem	Maßnahme
---------	----------

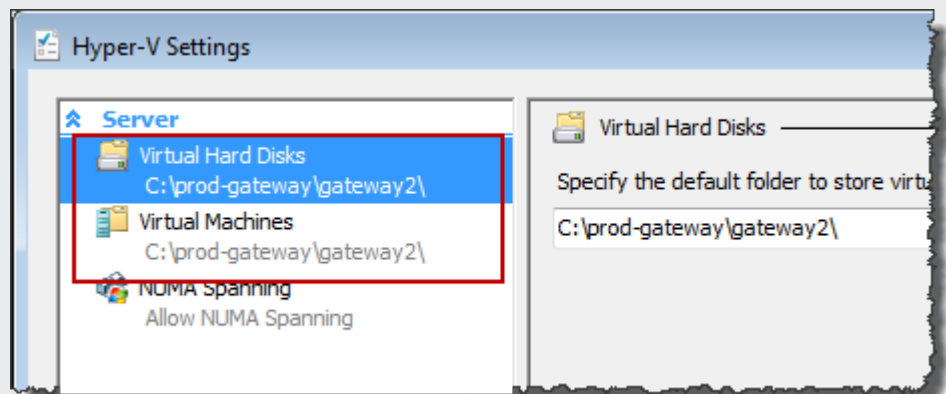
n müssen, wenn Sie aus einem entpackten Quelldateien-Speicherort mehrere Gateways erstellen möchten.



Sie versuchen, ein Gateway zu importieren und erhalten die Fehlermeldung: „Import ist fehlgeschlagen. Import Aufgabe zur Kopie der Datei fehlgeschlagen.“

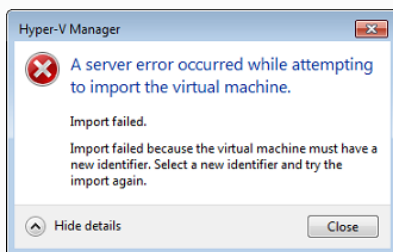


Wenn Sie bereits ein Gateway bereitgestellt haben und Sie versuchen den Standard-Ordner wiederzuverwenden, der die virtuelle Festplatten Dateien und die virtuelle Maschinen-Konfigurationsdateien speichert, wird dieser Fehler auftreten. Zur Behebung dieses Problems geben Sie neue Speicherorte im Dialogfeld Hyper-V Settings (Hyper-V-Einstellungen) an.



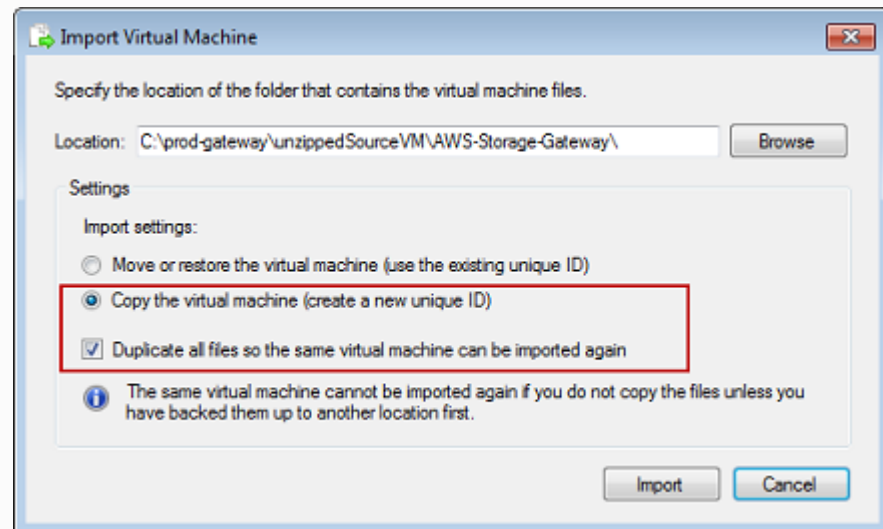
Problem

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.“

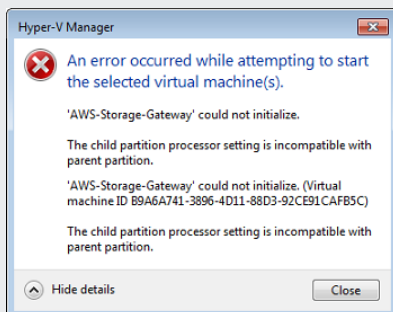


Maßnahme

Wenn Sie das Gateway importieren, stellen Sie sicher, dass Sie die Option Copy the virtual machine (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.

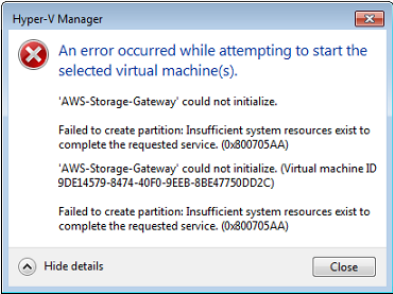


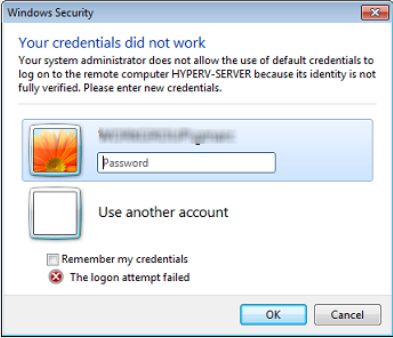
Sie versuchen, eine Gateway-VM zu starten und erhalten die Fehlermeldung erhalten: „Die untergeordnete Partitions-Prozessor-Einstellung ist nicht kompatibel mit der übergeordneten Partition.“



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
<p>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."</p> 	<p>Dieser Fehler wird wahrscheinlich durch eine RAM-Abweichungen zwischen dem erforderlichen RAM für das Gateway und den verfügbaren RAM auf dem Host verursacht.</p> <p>Weitere Informationen zu den Anforderungen für Storage Gateway finden Sie unter Voraussetzungen.</p>
<p>Ihre Snapshots und Gateway-Software-Aktualisierungen treten zu geringfügig anderen Zeiten als erwartet auf.</p>	<p>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.</p>
<p>Sie müssen die entzippten Microsoft Hyper-V-Dateien für Storage Gateway im Host-Dateisystem ablegen.</p>	<p>Greifen Sie auf den Host zu wie Sie auf einen typischen Microsoft Windows Server zugreifen würden. Zum Beispiel: Wenn der Hypervisor Host-Name <code>hyperv-server</code> lautet, dann können Sie den folgenden UNC-Pfad wählen <code>\\hyperv-server\c\$</code>, dieser geht davon aus, dass der Name <code>hyperv-server</code> in Ihrer lokalen Host-Datei aufgelöst oder definiert werden kann.</p>

Problem	Maßnahme
<p>Sie werden aufgefordert Anmeldeinformationen anzugeben, wenn Sie eine Verbindung zum Hypervisor herstellen.</p> 	<p>Fügen Sie Ihre Benutzer-Anmeldeinformationen als lokaler Administrator für den Hypervisor-Host mithilfe des Sconfig.cmd Tool hinzu.</p>
<p>Möglicherweise stellen Sie eine schlechte Netzwerkeistung fest, wenn Sie die Virtual Machine Queue (VMQ) auf einem Hyper-V-Host aktivieren, der einen Broadcom-Netzwerkadapter verwendet.</p>	<p>Informationen zu einer Problemlösung finden Sie in der Microsoft-Dokumentation zum Thema Schlechte Netzwerkeistung auf virtuellen Maschinen auf einem Windows Server 2012 Hyper-V-Host, wenn VMQ aktiviert ist.</p>

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 Volume 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](#)
- [Sie können keinen Initiator an ein Volume-Ziel auf dem EC2-Gateway 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 ausgeführt 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.

Sie können keinen Initiator an ein Volume-Ziel auf dem EC2-Gateway anfügen

Stellen Sie sicher, dass die Sicherheitsgruppe, mit der Sie die Instance gestartet haben, eine Regel enthält, die den Port zulässt, den Sie für den iSCSI-Zugriff verwenden. Der Port wird in der zu 3260 festgesetzt. Weitere Informationen zum Verbinden zu Volumes finden Sie unter [Verbinden eines Windows-Clients mit Volumes](#).

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 Volume 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 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 AWS öffnen 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 AWS öffnen 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 beschriebene 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.

The screenshot shows the AWS Storage Gateway console interface. At the top, a green notification banner states "Successfully launched File Gateway on praksuji-bh". Below this, there are buttons for "Order appliance", "Quotes and orders", "Activate appliance", and an "Actions" dropdown menu. A search filter is present: "Filter by hardware appliance name, ID or launched gateway type." A table lists hardware appliances:

	Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
<input checked="" type="checkbox"/>	praksuji-bh	v15loueix9yotyn5	Dell PowerEdge R640	File Gateway
<input type="checkbox"/>	praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Below the table, the "Details" section for the selected appliance "praksuji-bh" is shown:

Name	praksuji-bh	Vendor	Dell
ID	v15loueix9yotyn5	Model	Dell PowerEdge R640
Time Zone	GMT	Serial Number	5Q8Y0M2
		RAID Volume Manager	ZFS

Hardware-Registerkarte der Storage-Gateway-Konsole mit ausgewählter Appliance und angezeigten Details.

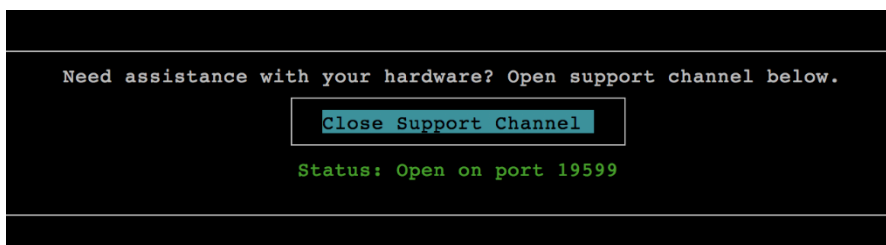
Wo Sie Hardware-Appliance-Support erhalten?

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.

Fehlerbehebung bei Volume-Problemen

Sie können Informationen über die typischsten Probleme finden, die beim Arbeiten mit Volumes auftreten können sowie Aktionen die wir vorschlagen auszuführen um diese zu beheben.

Themen

- [Die Konsole behauptet, dass Ihre Volume nicht konfiguriert ist](#)
- [Die Konsole gibt an, dass Ihre Volume verloren ist](#)
- [Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen](#)
- [Die Konsole gibt an, das Ihre Volume WEITERGABE Status hat](#)
- [Sie möchten Volume-Integrität überprüfen und möglicher Fehler beheben](#)
- [Ihre Volume-iSCSI-Target erscheint nicht in Windows Disk Management Konsole](#)
- [Sie möchten den iSCSI-Volumen-Zielnamen ändern](#)
- [Ihr geplanter Volume Snapshot taucht nicht auf](#)
- [Sie müssen eine Festplatte entfernen oder ersetzen, die ausgefallen ist](#)
- [Durchsatz von Ihrer Anwendung zu einem Volume ist auf Null abgefallen](#)
- [In einer Cache-Festplatte in Ihrem Gateway tritt ein Fehler auf](#)
- [Ein Volume Snapshot hat einen PENDING Status länger als erwartet](#)
- [High Availability-Zustandsbenachrichtigungen](#)

Die Konsole behauptet, dass Ihre Volume nicht konfiguriert ist

Wenn die Storage-Gateway-Konsole angibt, dass Ihr Volume den Status UPLOAD-PUFFER NICHT KONFIGURIERT besitzt, fügen Sie Upload-Pufferkapazität zu Ihrem Gateway hinzu. Sie können ein Gateway nicht zum Speichern Ihrer Anwendungsdaten verwenden, wenn der Upload-Puffer für das Gateway nicht konfiguriert ist. Weitere Informationen finden Sie unter [So konfigurieren Sie zusätzlichen Upload-Puffer oder Cache-Speicher für Ihr Gateway](#).

Die Konsole gibt an, dass Ihre Volume verloren ist

Wenn die Storage-Gateway-Konsole für gespeicherte Volumes angibt, dass Ihr Volume-Status NICHT WIEDERHERSTELLBAR ist, können Sie dieses Volume nicht mehr verwenden. Sie können versuchen, das Volume in der Storage-Gateway-Konsole zu löschen. Wenn sich Daten auf dem Volume befinden, können Sie die Daten wiederherstellen, wenn Sie einen neuen Volume erstellen der auf der lokalen Festplatte der VM basiert, die ursprünglich verwendet wurde, um das Volume zu erstellen. Wenn Sie das neue Volume erstellen, wählen Sie *Preserve existing data* (Vorhandene Daten behalten) aus. Stellen Sie sicher, ausstehende Snapshots des Volumes zu löschen, bevor Sie das Volume löschen. Weitere Informationen finden Sie unter [Löschen eines Snapshots](#). Wenn das Löschen des Volumes in der Storage-Gateway-Konsole nicht funktioniert, dann wurde der Datenträger für das Volume möglicherweise nicht ordnungsgemäß aus der VM entfernt und kann nicht aus der Appliance entfernt werden.

Wenn die Storage-Gateway-Konsole für zwischengespeicherte Volumes angibt, dass der Status Ihres Volumes NICHT WIEDERHERSTELLBAR lautet, können Sie dieses Volume nicht mehr verwenden. Wenn Daten auf dem Volume liegen, können Sie einen Snapshot des Volumes erstellen und dann Ihre Daten aus dem Snapshot wiederherstellen oder Sie können die Volumes vom letzten Wiederherstellungspunkt aus klonen. Sie können das Volume löschen, nachdem Sie Ihre Daten wiederhergestellt haben. Weitere Informationen finden Sie unter [Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen](#).

Für gespeicherte Volumes können Sie eine neue Volume von der Festplatte erstellen, die zum Erstellen des irreparablen Volumes verwendet wurde. Weitere Informationen finden Sie unter [Erstellen eines Volumes](#). Informationen zum Volume-Status finden Sie unter [Grundlagen zu Status und Übergängen bei Volumes](#).

Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen

Wenn Ihr Gateway nicht erreichbar ist (z. B. wenn es heruntergefahren wurde), haben Sie die Möglichkeit, entweder einen Snapshot von einem Volume-Wiederherstellungspunkt herzustellen und diesen Snapshot zu verwenden oder Sie klonen ein neues Volume anhand vom letzten Wiederherstellungspunktes für eine vorhandene Volume. Das Klonen eines Volume-Wiederherstellungspunkt ist schneller und kostengünstiger als das Erstellen eines Snapshots. Weitere Informationen zum Klonen eines Volumes finden Sie unter [Klonen einer Volume](#).

Storage Gateway bietet Wiederherstellungspunkte für jedes Volume in einer zwischengespeicherten Volume-Gateway-Architektur. Ein Volume-Wiederherstellungspunkt ist ein Zeitpunkt, zu dem alle Daten des Volumes konsistent sind und von dem Sie einen Snapshot erstellen oder ein Volume klonen können.

Die Konsole gibt an, das Ihre Volume WEITERGABE Status hat

In einigen Fällen kann die Storage-Gateway-Konsole darauf hinweisen, dass Ihr Volume den Status PASS-THROUGH aufweist. Ein Volume kann aus unterschiedlichen Gründen den Status „PASSTHROUGH“ annehmen. Einige Gründe erfordern Aktionen, andere nicht.

Ein Beispiel für wann Sie etwas unternehmen sollten, wenn Ihre Volume den WEITERGABE Status hat, ist, wenn Ihr Gateway keinen Upload-Pufferspeicherplatz mehr hat. Um zu überprüfen, ob Ihr Upload-Puffer in der Vergangenheit überschritten wurde, können Sie die `UploadBufferPercentUsed` Metrik in der Amazon- CloudWatch Konsole anzeigen. Weitere Informationen finden Sie unter [Überwachen des Upload-Puffers](#). Wenn Ihr Gateway den Status PASS-THROUGH aufweist, weil kein Upload-Pufferspeicher mehr verfügbar ist, sollten Sie Ihrem Gateway mehr Upload-Pufferspeicher zuweisen. Wenn Sie mehr Pufferspeicher hinzufügen, wechselt der Status Ihres Volumes von PASS-THROUGH über BOOTSTRAPPING automatisch zu VERFÜGBAR. Während das Volume den Status BOOTSTRAPPING aufweist, liest das Gateway Daten vom Datenträger des Volumes, lädt diese Daten in Amazon S3 und holt nach Bedarf auf. Nachdem das Gateway wieder den gewünschten Status hat und die Volume-Daten in Amazon S3 gespeichert wurden, lautet der Volume-Status VERFÜGBAR und Snapshots können erneut gestartet werden. Beachten Sie, wenn Ihr Volume den WEITERGABE oder BOOTSTRAPPING Status besitzt können Sie damit fortfahren, die Daten von der Volume Festplatte zu lesen und schreiben. Weitere Informationen zum Hinzufügen weiterer Upload-Pufferspeicher finden Sie unter [Bestimmen der Größe des zuzuordnenden Upload-Puffers](#).

Um Aktionen durchzuführen bevor der Upload-Puffer überschritten wird, können Sie einen Grenzwert-Überschreitungsalarm auf dem Upload-Puffer des Gateways einstellen. Weitere Informationen finden Sie unter [So richten Sie einen Obergrenzenalarm für den Gateway-Upload-Puffer ein](#).

Im Gegensatz dazu ist ein Beispiel für ein Volume an der keine entsprechende Maßnahme zu ergreifen ist, wenn die Volume auf eine Bootstrap-Aktion wartet, da eine andere Volume derzeit gestartet wird. Das Gateway führt Bootstrap-Aktionen an Volumes nacheinander aus.

Selten, gibt der WEITERGABE Status an, dass eine Festplatte die einem Upload-Puffer zugeordnet wurde fehlgeschlagen ist. In diesem Fall sollten Sie die Festplatte entfernen. Weitere Informationen

finden Sie unter [Volume Gateway](#). Informationen zum Volume-Status finden Sie unter [Grundlagen zu Status und Übergängen bei Volumes](#).

Sie möchten Volume-Integrität überprüfen und möglicher Fehler beheben

Wenn Sie Volume-Integrität überprüfen möchten und mögliche Fehler beheben möchten und Ihr Gateway für die Verbindung zu seinen Volumes, Microsoft Windows Initiatoren verwendet, können Sie das Windows CHKDSK Dienstprogramm verwenden, um die Integrität Ihrer Volumes zu überprüfen und jeglichen Fehler auf den Volumes beheben. Windows kann automatisch das CHKDSK-Tool ausführen, wenn auf einer Volume Beschädigungen festgestellt werden oder Sie können es selbst ausführen.

Ihre Volume-iSCSI-Target erscheint nicht in Windows Disk Management Konsole

Wenn Ihr Volume iSCSI-Ziel nicht in der Disk Management Konsole in Windows angezeigt wird, überprüfen Sie, ob der Upload-Puffer für das Gateway konfiguriert wurde. Weitere Informationen finden Sie unter [So konfigurieren Sie zusätzlichen Upload-Puffer oder Cache-Speicher für Ihr Gateway](#).

Sie möchten den iSCSI-Volumen-Zielnamen ändern

Wenn Sie den iSCSI-Zielnamen Ihres Volumes ändern möchten, müssen Sie das Volume löschen und es noch einmal mit neuem Zielnamen hinzufügen. Wenn Sie dies durchführen, können Sie die Daten auf dem Volume beibehalten.

Ihr geplanter Volume Snapshot taucht nicht auf

Wenn das geplante Snapshot eines Volumes nicht auftaucht, überprüfen Sie, ob Ihre Volume den Status „PASSTHROUGH“ besitzt, oder ob der Gateway Upload-Puffer gerade vor dem geplanten Snapshot Uhrzeit aufgefüllt wurde. Sie können die `-UploadBufferPercentUsed` Metrik für das Gateway in der Amazon CloudWatch-Konsole überprüfen und einen Alarm für diese Metrik erstellen. Weitere Informationen finden Sie unter [Überwachen des Upload-Puffers](#) und [So richten Sie einen Obergrenzenalarm für den Gateway-Upload-Puffer ein](#).

Sie müssen eine Festplatte entfernen oder ersetzen, die ausgefallen ist

Wenn Sie einen ausgefallenen Volume-Datenträger austauschen müssen oder ein Volume entfernen möchten, weil es nicht benötigt wird, sollten Sie das Volume zuerst mithilfe der Storage-Gateway-

Konsole entfernen. Weitere Informationen finden Sie unter [So löschen Sie ein Volume](#). Anschließend verwenden Sie den Hypervisor-Client, um den Backup-Speicher zu entfernen:

- Für VMware ESXi, entfernen Sie den Sicherungs-Speicher wie in beschrieben [Löschen eines Volumes](#).
- Für Microsoft Hyper-V, entfernen Sie den Backup-Speicher.

Durchsatz von Ihrer Anwendung zu einem Volume ist auf Null abgefallen

Wenn der Durchsatz von Ihrer Anwendung zu einem Volume auf Null abgefallen ist, versuchen Sie Folgendes:

- Wenn Sie den VMware vSphere-Client verwenden, prüfen Sie, ob die Host IP (Host-IP)-Adresse Ihres Volumes mit einer der Adressen übereinstimmt, die auf der Registerkarte Summary (Übersicht) im vSphere-Client angezeigt wird. Sie finden die Host-IP-Adresse für ein Speicher-Volume in der Storage-Gateway-Konsole auf der Registerkarte Details für das Volume. Unstimmigkeiten in der IP-Adresse können vorkommen, wenn Sie z. B. Ihrem Gateway eine neue statische IP-Adresse zuweisen. Wenn eine Diskrepanz vorliegt, starten Sie das Gateway über die Storage-Gateway-Konsole neu, wie in [Herunterfahren der Gateway-VM](#) dargestellt. Nach dem Neustart sollte die Host IP (Host-IP)-Adresse auf der Registerkarte iSCSI Target Info (iSCSI-Zielinformationen) für ein Speicher-Volume mit einer IP-Adresse in dem vSphere Client auf der Registerkarte Summary (Übersicht) für das Gateway übereinstimmen.
- Wenn keine IP-Adresse im Feld Host IP (Host-IP) für das Volume angezeigt wird und das Gateway online ist. Dies kann auftreten, wenn Sie beispielsweise ein Volume erstellen das einer IP-Adresse eines Netzwerkadapters von einem Gateway mit zwei oder mehr Netzwerkadaptern zugeordnet ist. Wenn Sie den Netzwerkadapter entfernen oder deaktivieren, der dem Volume zugeordnet ist, wird die IP-Adresse möglicherweise nicht im Feld Host-IP angezeigt. Um dieses Problem zu beheben, löschen Sie das Volume und erstellen Sie es dann erneut unter Beibehaltung der vorhandenen Daten.
- Stellen Sie sicher, dass der iSCSI-Initiator den Ihre Anwendung verwendet korrekt dem iSCSI-Ziel für das Speicher-Volume, zugeordnet ist. Weitere Informationen zum Verbinden zu Speicher Volumes finden Sie unter [Verbinden eines Windows-Clients mit Volumes](#).

Sie können den Durchsatz für Volumes anzeigen und Alarme von der Amazon CloudWatch-Konsole aus erstellen. Weitere Informationen über die Messung des Durchsatzes von Ihrer Anwendung zu einer Volume, finden Sie unter [Messung der Leistung zwischen Ihrer Anwendung und dem Gateway](#).

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 flüchtiger Laufwerke oder Datenträger ab.

Ein Volume Snapshot hat einen PENDING Status länger als erwartet

Wenn ein Volume-Snapshot länger als erwartet im Status PENDING bleibt, ist die Gateway-VM möglicherweise unerwartet abgestürzt oder der Status eines Volumes hat sich zu PASS THROUGH oder IRRECOVERABLE geändert. Wenn einer dieser Vorkommnisse der Fall ist, bleibt der Snapshot im PENDING Status und der Snapshot wird nicht vollständig ausgeführt. In diesen Fällen empfehlen

wir, dass Sie den Snapshot löschen. Weitere Informationen finden Sie unter [Löschen eines Snapshots](#).

Wenn das Volume auf den Status AVAILABLE zurückkehrt, erstellen Sie einen neuen Snapshot des Volumes. Informationen zum Volume-Status finden Sie unter [Grundlagen zu Status und Übergängen bei Volumes](#).

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](#)
- [Metriken](#)

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](#)
- [Benachrichtigung: HardReboot](#)
- [Benachrichtigung: HealthCheckFailure](#)
- [Benachrichtigung: AvailabilityMonitorTest](#)

Benachrichtigung: Reboot

Sie können eine Neustart-Benachrichtigung erhalten, wenn die Gateway-VM neu gestartet wird. Sie können eine Gateway-VM mithilfe der VM Hypervisor-Managementkonsole oder der Storage-Gateway-Konsole neu starten. Sie können den Neustart auch mithilfe der Gateway-Software während des Wartungszyklus des Gateways ausführen.

Maßnahme

Wenn die Zeit des Neustarts innerhalb von 10 Minuten nach der konfigurierten [Wartungsstartzeit](#) des Gateways liegt, handelt es sich wahrscheinlich um ein normales Ereignis und es deutet nicht auf ein Problem hin. Wenn der Neustart deutlich außerhalb des Wartungsfensters stattgefunden hat, überprüfen Sie, ob das Gateway manuell neu gestartet wurde.

Benachrichtigung: HardReboot

Sie können eine HardReboot-Benachrichtigung erhalten, wenn die Gateway-VM unerwartet neu gestartet wird. Ein solcher Neustart kann auf Stromausfall, einen Hardwarefehler oder ein anderes Ereignis zurückzuführen sein. Bei VMware-Gateways kann ein 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 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](#)

- [Wiederherstellen Ihrer Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM](#)
- [Wiederherstellung Ihrer Daten von einem nicht wiederherstellbaren Volume](#)
- [Wiederherstellen Ihrer Daten von einer fehlerhaften Cache-Festplatte](#)
- [Wiederherstellen Ihrer Daten von einem beschädigten Datensystem](#)
- [Wiederherstellen Ihrer Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann](#)

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 zwischengespeicherten Volumes erreichbar ist, werden Ihre Volumes 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 [Grundlagen zu Status und Übergängen bei Volumes](#).
- 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 Ihr Gateway oder Ihre virtuelle Maschine fehlerhaft ist, können Sie Daten wiederherstellen, die auf ein Volume in Amazon S3 hochgeladen AWS und dort gespeichert wurden. Für Cached-Volumes-Gateways, können Sie Daten von einem Recovery-Snapshot aus wiederherstellen. Bei Gateways für gespeicherte Volumes können Sie Daten von Ihrem letzten Amazon-EBS-Snapshot des Volumes wiederherstellen. Bei Tape Gateways stellen Sie ein oder mehrere Bänder von einem Wiederherstellungspunkt auf einem neuen Tape Gateway wieder her.

Wenn Ihr Cached-Volumes-Gateway nicht erreichbar sein sollte, können Sie die folgenden Schritte zum Wiederherstellen Ihrer Daten von einem Recovery-Snapshot versuchen:

1. Wählen AWS Management Console Sie in der das fehlerhafte Gateway aus, wählen Sie das Volume aus, das Sie wiederherstellen möchten, und erstellen Sie dann daraus einen Wiederherstellungs-Snapshot.
2. Stellen Sie ein neues Volume Gateway bereit und aktivieren Sie es. Wenn Sie bereits ein funktionierendes Volume Gateway besitzen, können Sie das Gateway verwenden, um Ihre Volume-Daten wiederherzustellen.
3. Finden Sie die Snapshots, die Sie erstellt haben, und stellen Sie sie auf einem neuen funktionierendem Gateway wieder her.
4. Mounten Sie das neue Volume als iSCSI-Gerät auf Ihrem lokalen Anwendungsserver.

Ausführliche Informationen, zur Wiederherstellung von Cached-Volumes-Daten von einem wiederhergestelltem Snapshot, finden Sie unter [Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen](#).

Wiederherstellung Ihrer Daten von einem nicht wiederherstellbaren Volume

Wenn der Status Ihrer Volume IRRECOVERABLE ist, können Sie diese Volume nicht länger verwenden.

Für gespeicherte Volumes, können Sie Ihre Daten aus dem irreparablen Volume in einem neuem Volume abrufen, indem Sie die folgenden Schritte befolgen:

1. Erstellen einer neuen Volume von einer Festplatte, die verwendet wurde um ein irreparables Volume zu erstellen.
2. Behalten der existierenden Daten, wenn Sie die neue Volume erstellen.
3. Löschen Sie alle ausstehenden Snapshot-Jobs für das irreparable Volume.
4. Löschen Sie das irreparable Volume aus dem Gateway.

Für Cached-Volumes empfehlen wir den Einsatz von des letzten Wiederherstellungspunkts ein neues Volume zu klonen.

Detaillierte Informationen, zum Abrufen Ihrer Daten aus einem irreparablen Volume zu einem neuen Volume, finden Sie unter [Die Konsole gibt an, dass Ihre Volume verloren ist](#).

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.

Wiederherstellen Ihrer Daten von einem beschädigten Dateisystem

Wenn Ihr Dateisystem beschädigt wird, können Sie den Befehl **fsck** verwenden, um zu überprüfen, ob Ihr Dateisystem Fehler aufweist, und diese beseitigen. Wenn Sie das Dateisystem reparieren können, können Sie Ihre Daten von den Volumes auf dem Dateisystem wiederherstellen, im Nachfolgenden beschrieben:

1. Fahren Sie Ihre virtuelle Maschine herunter und verwenden Sie die Storage-Gateway-Management-Console, um einen Wiederherstellungs-Snapshot zu erstellen. Dieser Snapshot stellt die aktuellen Daten dar, die in gespeichert sind AWS.

Note

Sie verwenden diesen Snapshot als Fallback, wenn Ihr Dateisystem nicht repariert werden kann oder der Snapshot-Erstellungsprozess nicht erfolgreich abgeschlossen werden kann.

Weitere Informationen, wie Sie einen Recovery-Snapshot erstellen, finden Sie unter [Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen](#).

2. Verwenden Sie den Befehl **fsck**, um zu überprüfen, ob Ihr Dateisystem Fehler aufweist, und versuchen Sie, es zu reparieren.
3. Starten Sie Ihre Gateway-VM neu.
4. Wenn Ihr Hypervisor-Host anfängt zu booten, halten Sie die Umschalttaste gedrückt, um in das Grub-Boot-Menü zu gelangen.
5. Drücken Sie zum Bearbeiten im Menü **e**.

6. Wählen Sie die Kernel-Zeile (die zweite Zeile) und drücken Sie dann zum Bearbeiten **e**.
7. Fügen Sie die folgende Option an die Kernel-Befehlszeile an: **init=/bin/bash**. Verwenden Sie ein Leerzeichen um die vorherigen Option von der Option, die Sie gerade hinzugefügt haben, zu trennen.
8. Löschen Sie beide `console=`-Zeilen und achten Sie darauf, alle Werte zu löschen, die auf das Symbol = folgen, einschließlich der durch Kommas getrennten Werte.
9. Drücken Sie **Return**, um die Änderungen zu speichern.
10. Drücken Sie **b**, um Ihren Computer mit der geänderten Kernel-Option zu starten. Ihr Computer wird beim Starten eine `bash#` Eingabeaufforderung anzeigen.
11. Geben Sie **`/sbin/fsck -f /dev/sda1`** ein, um diesen Befehl manuell von der Eingabeaufforderung auszuführen, um Ihr Dateisystem zu prüfen und zu reparieren. Falls der Befehl mit dem Pfad `/dev/sda1` nicht funktioniert, können Sie **`lsblk`** verwenden, um das Root-Dateisystemgerät für `/` zu ermitteln, und stattdessen diesen Pfad verwenden.
12. Wenn die Überprüfung und Reparatur des Dateisystems abgeschlossen ist, starten Sie die Instance neu. Die Grub-Einstellungen werden auf die ursprünglichen Werte zurückgesetzt und der Gateway wird normal starten.
13. Warten Sie auf Snapshots, des ursprünglichen Gateways, die in Arbeit sind, bis sie ausgeführt worden sind und validieren Sie die Snapshot-Daten.


Sie können weiterhin die ursprünglichen Volumes so verwenden wie sie sind oder Sie können ein neues Gateway mit einem neuen Volume erstellen, die entweder auf dem Recovery-Snapshot oder auf dem ausgefüllten Snapshot, basiert. Alternativ können Sie von allen Ihrer abgeschlossenen Snapshots dieser Volume, ein neues Volume erstellen.

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 Volume Gateway in einem Rechenzentrum wieder her, auf das nicht zugegriffen werden kann

1. Erstellen und aktivieren Sie ein neues Volume Gateway auf einem Amazon-EC2-Host. Weitere Informationen finden Sie unter [Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Volume Gateway](#).

 Note

In einem Gateway gespeicherte Volumes können nicht auf einer Amazon-EC2-Instance gehostet werden.

2. Erstellen Sie ein neues Volume, und wählen Sie die EC2-Gateway als Ziel-Gateway. Weitere Informationen finden Sie unter [Erstellen eines Volumes](#).

Erstellen Sie das neue Volume auf der Grundlage eines Amazon-EBS-Snapshot oder Klon von dem letzten Wiederherstellungspunkt des Volumes, das Sie wiederherstellen möchten.

Wenn Ihr Volume auf einem Snapshot basiert, geben Sie die Snapshot-ID ein.

Wenn Sie ein Volume aus einem Wiederherstellungspunkt klonen, wählen Sie den Quell-Volume.

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](#)
- [Volume Gateway](#)
- [Abrufen eines Aktivierungsschlüssels für das Gateway](#)
- [Verbinden von iSCSI-Initiatoren](#)
- [Verwenden von AWS Direct Connect mit Storage Gateway](#)
- [Port-Anforderungen](#)
- [Herstellen einer Verbindung mit einem Gateway](#)
- [Grundlegendes zu Ressourcen und Ressourcen-IDs von Storage Gateway](#)
- [Kennzeichnen der Storage Gateway-Ressourcen](#)
- [Arbeiten mit Open-Source-Komponenten für AWS Storage Gateway](#)
- [AWS Storage Gateway -Kontingente](#)

Host-Setup

Themen

- [Konfiguration von VMware für Storage Gateway](#)
- [Synchronisieren der Gateway-VM-Zeit](#)
- [Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Volume Gateway](#)
- [Bereitstellen von Amazon EC2 mit Standardeinstellungen](#)
- [Ändern von Amazon EC2-Instance-Metadatenoptionen](#)

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](#)
- [Konfigurieren der AWS Storage Gateway VM für die Verwendung paravirtualisierter Festplattencontroller](#)
- [Verwenden von Storage Gateway mit VMware High Availability](#)

Synchronisieren der VM-Zeit mit der Host-Zeit

Damit das Gateway erfolgreich aktiviert wird, müssen Sie sicherstellen, dass die VM-Zeit mit der Host-Zeit synchronisiert ist und dass die Host-Zeit richtig eingestellt ist. In diesem Abschnitt synchronisieren Sie zunächst die Zeit für die VM mit der Host-Zeit. Anschließend prüfen Sie die Host-Zeit. Stellen Sie dann bei Bedarf die Host-Zeit ein und konfigurieren Sie den Host so, dass die Zeit automatisch mit einem NTP-Server (Network Time Protocol) synchronisiert wird.

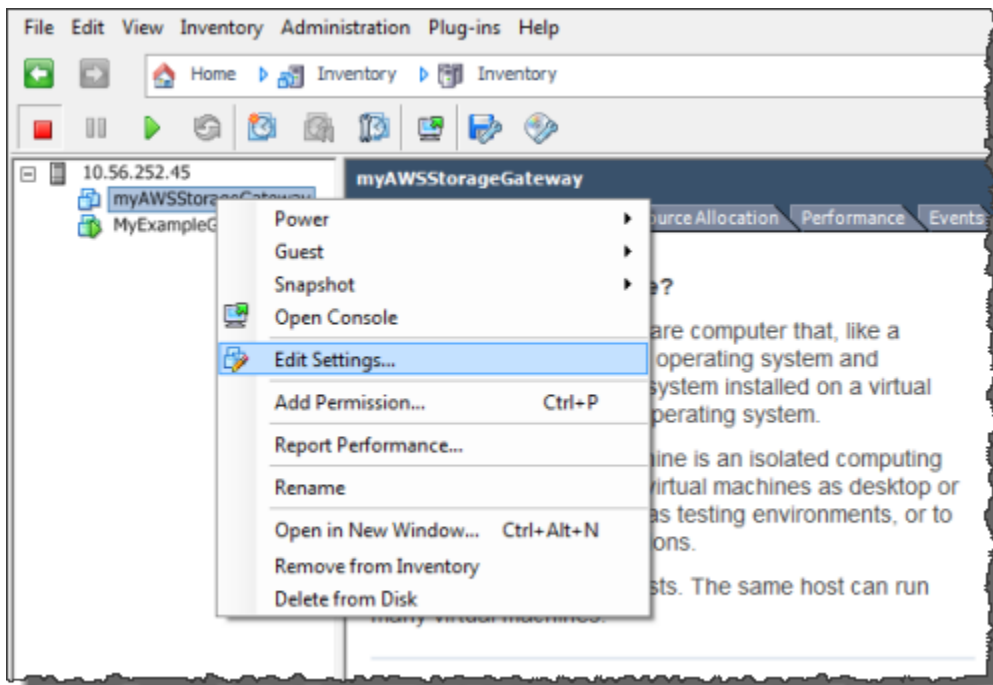
Important

Das Synchronisieren der VM-Zeit mit der Host-Zeit ist erforderlich, um das Gateway erfolgreich zu aktivieren.

So synchronisieren Sie die VM-Zeit mit der Host-Zeit

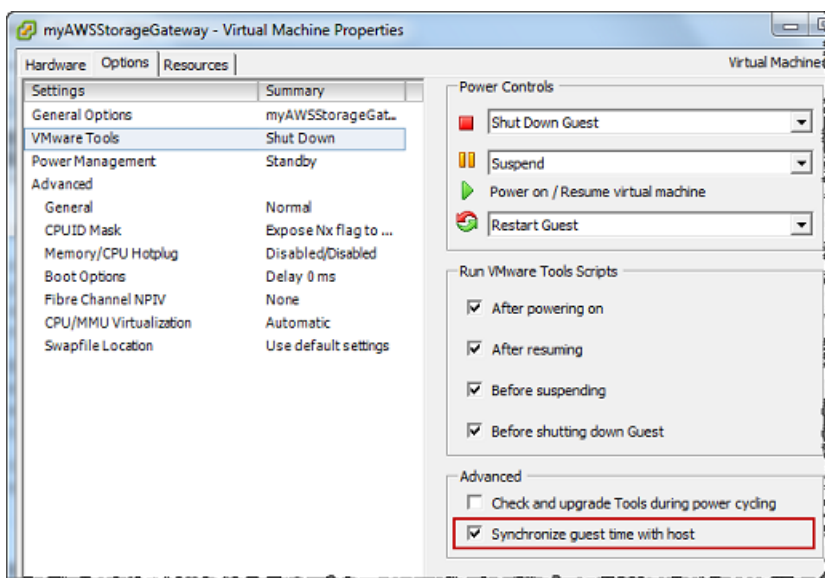
1. Konfigurieren Sie Ihre VM-Zeit.
 - a. Öffnen Sie im vSphere-Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM und wählen Sie Edit Settings (Einstellungen bearbeiten).

Das Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) wird geöffnet.



- b. Wählen Sie die Registerkarte Options (Optionen) und wählen Sie die Option VMware Tools (VMware-Tools) in der Optionenliste.
- c. Aktivieren Sie die Option Synchronize guest time with host (Gastzeit mit Host synchronisieren) und wählen Sie dann OK.

Die VM synchronisiert ihre Zeit mit dem Host.

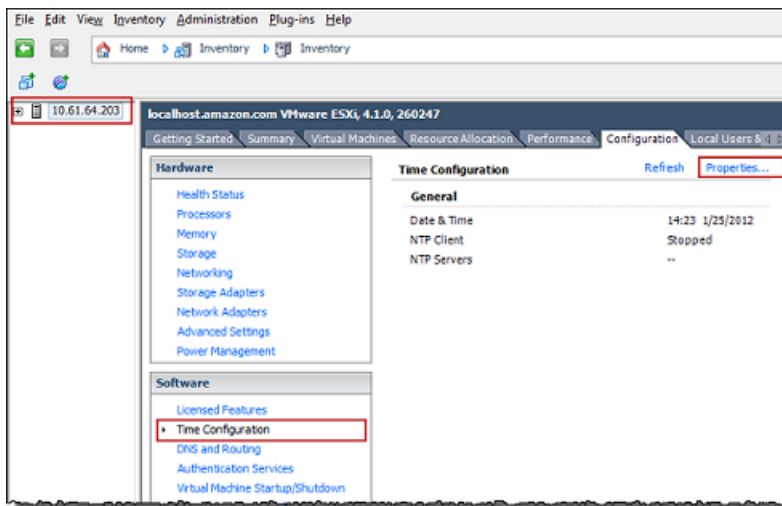


2. Konfigurieren Sie die Host-Zeit.

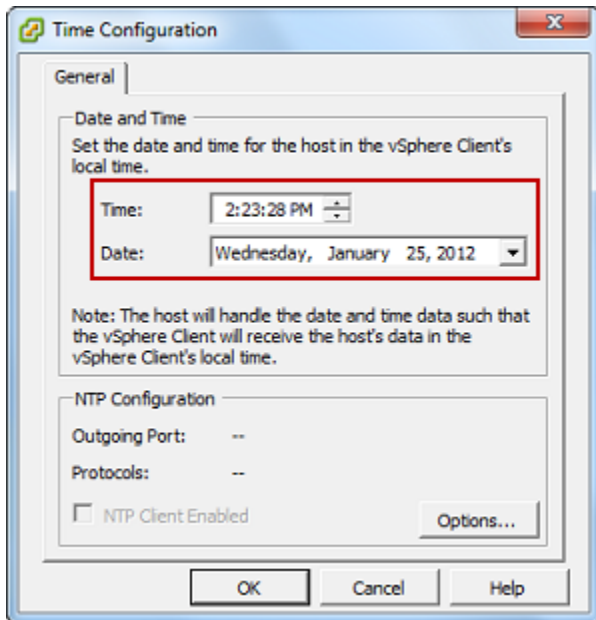
Es muss unbedingt sichergestellt werden, dass die Host-Uhr auf die korrekte Zeit eingestellt ist. Wenn Sie die Host-Uhr noch nicht konfiguriert haben, führen Sie die folgenden Schritte aus, um sie einzurichten und mit einem NTP-Server zu synchronisieren.

- a. Wählen Sie im VMware vSphere-Client den vSphere Host-Knoten im linken Bereich und wählen Sie dann die Registerkarte Configuration (Konfiguration).
- b. Wählen Sie die Option Time Configuration (Zeitkonfiguration) im Bereich Software und wählen Sie dann den Link Properties (Eigenschaften).

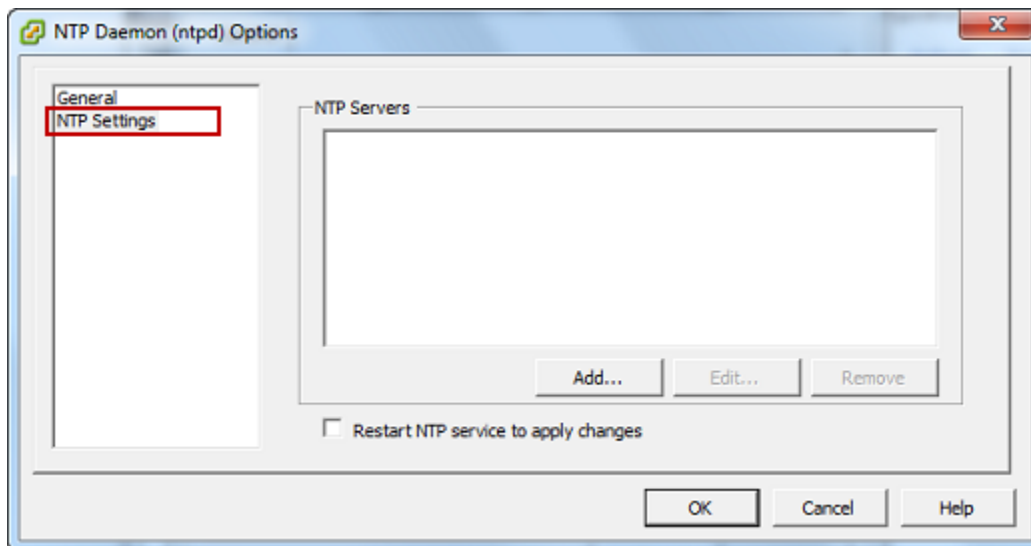
Das Dialogfeld Time Configuration (Zeitkonfiguration) wird geöffnet.



- c. Legen Sie im Bereich Date and Time (Datum und Uhrzeit) das Datum und die Uhrzeit fest.



- d. Konfigurieren Sie den Host so, dass seine Zeit automatisch mit einem NTP-Server synchronisiert wird.
 - i. Wählen Sie Options (Optionen) im Dialogfeld Time Configuration (Zeitkonfiguration) und wählen Sie dann im Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) die Option NTP Settings (NTP-Einstellungen) im linken Bereich.



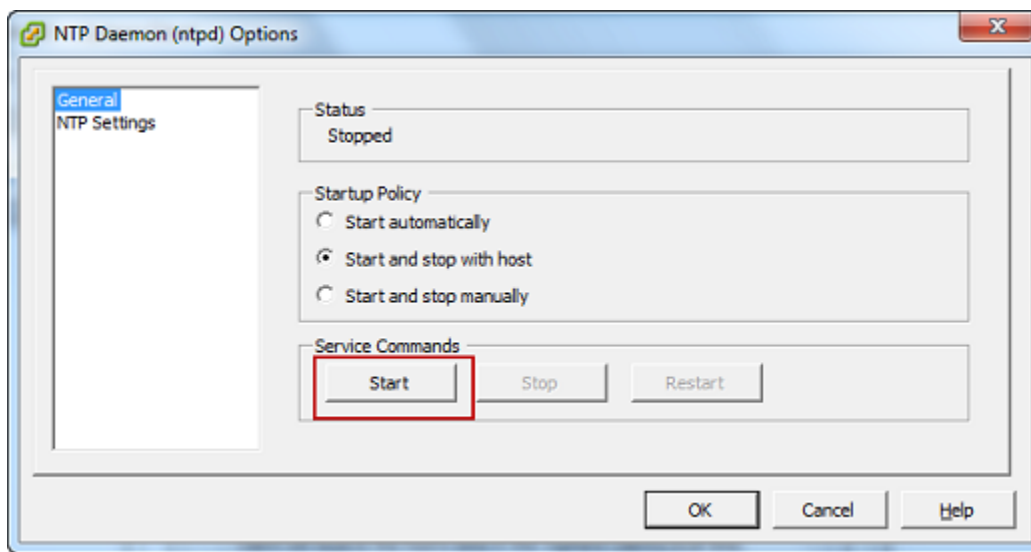
- ii. Wählen Sie Add (Hinzufügen), um einen neuen NTP-Server hinzuzufügen.
- iii. Geben Sie im Dialogfeld Add NTP Server (NTP-Server hinzufügen) die IP-Adresse oder den vollqualifizierten Domännennamen eines NTP-Servers ein und wählen Sie dann OK.

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

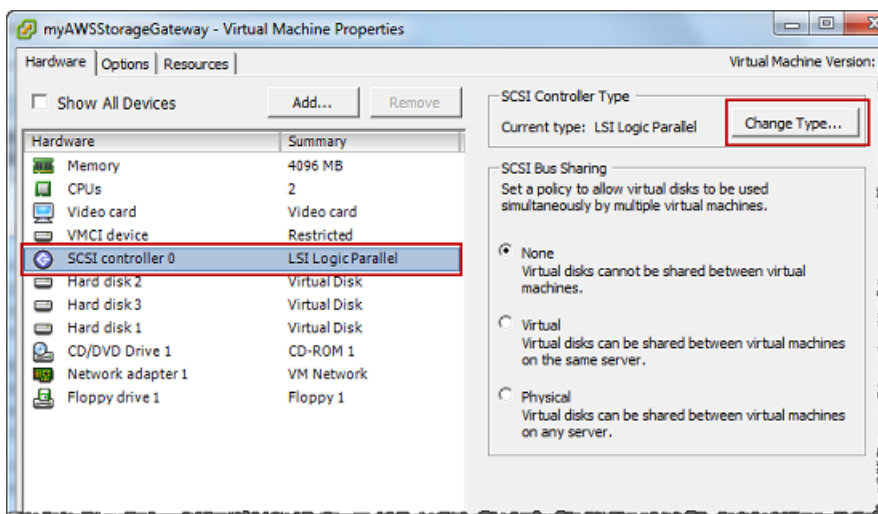
In diesem Schritt legen Sie den iSCSI-Controller so fest, dass die VM Paravirtualisierung verwendet. Paravirtualisierung ist ein Modus, in dem die Gateway-VM mit dem Host-Betriebssystem arbeitet, damit die Konsole die der VM hinzugefügten virtuellen Festplatten identifizieren kann.

Note

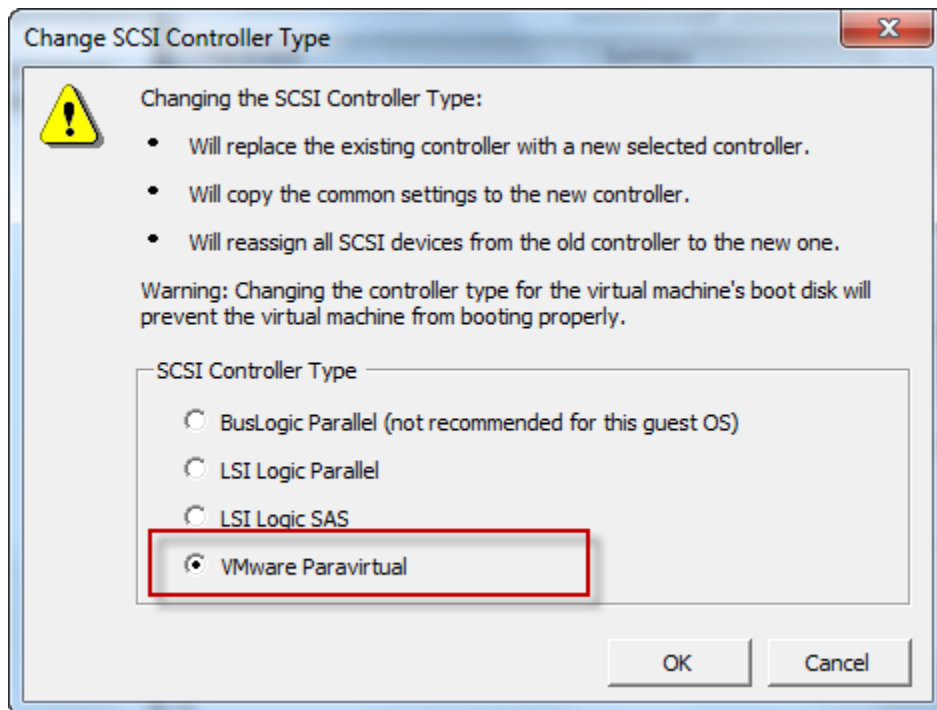
Dieser Schritt ist erforderlich, um Probleme beim Identifizieren dieser Festplatten zu verhindern, wenn Sie sie in der Gateway-Konsole konfigurieren.

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.


```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

3. Geben Sie im Menü System Time Management (Systemzeit-Management) die Option **1** für View and Synchronize System Time (Systemzeit anzeigen und synchronisieren) ein.

```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: _
```

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.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 0.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

Der folgende Screenshot zeigt eine VM, die eine Zeitsynchronisierung erfordert.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 61.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Volume Gateway

Sie können ein auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance bereitstellen und aktivieren. Das AWS Storage Gateway Amazon Machine Image (AMI) ist als Community-AMI verfügbar.

Note

Die AMIs der Storage Gateway-Community werden von AWS veröffentlicht und vollständig unterstützt. Sie können sehen, dass der Herausgeber ist AWS, ein verifizierter Anbieter.

Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Volume Gateway

1. Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter [Einrichten eines Volume 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 Volume Gateway hosten wird.

Note

Die Amazon-EC2-Hostplattform unterstützt nur Cached-Volumes. Gateways für gespeicherte Volumes können nicht auf EC2-Instances bereitgestellt werden.

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 Volume 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 Schlüsselpaar 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 Öffentliche IP automatisch zuweisen Aktivieren aus.
7. Überprüfen Sie im Unterabschnitt Firewall (Sicherheitsgruppen) die vorkonfigurierten Einstellungen. Sie können den Standardnamen und die Beschreibung der neuen Sicherheitsgruppe, die für Ihre Amazon-EC2-Instance erstellt werden soll, ändern, wenn Sie möchten, oder sich dafür entscheiden, stattdessen Firewallregeln aus einer vorhandenen Sicherheitsgruppe anzuwenden.
8. Fügen Sie im Unterabschnitt Eingehende Sicherheitsgruppenregeln Firewallregeln hinzu, um die Ports zu öffnen, über die Clients eine Verbindung zu Ihrer Instance herstellen. Weitere Informationen zu den für erforderlichen Ports finden Sie unter . Weitere Informationen finden Sie unter [Sicherheitsgruppenregeln](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances.

 Note

Volume 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 Volume Gateways.

Sie können die AMI-ID ermitteln, die zum Starten eines Volume Gateway verwendet 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 Volume 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 `/aws/service/storagegateway/ami/CACHED/latest` für zwischengespeicherte Volume Gateways oder `/aws/service/storagegateway/ami/STORED/latest` für gespeicherte Volume Gateways abzufragen. Wenn Sie beispielsweise den folgenden CLI-Befehl verwenden, wird die ID des aktuellen AMI in der von AWS-Region Ihnen angegebenen zurückgegeben.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/STORED/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/STORED/latest",
    "Name": "/aws/service/storagegateway/ami/STORED/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 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 Volume 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 Dropdown-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

Standard- instellungen	AMI-Root- Volume	Volume 2 Cache	Volume 3 Cache			
Gerätenamen		/dev/sdf	/dev/sdf			
Größe	80 GiB	250 GiB	250 GiB			
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 sitzungorientierte 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.

Volume Gateway

Themen

- [Entfernen von Datenträgern aus dem Gateway](#)
- [Hinzufügen und Entfernen von Amazon-EBS-Volumes für Ihr in Amazon EC2 gehostetes Gateway](#)

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.

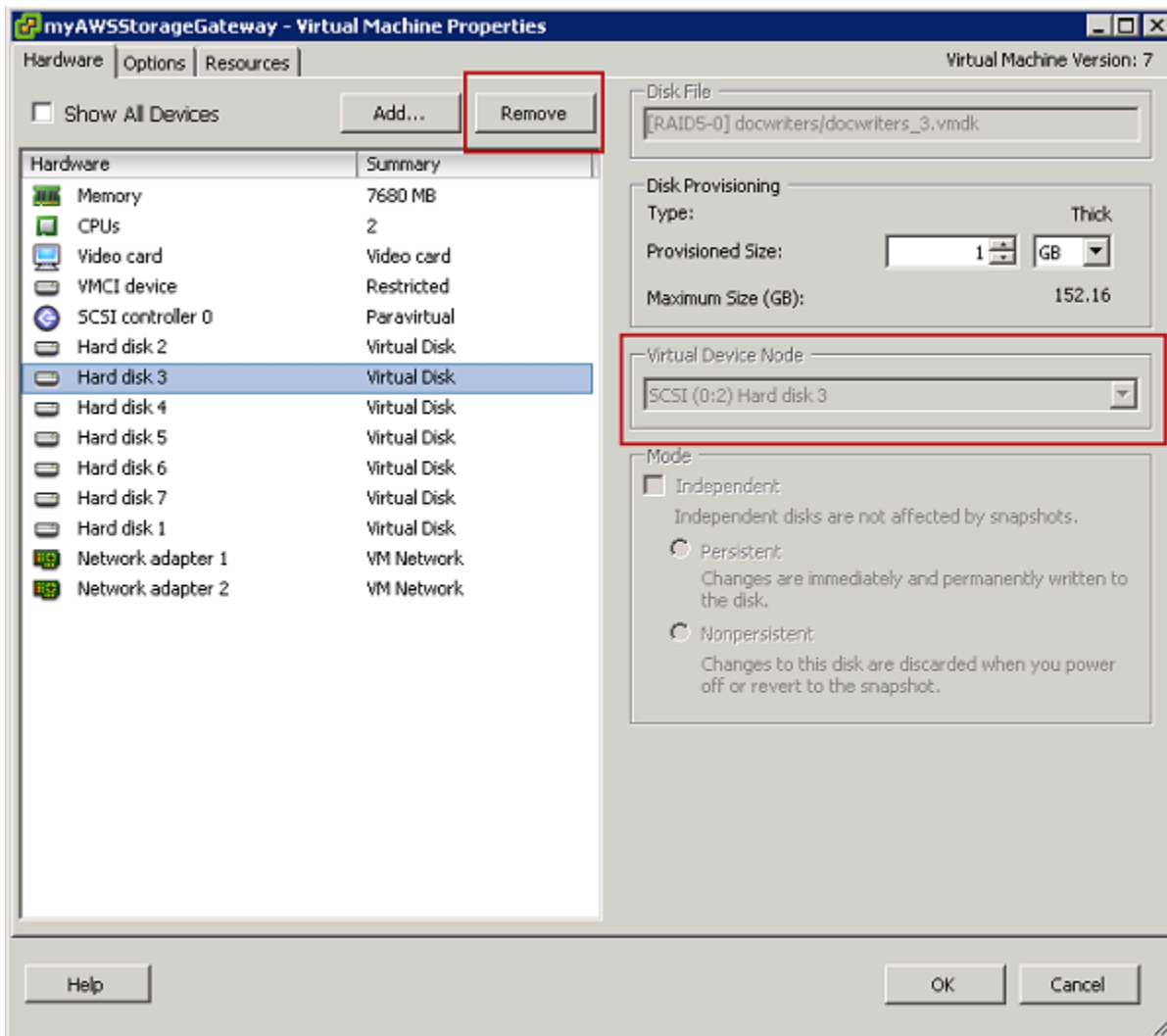
Entfernen eines Datenträgers aus einem auf VMware ESXi gehosteten Gateway

Sie können mit dem folgenden Verfahren einen Datenträger aus dem auf VMware-Hypervisor gehosteten Gateway entfernen.

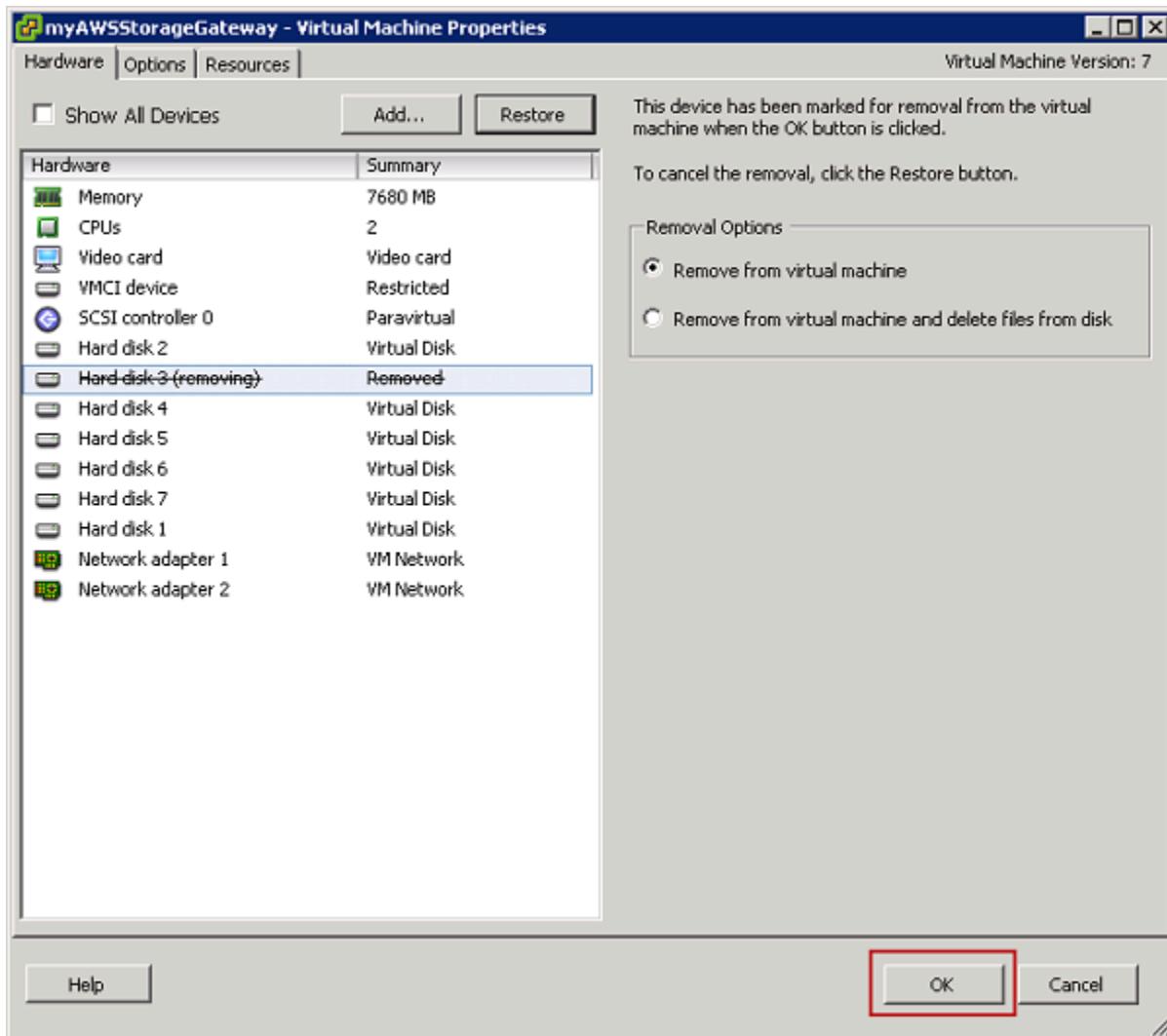
So entfernen Sie einen Datenträger für den Upload-Puffer (VMware ESXi)

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 Geräteknotten 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.

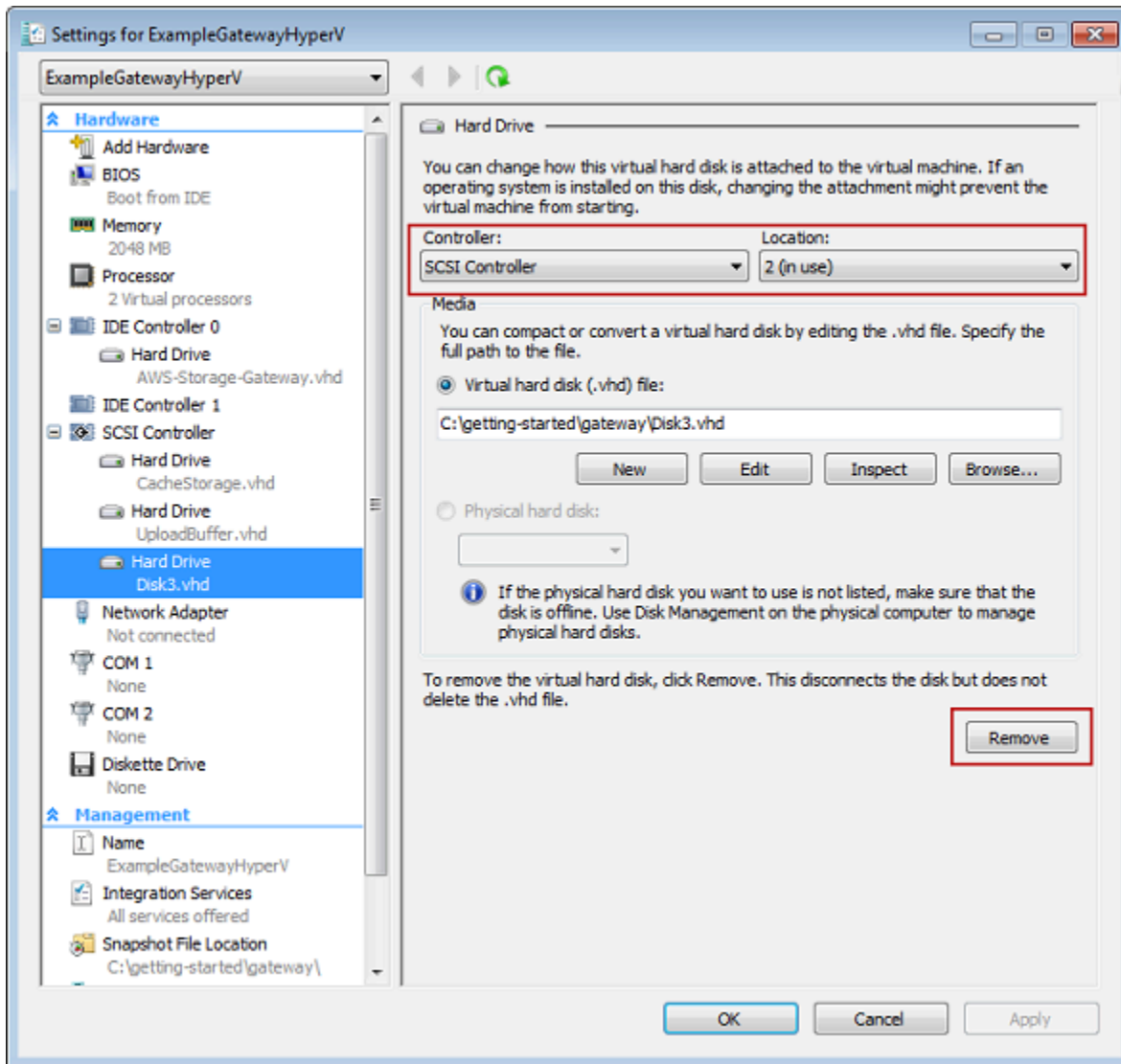
So löschen Sie einen zugrunde liegenden Datenträger für den Upload-Puffer (Microsoft Hyper-V)

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.

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.

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 \(curl\)](#)
- [Linux \(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)
- [Verwenden der lokalen Konsole](#)

Linux (curl)

In den folgenden Beispielen wird gezeigt, wie Sie mithilfe von Linux (curl) einen Aktivierungsschlüssel abrufen.

Note

Ersetzen Sie die hervorgehobenen Variablen durch tatsächliche Werte für Ihr Gateway. Zulässige Werte sind:

- `gateway_ip_address`: 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

- [Verbinden eines Windows-Clients mit Volumes](#)
- [Verbinden von Volumes oder VTL-Geräten mit einem Linux-Client](#)
- [Anpassen von iSCSI-Einstellungen](#)
- [Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele](#)

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.

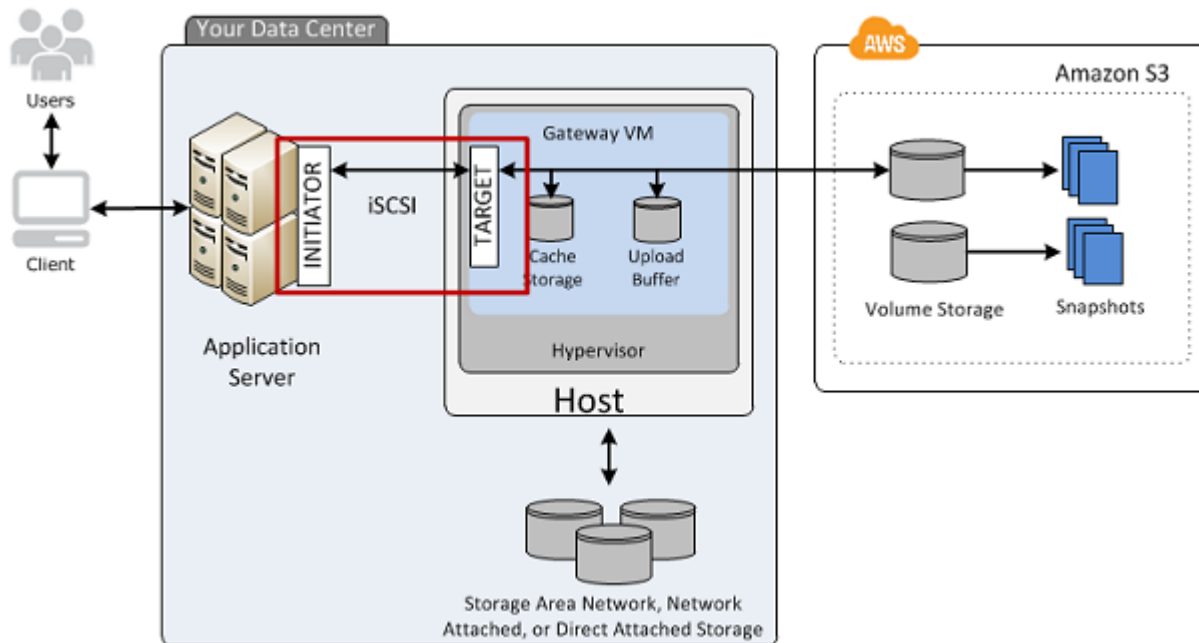
Verbinden eines Windows-Clients mit Volumes

Ein Volume Gateway macht alle Volumes, die Sie für dieses Gateway erstellt haben, als iSCSI-Ziele verfügbar. Weitere Informationen finden Sie unter [Verbinden Ihrer Volumes mit Ihrem Client](#).

Note

Damit Ihr Gateway eine Verbindung zu einem Volume-Ziel herstellen kann, müssen Sie für das Gateway einen Upload-Puffer konfigurieren. Wenn Sie keinen Upload-Puffer für das Gateway konfigurieren, wird als Status Ihrer Volumes `UPLOAD BUFFER NOT CONFIGURED` angezeigt. Wie Sie einen Upload-Puffer für ein Gateway in der Stored Volume-Konfiguration konfigurieren, können Sie unter [So konfigurieren Sie zusätzlichen Upload-Puffer oder Cache-Speicher für Ihr Gateway](#) nachlesen. Wie Sie einen Upload-Puffer für ein Gateway in der Cached Volume-Konfiguration konfigurieren, ist unter [So konfigurieren Sie zusätzlichen Upload-Puffer oder Cache-Speicher für Ihr Gateway](#) beschrieben.

Die folgende Abbildung verdeutlicht die Position des iSCSI-Ziels im größeren Zusammenhang der Storage-Gateway-Architektur. Weitere Informationen finden Sie unter [So funktioniert Volume Gateway \(Architektur\)](#).



Sie können entweder über einen Windows-Client oder über einen Red Hat Linux-Client eine Verbindung mit Ihrem Volume herstellen. Für beide Client-Typen lässt sich optional CHAP konfigurieren.

Ihr Gateway macht Ihr Volume als iSCSI-Ziel verfügbar, unter einem benutzerdefinierten Namen, dem `iqn.1997-05.com.amazon:` vorangestellt wird. Wenn Sie für Ihr Ziel beispielsweise den Namen `myvolume` festlegen, lautet der Name des iSCSI-Ziels, über das die Verbindung mit dem Volume hergestellt wird, `iqn.1997-05.com.amazon:myvolume`. Weitere Informationen dazu, wie Sie Ihre Anwendungen so konfigurieren können, dass Volumes über iSCSI gemountet werden, finden Sie unter [Verbinden eines Windows-Clients mit Volumes](#).

Bis	Siehe
Herstellen einer Volume-Verbindung unter Windows	Herstellen einer Verbindung mit einem Microsoft Windows-Client
Herstellen einer Volume-Verbindung unter Red Hat Linux	Herstellen einer Verbindung mit Red Hat Enterprise Linux-Client
Konfigurieren der CHAP-Authentifizierung unter Windows und Red Hat Linux	Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele

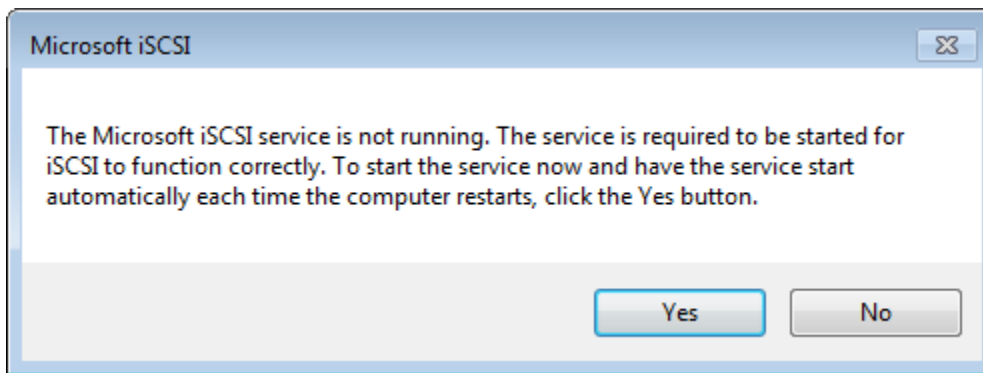
Einen Windows-Client verbinden Sie wie folgt mit einem Speicher-Volume:

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.

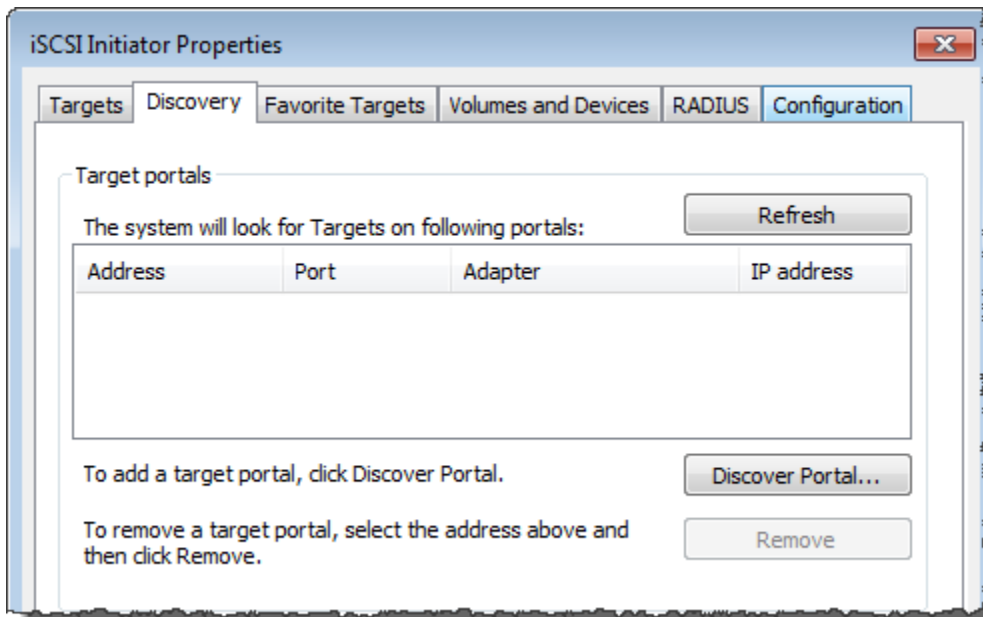
Note

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

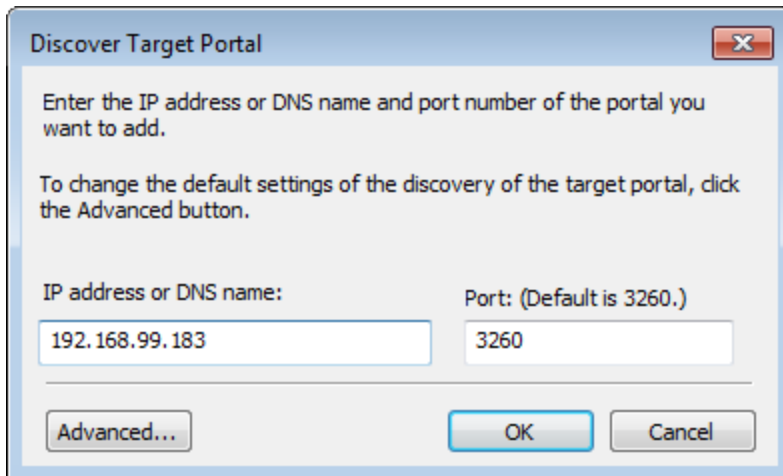
2. Klicken Sie bei Aufforderung auf Ja, um den Microsoft iSCSI-Dienst zu starten.



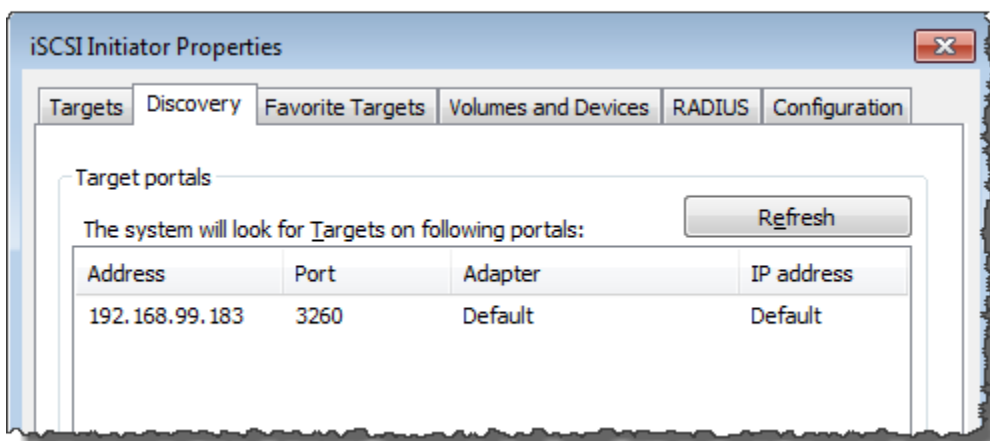
3. Wählen Sie im Dialogfeld iSCSI Initiator-Eigenschaften die Registerkarte Ermittlung aus und klicken Sie dann auf Portal ermitteln.



4. Geben Sie im Dialogfeld Zielportal ermitteln unter IP-Adresse oder DNS-Name die IP-Adresse Ihres iSCSI-Ziels ein und wählen Sie OK aus. 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.



Die IP-Adresse wird jetzt in der Liste Zielportale auf der Registerkarte Ermittlung aufgeführt.



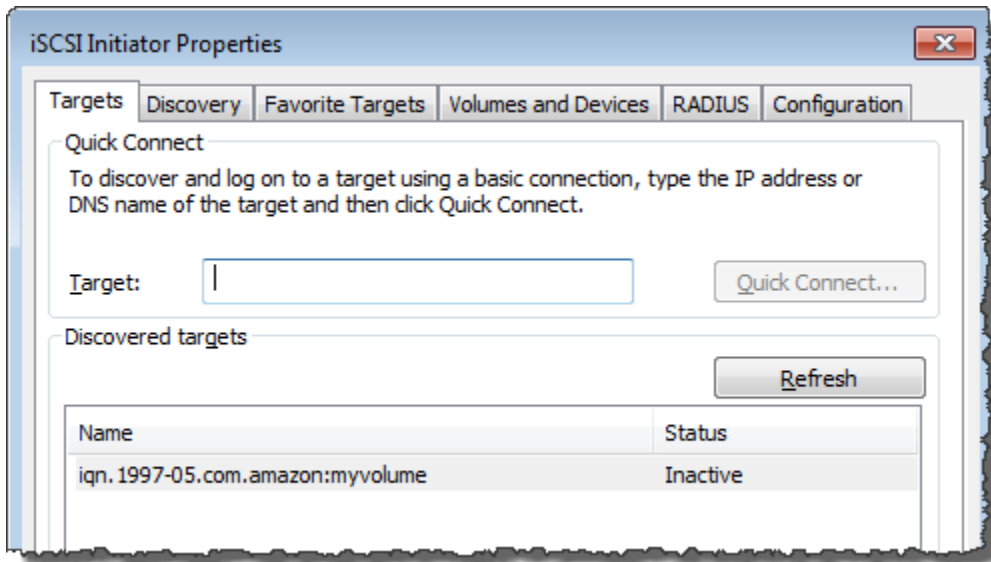
Warning

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. Verbinden Sie das neue Zielportal mit dem Speicher-Volume-Ziel auf dem Gateway:

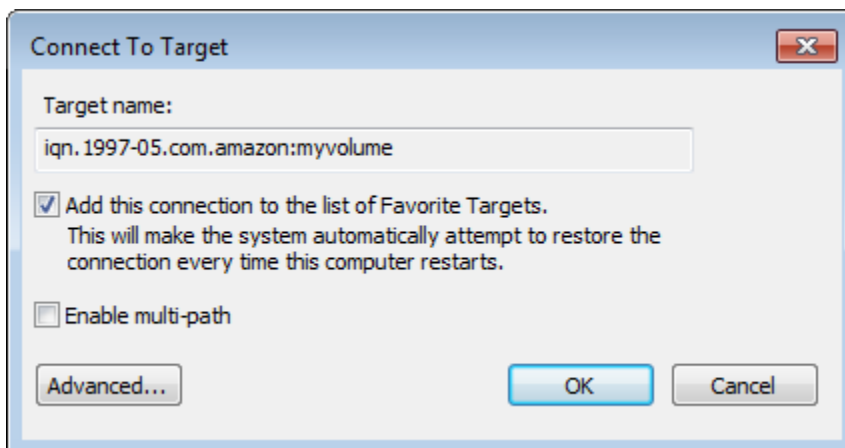
- a. Wählen Sie die Registerkarte Ziele.

Das neue Zielportal wird mit dem Status "Inaktiv" angezeigt. Der angezeigte Zielname sollte der Name sein, den Sie in Schritt 1 für Ihr Speicher-Volume festgelegt haben.

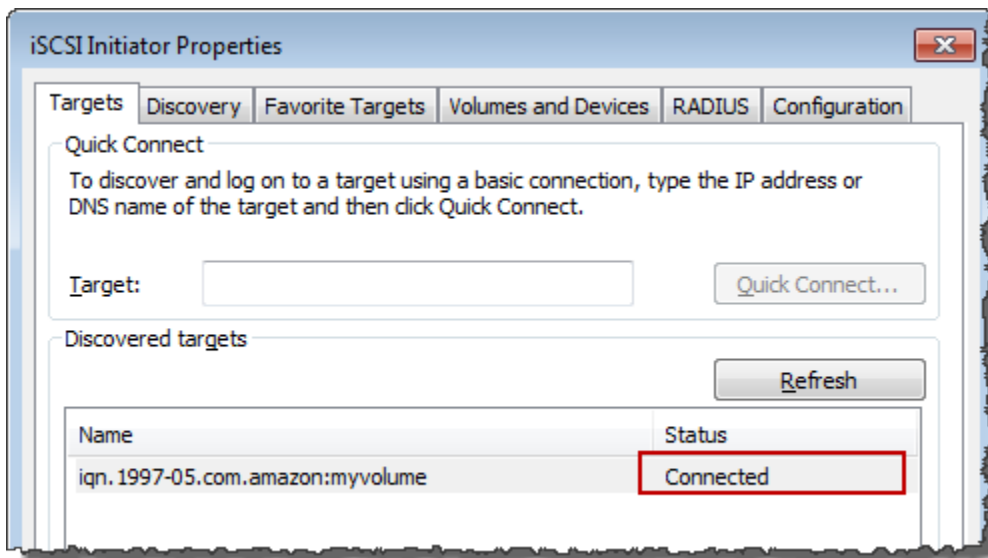


- b. Wählen Sie das Ziel und klicken Sie auf Connect (Verbinden).

Wenn der Zielname noch nicht ausgefüllt ist, geben Sie den Namen des Ziels ein, wie in Schritt 1 gezeigt. Wählen Sie im Dialogfeld Mit Ziel verbinden die Option Diese Verbindung zur Liste der bevorzugten Ziele hinzufügen aus, und klicken Sie dann auf OK.



- c. Vergewissern Sie sich auf der Registerkarte Ziele, dass für das Ziel Status der Wert Verbunden angezeigt wird (d. h. dass eine Verbindung zum Ziel besteht), und klicken Sie auf OK.



Nun können Sie dieses Speicher-Volume für Windows initialisieren und formatieren, damit Sie Daten in ihm speichern können. Dazu verwenden Sie die Windows-Datenträgerverwaltung.

Note

Obwohl es im Rahmen dieser Übung nicht erforderlich ist, empfehlen wir Ihnen dringend, Ihre iSCSI-Einstellungen wie unter [Anpassen der Windows iSCSI-Einstellungen](#) beschrieben für eine reale Anwendung anzupassen.

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 Eigenschaftsbereich 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

Wenn Sie einen Windows-Client verwenden, verwenden Sie den Microsoft iSCSI-Initiator für die Verbindung zu Ihrem Gateway-Volume. Anleitungen zum Verbinden Ihrer Volumes finden Sie unter [Verbinden Ihrer Volumes mit Ihrem Client](#).

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.

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 eindeutigen 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.

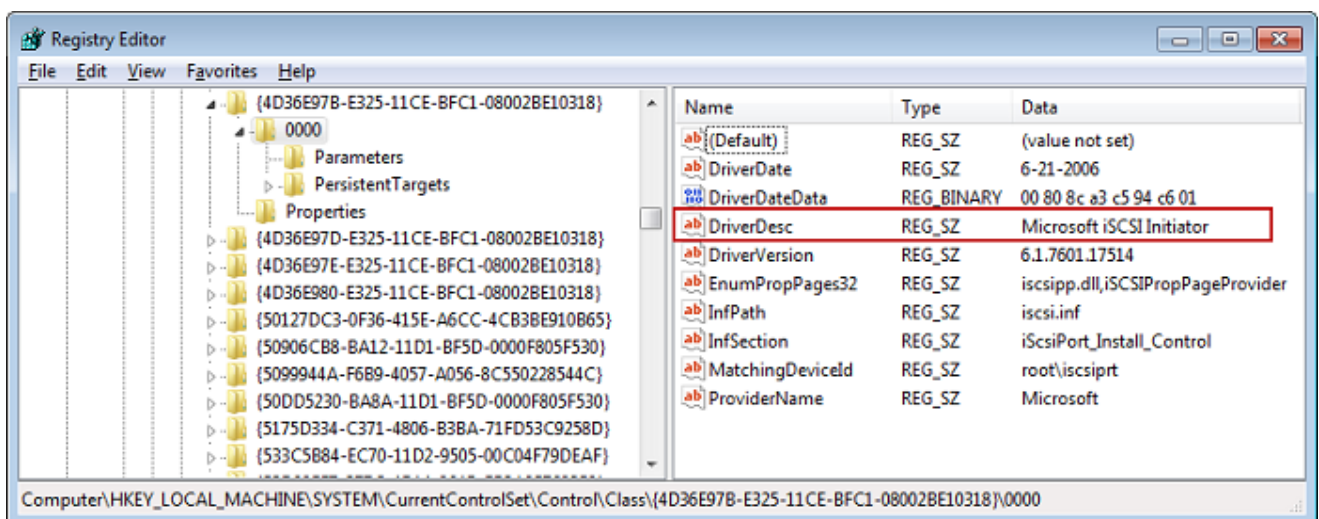
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

- 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.

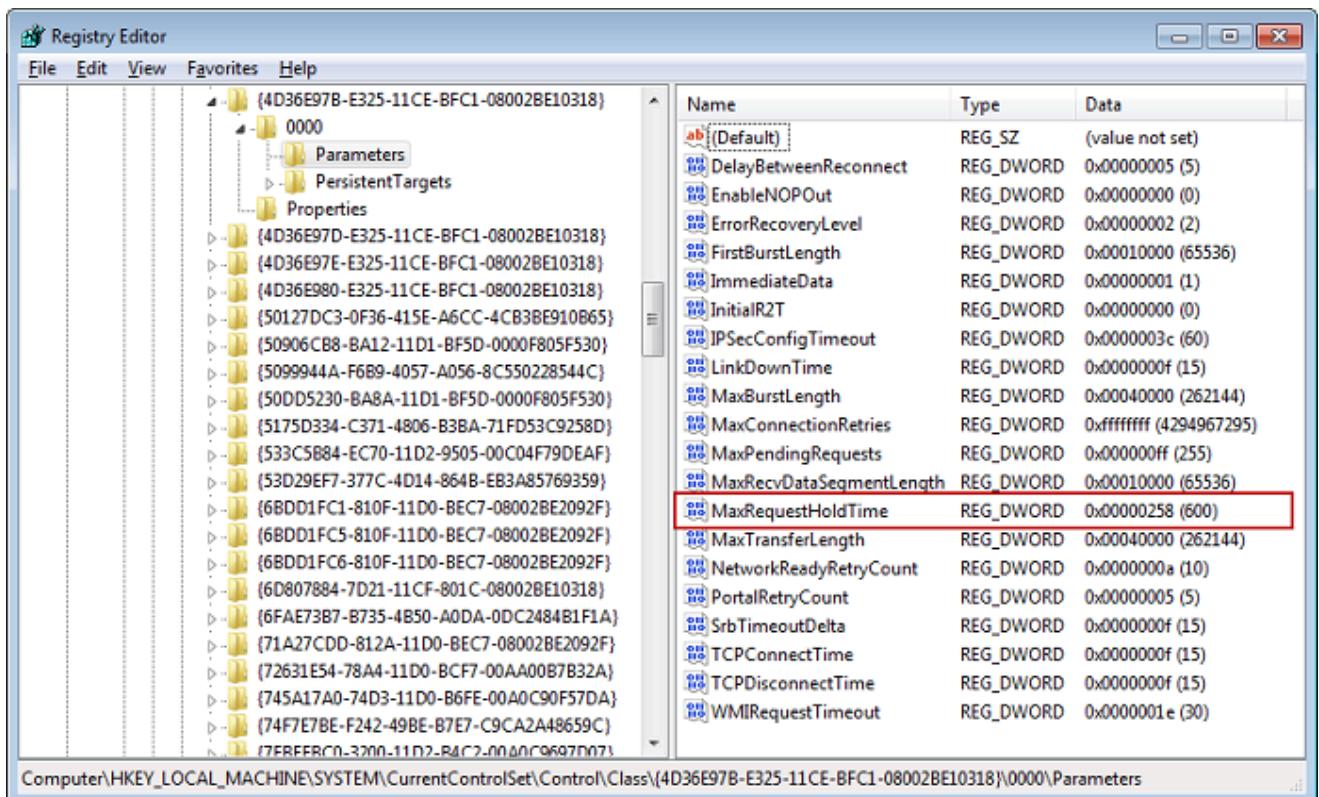
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number>]
```

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 indem Sie die Zeichenfolge mit dem DriverDesc Wert Microsoft iSCSI Initiator prüfen, so wie im folgenden Beispiel beschrieben.



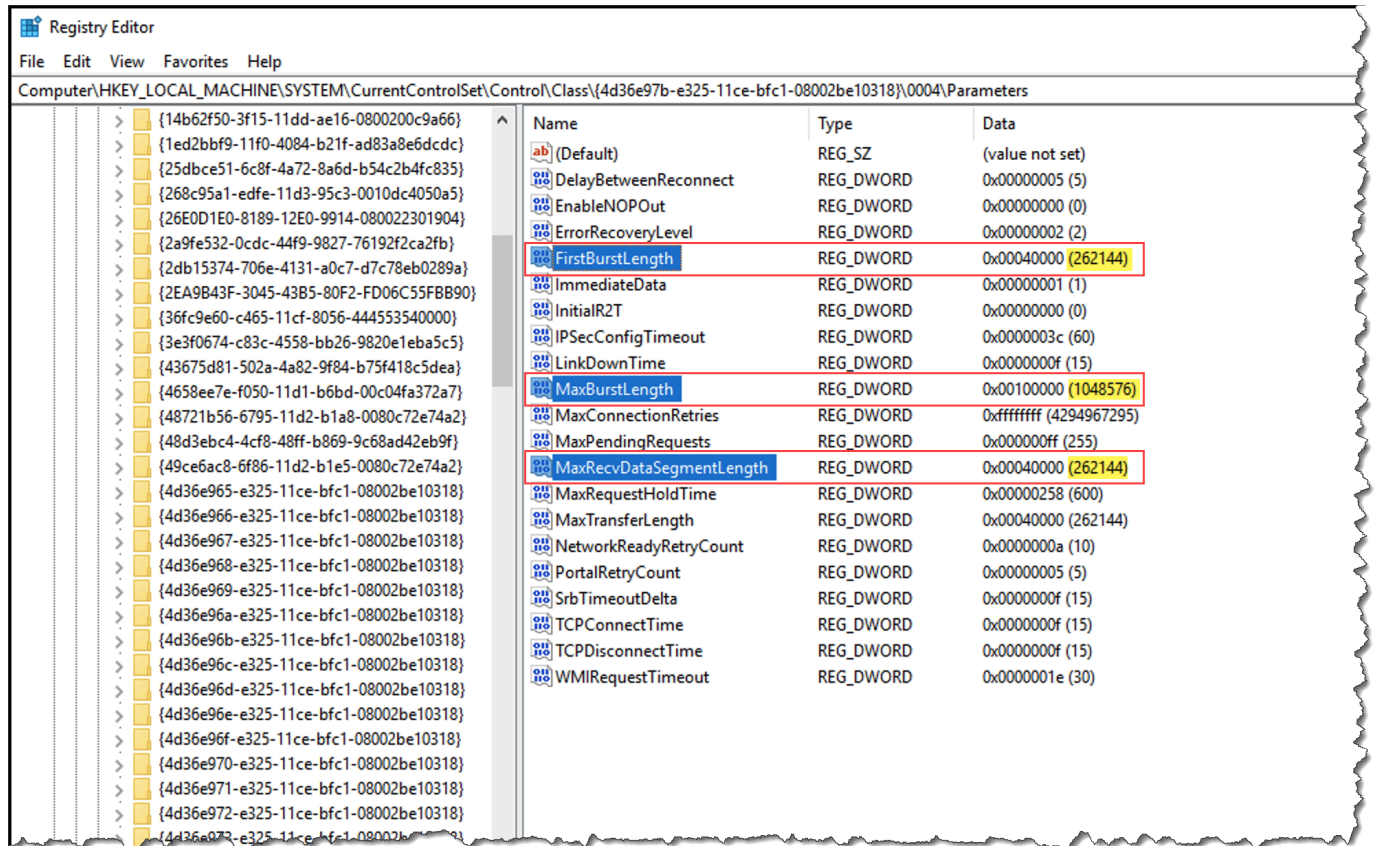
- d. Um die iSCSI-Einstellungen anzuzeigen, wählen Sie den Unterschlüssel Parameters (Parameter) aus.
- e. Öffnen Sie das Kontextmenü (rechte Maustaste) für den MaxRequestHoldTime DWORD-Wert (32-Bit), wählen Sie Ändern und ändern Sie dann den Wert in **600**.

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 Schreibenforderung 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

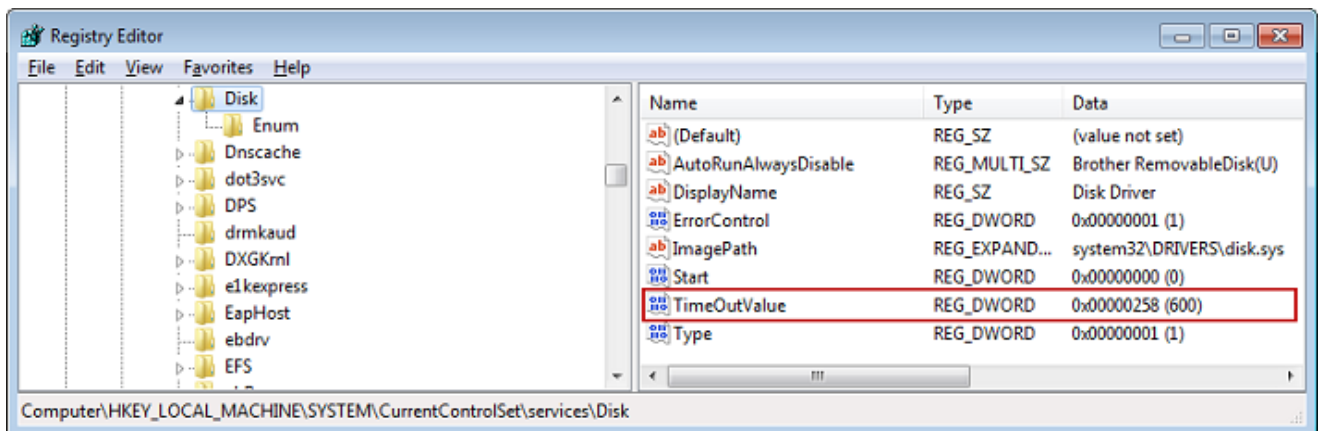
Unterschiedliche Backup-Software kann optimiert werden, um mit verschiedenen iSCSI-Einstellungen möglichst gut zu funktionieren. Informationen zur Überprüfung, welche Werte für diese Parameter die beste Leistung bieten, finden Sie in der Dokumentation zu Ihrer Backup-Software.

- Erhöhen Sie den Datenträger-Timeout-Wert, der wie folgt angezeigt wird:
 - Starten Sie den Registrierungs-Editor (Regedit.exe), falls Sie dies noch nicht getan haben.
 - 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-Geräteziel 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 Volume-Ziel 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 Volume-Ziel in der Storage-Gateway-Konsole

In dieser Anleitung geben Sie zwei geheime Schlüssel an, die verwendet werden, um vom Volume zu lesen und in das Volume zu schreiben. Dieselben Schlüssel werden auch in der Anleitung zur Konfiguration des Client-Initiators verwendet.

1. Klicken Sie in der Storage-Gateway-Konsole im Navigationsbereich auf Volumes.
2. Wählen Sie für Aktionen die Option CHAP-Authentifizierung konfigurieren aus.
3. 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-volume-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.

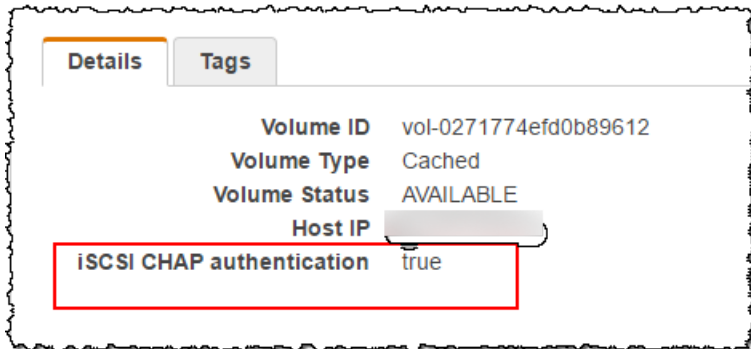
- c. Geben Sie unter Für Authentifizierung des Ziels verwendeter geheimer Schlüssel (wechselseitige CHAP-Authentifizierung) den entsprechenden geheimen Schlüssel ein.

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.
4. Wechseln Sie auf die Registerkarte Details und vergewissern Sie sich, dass iSCSI CHAP authentication (iSCSI CHAP-Authentifizierung) 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.

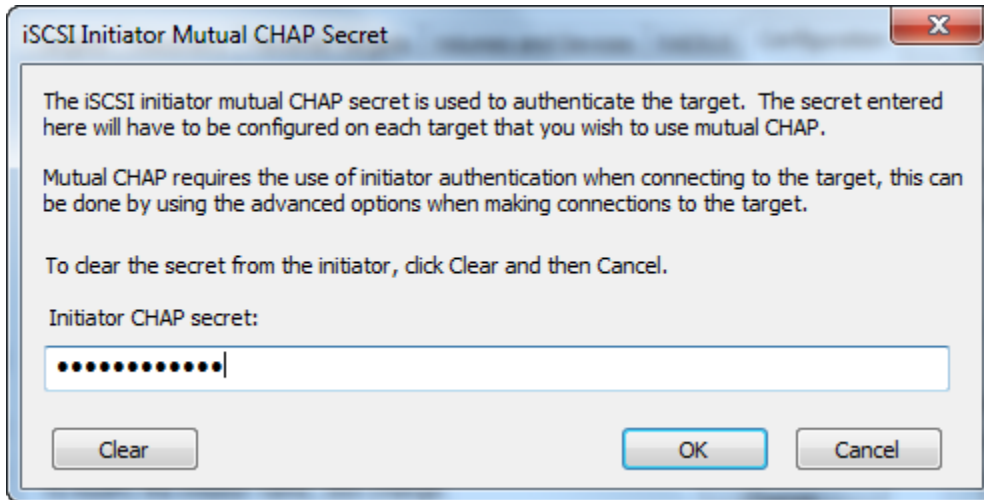
1. Falls der iSCSI-Initiator noch nicht ausgeführt wird, klicken Sie im Menü Start Ihres Windows-basierten Client-Computers auf Ausführen, geben Sie **iscsicpl.exe** ein und klicken Sie dann auf OK, um das Programm auszuführen.
2. Konfigurieren Sie die wechselseitige CHAP-Authentifizierung für den Initiator (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.

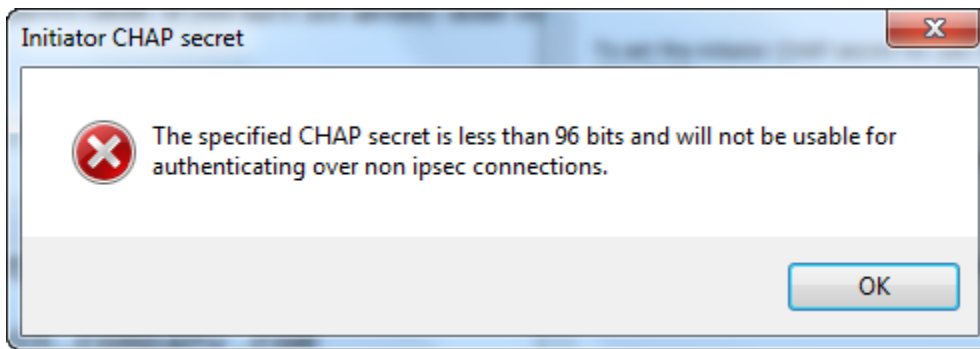
- b. Klicken Sie auf CHAP.
- c. Geben Sie im Dialogfeld iSCSI-Initiator: Geheimer Schlüssel für wechselseitige CHAP-Authentifizierung den geheimen Schlüssel für die wechselseitige CHAP-Authentifizierung ein.



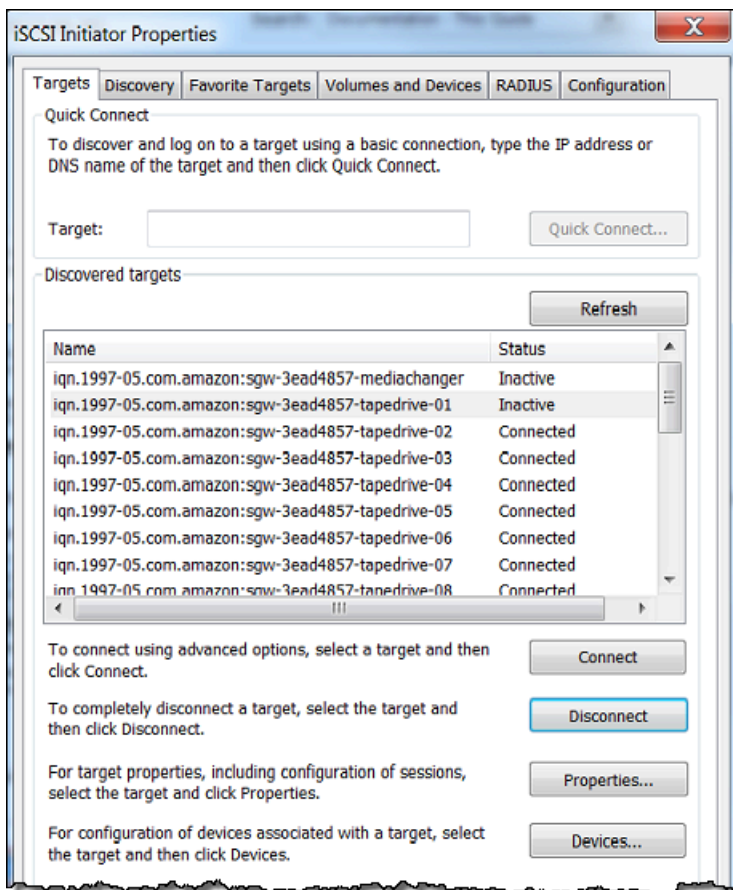
In diesem Dialogfeld geben Sie den geheimen Schlüssel ein, den der Initiator (Windows-Client) zur Authentifizierung des Ziels (Speicher-Volume) verwendet. Dieser geheime Schlüssel gewährt dem Ziel Lese- und Schreibrechte für den Initiator. Es handelt sich hierbei um denselben geheimen Schlüssel, den 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.

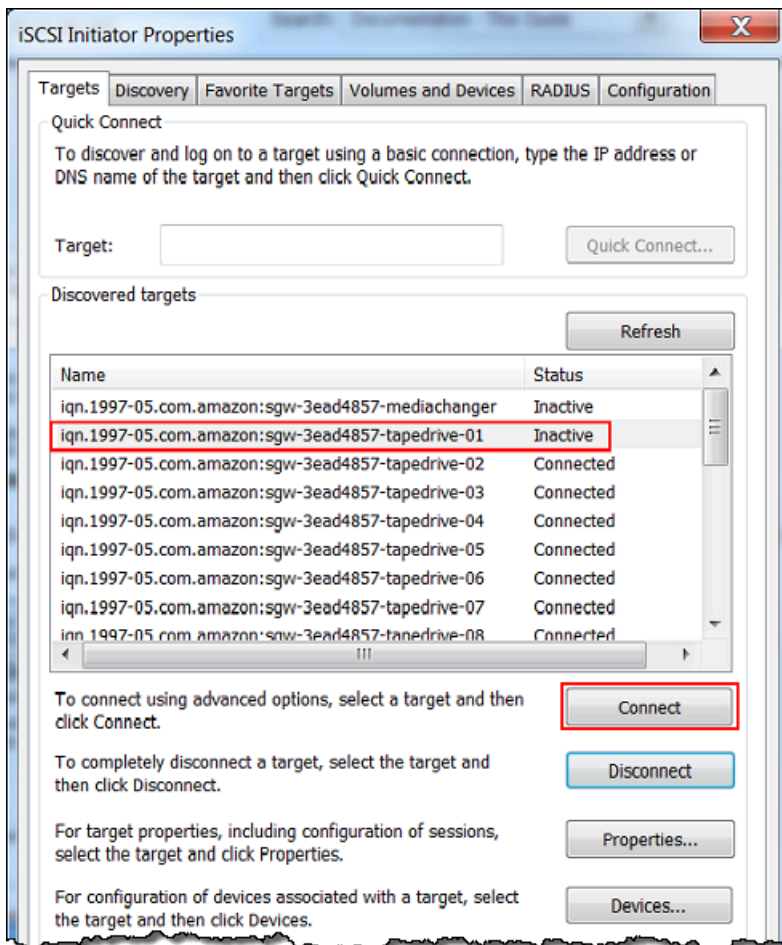
Klicken Sie auf OK und geben Sie den Schlüssel erneut ein.



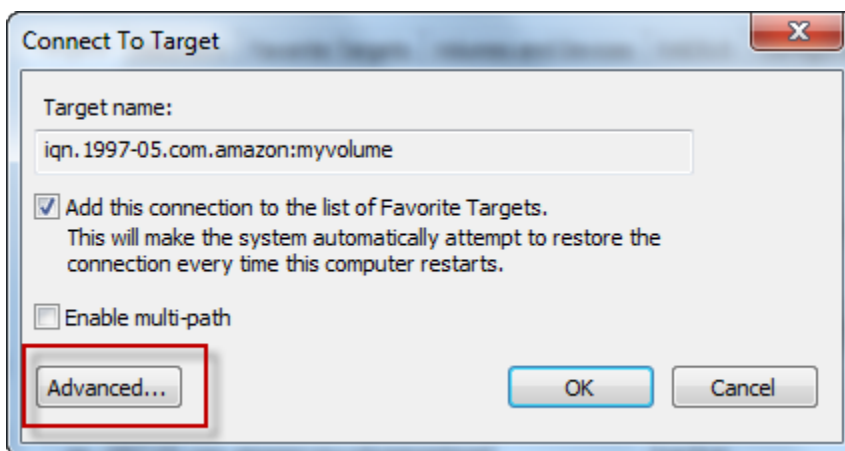
3. Konfigurieren Sie das Ziel mit dem geheimen Schlüssel des Initiators, um die Konfiguration der wechselseitigen CHAP-Authentifizierung abzuschließen:
 - a. Wählen Sie die Registerkarte Ziele.



- 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).

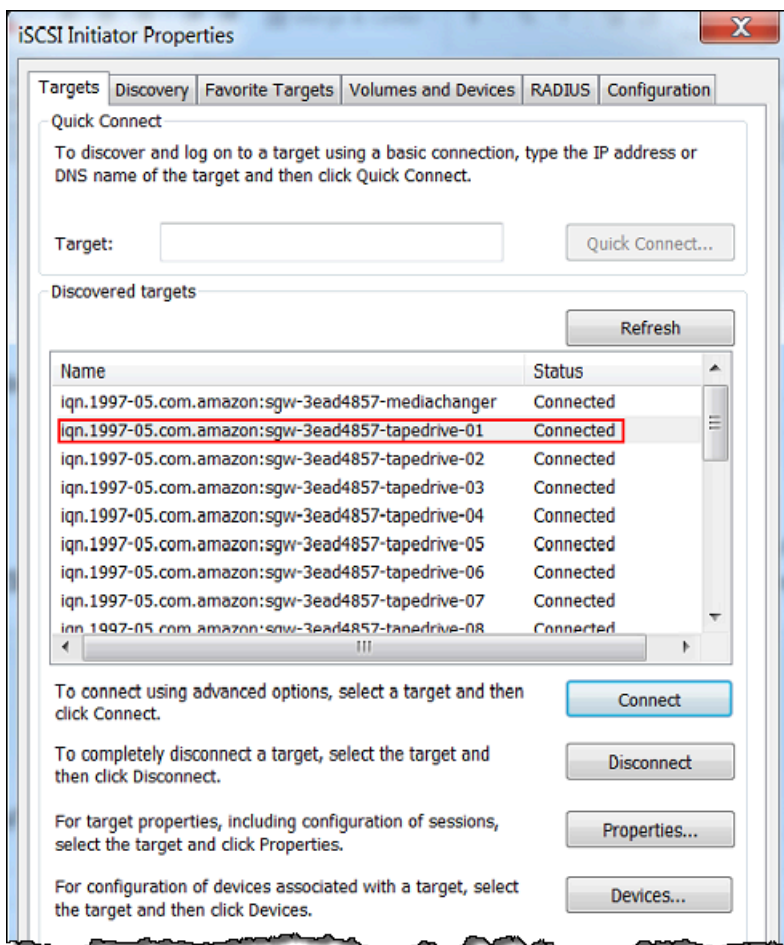


- d. Klicken Sie im Dialogfeld Connect to Target (Mit Ziel verbinden) auf Advanced (Erweitert).



- 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 Red Hat Enterprise 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
<i>username</i> (<i>Benutzername</i>)	Gibt den Initiatornamen an, den Sie im vorherigen Schritt der Anleitung abgerufen haben. Der Wert beginnt mit <code>iqn.1994-05.com.redhat:8e89b27b5b8</code> ist beispielsweise ein gültiger Wert für <code>username</code> .
<i>password</i>	Gibt den geheimen Schlüssel an, der zur Authentifizierung des Initiators (also des verwendeten Clients) verwendet wird, wenn dieser mit dem Volume kommuniziert.

Konfigurationseinstellung	Wert
<i>username_in</i>	Gibt den IQN des Ziel-Volumes an. Der Wert beginnt mit <code>iqn</code> und endet mit dem Namen des Ziels. iqn.1997-05.com.amazon:myvolume ist beispielsweise ein gültiger Wert für <i>username_in</i> .
<i>password_in</i>	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 Red Hat Enterprise 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 .

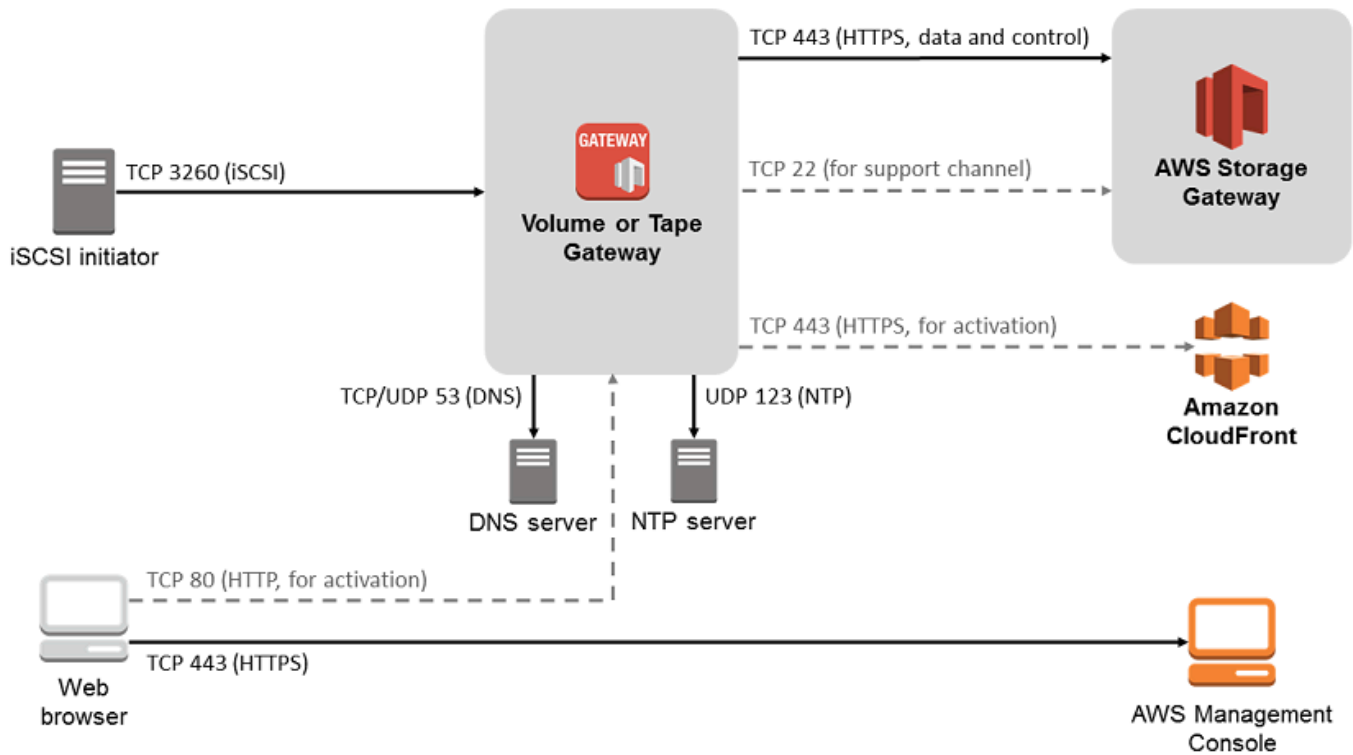
Weitere Informationen zu AWS Direct Connect finden Sie unter [Was ist AWS Direct Connect?](#) im AWS Direct Connect -Benutzerhandbuch.

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 Volume Gateway.

Volume Gateway

Die folgende Abbildung zeigt die Ports, die für den Betrieb von Gateways vom Typ Volume 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)	<p>Von lokalen Systemen zum Abrufen des Storage-Gateway-Aktivierungsschlüssels. Port 80 wird nur während der Aktivierung einer Storage-Gateway-Appliance verwendet.</p> <p>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</p>	

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)	<p>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:</p> <ul style="list-style-type: none"> • 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 Volume 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 verfügbaren 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: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
Volume-ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /volume/ <i>volume-id</i>
Ziel-ARN (iSCSI-Ziel)	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSItarget</i>

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 Tags und 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 Volumes](#)
- [Empfohlene Kapazität für die lokalen Datenträger des Gateways](#)

Kontingente für Volumes

In der folgenden Tabelle sind Kontingente für Volumes aufgeführt.

Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
Maximalgröße eines Volumes	32 TiB	16 TiB

Note

Wenn Sie einen Snapshot von einem zwischengespeicherten Volume erstellen, das größer als 16 TiB ist, können Sie das Volume in ein Storage Gateway-Volume wiederherstellen. Eine Wiederherstellung in ein Amazon Elastic Block

Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
Store (Amazon EBS)-Volume ist jedoch nicht möglich.		
Maximale Anzahl von Volumes pro Gateway	32	32
Gesamtgröße aller Volumes pro Gateway	1,024 TiB	512 TiB

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
Gateway für zwischengespeicherte Volumes	150 GiB	64 TiB	150 GiB	2 TiB	—
Gateway für gespeicherte Volumes	—	—	150 GiB	2 TiB	1 oder mehr für gespeicherte Volumes oder Volumes

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](#)
- [Signieren von Anforderungen](#)
- [Fehlermeldungen](#)
- [Aktionen](#)

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 [-ActivateGateway](#) Operation verwendet werden.

```

POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway

```

Die folgenden Kopfzeilen müssen mit in den POST-Abfragen an 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	<p>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):</p> <pre> Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd/region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i> </pre> <p>In der vorherigen Syntax geben Sie , <i>YourAccessKey</i> das Jahr, den Monat und den Tag (<i>jjjjmmdd</i>), die Region und die <i>anCalculatedSignatur</i>e. 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.</p>
Content-Type	<p>Verwenden Sie <code>application/x-amz-json-1.1</code> als Inhaltstyp für alle Abfragen an Storage Gateway.</p> <pre> Content-Type: application/x-amz-json-1.1 </pre>

Header	Beschreibung
Host	<p>Verwenden Sie den Host-Header, um den Storage Gateway-Endpunkt anzugeben, an den Sie die Abfrage senden. <code>storagegateway.us-east-2.amazonaws.com</code> 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.</p> <pre data-bbox="475 569 1507 646">Host: storagegateway. <i>region</i>.amazonaws.com</pre>
x-amz-date	<p>Sie müssen den Zeitstempel entweder im HTTP-DateHeader oder im AWS <code>x-amz-date</code> -Header angeben. (Einige HTTP-Client-Bibliotheken lassen den Header <code>Date</code> nicht zu.) Ist der Header <code>x-amz-date</code> vorhanden, ignoriert das Storage Gateway System bei der Abfrageauthentifizierung alle Header des Typs <code>Date</code>. Das Format <code>x-amz-date</code> muss ISO8601 Basic dem Format <code>JJJJMMTT'T'HHMMSS'Z'</code> entsprechen. Wenn sowohl der <code>Date</code>- als auch der <code>x-amz-date</code> -Header verwendet werden, muss das Format des Datum-Headers nicht ISO8601 entsprechen.</p> <pre data-bbox="475 1178 1507 1255">x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>
x-amz-target	<p>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.</p> <pre data-bbox="475 1541 1507 1619">x-amz-target: StorageGateway_ <i>APIversion</i> .<i>operationName</i></pre> <p>Der Wert <code>operationName</code> (z. B. „ActivateGateway“) finden Sie in der API-Liste API-Referenz für Storage Gateway.</p>

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
92c0efffa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

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

- [Ausnahmen](#)
- [Operationsfehlercodes](#)
- [Fehlermeldungen](#)

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 zurückgeben. 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
<code>IncompleteSignatureException</code>	Die angegebene Signatur ist unvollständig.	400 Ungültige Anfrage
<code>InternalFailure</code>	Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.	500 Internal Server Error
<code>InternalServerError</code>	Eine der Operationsfehlercode-Nachrichten Operationsfehlercodes .	500 Internal Server Error
<code>InvalidAction</code>	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-Minutenschritten) 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 unbekannt 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 überschritten.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
NetworkConfigurationChanged	Die Gateway-Netzwerkconfiguration 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 angegebene 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 Volume 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 .	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 Konfigurationseinstellungen wurden auch für HealthNotifications	2. Oktober 2023

und AvailabilityNotifications aktualisiert.

Weitere Informationen finden Sie unter [Grundlegendes zu CloudWatch Alarmen](#).

[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 relevanten Verfahren in diesem Handbuch wurden aktualisiert, um die neuen Funktionen 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 Einrichtung 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 zwischengespeicherte Volume und Tape Gateways und verbessert so die Leistung für On-Premises-Anwendungen, indem der Zugriff mit geringer Latenz auf größere Arbeitsdatensätze ermöglicht wird. Weitere Informationen finden Sie unter Empfohlene lokale Festplattengrößen für Ihr Gateway .	9. November 2020

Gateway-Migration

Storage Gateway unterstützt jetzt die Migration zwischengespeicherter Volume Gateways auf neue virtuelle Maschinen. Weitere Informationen finden Sie unter [Verschieben zwischengespeicherter Volumes auf eine neue virtuelle zwischengespeicherte 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 [. CloudWatch](#)

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 Informationen finden Sie unter [Sichern Ihrer Volumes](#).

16. Januar 2019

[Unterstützung für Bacula Enterprise und IBM Spectrum Protect](#)

Tape Gateways unterstützen 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-Appliance 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 Data Protection Manager \(DPM\)](#)

Tape Gateways sind jetzt mit dem Microsoft System Center 2016 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 DataCenter/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 Informationen 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-Speicherklasse	Für File Gateways können Sie jetzt die S3 One Zone_IA als Standard-Speicherklasse für Ihre Dateifreigaben wählen. Diese Speicherklasse ermöglicht Ihnen das Speichern Ihrer Objektdaten in einer einzelnen Availability Zone in Amazon S3. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe .	4. April 2018
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 Benachrichtigung	Mit File Gateways können Sie nun eine Benachrichtigung erhalten, wenn ein Gateway die Aktualisierung	1. März 2018

Änderung	Beschreibung	Änderungsdatum
Änderungen zur Cache-Aktualisierung, Zahlung durch den Anforderer und vorgefertigte ACLs für Amazon S3-Buckets.	<p>des Caches für Ihren Amazon S3-Bucket abgeschlossen hat. Weitere Informationen finden Sie unter RefreshCache.html in der Storage Gateway-API-Referenz .</p> <p>Mithilfe von File Gateways kann nun der Anforderer oder Abrufende anstelle des Bucket-Eigentümers für den Zugriff zahlen.</p> <p>Mithilfe von File Gateways können Sie nun dem Eigentümer des S3-Buckets, der der NFS-Datei freigabe zugeordnet ist, die volle Kontrolle gewähren.</p> <p>Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.</p>	
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	<p>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.</p> <p>Mit File Gateways können Sie jetzt den MIME-Typ für hochgeladene Objekte basierend auf Dateierweiterungen bestimmen. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.</p>	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 Informationen finden Sie unter Testen Ihrer 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 Branchensstandard 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-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer 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 2 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 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
<p>Neue -Region</p> <p>Unterstützung für Stored Volumes mit bis zu 512 TiB Speicherkapazität</p> <p>Sonstige Gateway-Updates und -Verbesserungen in der lokalen Storage-Gateway-Konsole</p>	<p>Tape Gateway ist nun in der Region Asien-Pazifik (Seoul) verfügbar. Weitere Informationen finden Sie unter AWS Regionen.</p> <p>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.</p> <p>Die zulässige Gesamtgröße aller Bänder in einer virtuellen Bandbibliothek wurde auf 1 PiB erhöht. Weitere Informationen finden Sie unter AWS Storage Gateway -Kontingente.</p> <p>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.</p>	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 Inhaltsumstrukturierung	<p>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.</p> <p>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.</p>	20. Oktober 2015

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Cached Volumes mit bis zu 1 024 TiB Speicherkapazität	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 .	16. September 2015
Unterstützung für Netzwerkdapter des Typs VMXNET3 (10GbE) im Hypervisor VMware ESXi	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 .	
Leistungsverbesserungen	Die maximale Upload-Rate für Storage Gateway wurde auf 120 MB pro Sekunde erhöht, die maximale Download-Rate auf 20 MB pro Sekunde.	
Verschiedene Verbesserungen und Aktualisierungen in der lokalen Storage Gateway-Konsole	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 .	
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 Kennzeichen 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 archivieren. 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 .	
	<p>Diese Version umfasst die folgenden Verbesserungen und Aktualisierungen für Storage Gateway:</p> <ul style="list-style-type: none"> • 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 ListVolumelInitiators 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 Exec	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-Authentifizierung 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	<p>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.</p> <p>Diese Version umfasst die folgenden Verbesserungen und Aktualisierungen für Storage Gateway:</p> <ul style="list-style-type: none">• 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
<p>Kompatibilität mit weiterer Sicherungsssoftware und einem weiteren Medienwechsler</p>	<p>Tape-Gateway ist nun kompatibel mit der folgenden Sicherungssoftware:</p> <ul style="list-style-type: none"> • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 <p>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.</p> <p>Storage Gateway bietet nun einen zusätzlichen Medienwechsler, der mit der neuen Sicherungsssoftware kompatibel ist.</p> <p>Diese Version enthält verschiedene AWS Storage Gateway Verbesserungen und Updates.</p>	<p>3. November 2014</p>
<p>Region Europa (Frankfurt)</p>	<p>Storage Gateway ist jetzt in der Region Europa (Frankfurt) verfügbar. Weitere Informationen hierzu finden Sie unter AWS Regionen.</p>	<p>23. Oktober 2014</p>

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 Exec	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
<p>Unterstützung für Windows Server Failover Clustering</p> <p>Unterstützung für den VMware ESX-Initiator</p> <p>Unterstützung für die Durchführung von Konfigurationsaufgaben in der lokalen Storage Gateway-Konsole</p>	<ul style="list-style-type: none"> • 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. 	<p>31. Januar 2014</p>

Änderung	Beschreibung	Änderungsdatum
Unterstützung für virtuelle Bandbibliotheken und Einführung der API-Version 2013-06-30	<p>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:</p> <ul style="list-style-type: none">• 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	<p>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.</p>	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 Volume Gateway .	15. Januar 2013

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Cached Volumes und Einführung der API-Version 2012-06-30	<p>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.</p> <p>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.</p> <p>Weitere Informationen zu den beiden Storage Gateway-Lösungen finden Sie unter So funktioniert Volume Gateway (Architektur).</p> <p>Sie können auch eine Testkonfiguration einrichten. Anweisungen finden Sie unter Erstellen eines Tape Gateways.</p>	29. Oktober 2012

Änderung	Beschreibung	Änderungsdatum
API- und IAM-Unterstützung	<p>In dieser Version führt Storage Gateway API-Unterstützung sowie Unterstützung für AWS Identity and Access Management(IAM) ein.</p> <ul style="list-style-type: none">• 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 Volume Gateway-Appliance-Software

In diesen Versionshinweisen werden die neuen und aktualisierten Funktionen, Verbesserungen und Korrekturen beschrieben, die in jeder Version der 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 [DescribeGatewayInformation](#) API-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 , einschließlich der Änderung des standardmäßigen automatischen Wartungs- und Aktualisierungszeitplans für ein Gateway, finden Sie unter [verwalten Gateway-Updates mit der AWS Storage Gateway Console](#) verwalten.

Veröffentlichungsdatum	Version der Software	Versionshinweise
2024-04-10	2.8.1	<ul style="list-style-type: none">• Ein in 2.8.0 eingeführtes Problem mit der Speichernutzung wurde behoben

Veröffentlichungsdatum	Version der Software	Versionshinweise
		<ul style="list-style-type: none">• Sicherheitspatch-Updates• Verbesserter Software-Aktualisierungsprozess• Die fehlende NTP-Komponente (Network Time Protocol) für neue Gateways wurde behoben
2024-03-06	2.8.0	<ul style="list-style-type: none">• Betriebssystem-Updates für neue Gateways• Sicherheitspatch-Updates
2023-12-19	2.7.0	<ul style="list-style-type: none">• Betriebssystem-Updates für neue Gateways
2023-12-14	2,6.6	<ul style="list-style-type: none">• Wartungsversion