Benutzerhandbuch für Tape Gateway

AWS Storage Gateway

API-Version 2013-06-30

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Benutzerhandbuch für Tape Gateway

Copyright © 2025 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

Was ist Tape Gateway? ... 1
So funktioniert Tape Gateway ... 2
Tape Gateways ... 2
Erste Schritte mit AWS Storage Gateway ... 6
Melde dich an für AWS Storage Gateway ... 6
Erstellen Sie einen IAM-Benutzer mit Administratorrechten ... 7
Zugreifen AWS Storage Gateway ... 9
AWS-Regionen die Storage Gateway unterstützen ... 9
Anforderungen an die Einrichtung von Tape Gateway ... 11
Hardware- und Speicheranforderungen ... 11
Hardwareanforderungen für VMs ... 11
Anforderungen für EC2 Amazon-Instance-Typen ... 12
... 12
Speicheranforderungen ... 12
Netzwerk- und Firewall-Anforderungen ... 13
Port-Anforderungen ... 14
Netzwerk- und Firewall-Anforderungen für die Hardware-Appliance ... 27
Gewähren von Gateway-Zugriff über Firewalls und Router ... 30
Konfigurieren einer Sicherheitsgruppe ... 32
Unterstützte Hypervisoren und Host-Anforderungen ... 33
Unterstützte iSCSI-Initiatoren ... 34
Unterstützte Sicherungsanwendungen von Drittanbietern ... 35
Verwenden der Hardware-Appliance ... 37
Einrichten Ihrer Hardware-Appliance ... 38
Physische Installation Ihrer Hardware-Appliance ... 40
Zugreifen auf die Hardware-Appliance-Konsole ... 42
Netzwerkparameter der Hardware-Appliance konfigurieren ... 43
Aktivieren Ihrer Hardware-Appliance ... 45
Erstellen eines Gateways auf Ihrer Hardware-Appliance ... 46
Konfiguration einer Gateway-IP-Adresse auf der Hardware-Appliance ... 47
Gateway-Software von Ihrer Hardware-Appliance entfernen ... 50
Löschen Ihrer Hardware-Appliance ... 51
Erstellen Sie Ihr Gateway ... 53
Überblick – Gateway-Aktivierung ... 53

Einrichten eines Gateways ... 53
Verbinden mit AWS ... 54
Überprüfen und aktivieren ... 54
Überblick – Gateway-Konfiguration ... 54
Überblick – Speicherressourcen ... 54
Ein Tape Gateway erstellen und aktivieren ... 55
Einrichten eines Tape Gateways ... 55
Connect Ihr Tape Gateway mit AWS ... 56
Überprüfen von Einstellungen und Aktivieren Ihres Tape Gateways ... 58
Konfigurieren von Tape Gateway ... 58
Erstellen von Bändern ... 61
WORM-Bandschutz ... 62
Manuelles Erstellen von Bändern ... 62
Zulassen der automatischen Banderstellung ... 65
Erstellen von benutzerdefinierten Bandpools ... 68
Auswahl eines Typs ... 68
Bandaufbewahrungssperre ... 69
Erstellen eines benutzerdefinierten Bandpools ... 70
Verbinden von VTL-Geräten ... 71
Herstellen einer Verbindung mit einem Microsoft Windows-Client ... 71
Herstellen einer Verbindung mit einem Linux-Client ... 73
Testen Ihres Gateways ... 76
Arcserve Backup ... 77
Bacula Enterprise ... 81
Commvault ... 85
Dell EMC NetWorker ... 92
IBM Data Protect ... 96
OpenText Data Protector ... 100
Microsoft System Center DPM ... 108
NovaStor DataCenter/Netzwerk ... 113
NetVault Quest-Backup ... 119
Veeam Backup & Replication ... 123
Veritas Backup Exec ... 126
Veritas NetBackup ... 131
Wie geht es weiter? ... 138
Aktivieren eines Gateways in einer Virtual Private Cloud ... 139

Erstellen eines VPC-Endpunkts für Storage Gateway ... 140
Verwaltung Ihres Tape Gateways ... 142
Bearbeiten von Gateway-Informationen ... 143
Verwalten der automatischen Banderstellung ... 144
Archivieren von Bändern ... 147
Bänder nach S3 Glacier Deep Archive verschieben ... 147
Abrufen archivierter Bänder ... 148
Statistiken zur Bandnutzung anzeigen ... 150
Löschen von Bändern ... 151
Löschen von benutzerdefinierten Bandpools ... 152
Deaktivieren Ihres Tape Gateways ... 153
Grundlegendes zum Bandstatus ... 154
Grundlegendes zu Bandstatusinformationen in einer VTL ... 154
Bestimmen des Bandstatus in einem Archiv ... 156
Verschieben Ihrer Daten auf ein neues Gateway ... 156
Verschieben virtueller Bänder auf ein neues Tape Gateway ... 157
Überwachen von Storage Gateway ... 162
Grundlagen zu Gateway-Metriken ... 163
Dimensionen für Storage-Gateway-Metriken ... 167
Überwachen des Upload-Puffers ... 168
Überwachen des Cache-Speichers ... 170
CloudWatch Alarme verstehen ... 172
Empfohlene CloudWatch Alarme erstellen ... 174
Einen benutzerdefinierten CloudWatch Alarm erstellen ... 175
Überwachen von Tape Gateway ... 177
Abrufen von Zustandsprotokollen für Tape Gateway ... 178
Amazon CloudWatch Metrics verwenden ... 180
Metriken für virtuelle Bänder verstehen ... 181
Messung der Leistung zwischen Ihrem Tape Gateway und AWS ... 184
Warten eines Gateways ... 188
Verwalten von lokalen Festplatten ... 188
Bestimmen der Größe des lokalen Festplattenspeichers ... 189
Hinzufügen von Upload-Puffer oder Cache-Speicher ... 192
Verwalten der Bandbreite ... 193
Ändern der Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole ... 194
Planung der Bandbreitendrosselung ... 195

Unter Verwendung der AWS SDK für Java ... 197
Unter Verwendung der AWS SDK für .NET ... 199
Unter Verwendung der AWS Tools for Windows PowerShell ... 201
Verwaltung von Gateway-Updates ... 202
Aktualisierungshäufigkeit und erwartetes Verhalten ... 203
Wartungsupdates ein- oder ausschalten ... 204
Ändern Sie den Zeitplan für das Gateway-Wartungsfenster ... 204
Manuelles Anwenden eines Updates ... 206
Herunterfahren der Gateway-VM ... 207
Starten und Anhalten eines Tape Gateways ... 208
Löschen Sie Ihr Gateway und entfernen Sie Ressourcen ... 208
Löschen eines Gateways mithilfe der Storage-Gateway-Konsole ... 209
Entfernen von Ressourcen von einem lokal bereitgestellten Gateway ... 211
Ressourcen aus einem Gateway entfernen, das auf einer EC2 Amazon-Instance bereitgestellt wird ... 212
Durchführung von Wartungsaufgaben über die lokale Konsole ... 214
Zugreifen auf die lokale Konsole des Gateways ... 214
Zugreifen auf die lokale Konsole des Gateways mit Linux KVM ... 215
Zugreifen auf die lokale Gateway-Konsole mit VMware ESXi ... 216
Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V ... 217
Ausführen von Aufgaben in der lokalen VM-Konsole von ... 218
An der lokalen Konsole von Tape Gateway anmelden ... 218
Konfiguration eines SOCKS5 Proxys für Ihr lokales Gateway ... 220
Konfigurieren Ihres Gateway-Netzwerks ... 222
Testen Sie Ihre Gateway-Konnektivität zum Internet ... 228
Storage-Gateway-Befehle in der lokalen Konsole für ein lokales Gateway ausführen ... 229
Anzeigen des Gateway-Systemressourcen-Status ... 232
Aufgaben auf der EC2 lokalen Konsole ausführen ... 233
Melden Sie sich bei Ihrer lokalen EC2 Gateway-Konsole an ... 234
Konfigurieren eines HTTP-Proxys ... 235
Testen der Gateway-Netzwerkkonnektivität ... 236
Anzeigen des Gateway-Systemressourcen-Status ... 237
Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole ... 238
Leistung und Optimierung für Tape Gateway ... 241
Leistungsleitfaden für Tape Gateway ... 241
Optimierung der Gateway-Leistung ... 244

Empfohlene Konfiguration 244
Hinzufügen von Ressourcen zu Ihrem Gateway 245
Optimieren von iSCSI-Einstellungen 248
Verwenden Sie eine größere Blockgröße für Bandlaufwerke 248
Optimieren der Leistung von virtuellen Bandlaufwerken 249
Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung 249
Sicherheit 251
Datenschutz 252
Datenverschlüsselung 253
Identitäts- und Zugriffsverwaltung 255
Zielgruppe 255
Authentifizierung mit Identitäten 256
Verwalten des Zugriffs mit Richtlinien 260
So funktioniert AWS Storage Gateway mit IAM 263
Beispiele für identitätsbasierte Richtlinien 270
Fehlerbehebung 273
Compliance-Validierung 275
Ausfallsicherheit 276
Sicherheit der Infrastruktur 277
AWS Bewährte Methoden im Bereich Sicherheit 278
Protokollieren und Überwachen 278
Storage Gateway Gateway-Informationen in CloudTrail 279
Informationen zu Storage-Gateway-Protokolldateieinträgen 280
Fehlerbehebung bei Gateway-Problemen 283
Fehlerbehebung: Gateway-Offline-Probleme 283
Überprüfen Sie die zugehörige Firewall oder den zugehörigen Proxy 284
Suchen Sie nach einer laufenden SSL- oder Deep-Packet-Inspektion des Datenverkehrs Ihres Gateways 284
Suchen Sie nach einem Strom- oder Hardwarefehler auf dem Hypervisor-Host 284
Suchen Sie nach Problemen mit einer zugehörigen Cache-Festplatte 285
Fehlerbehebung: Probleme mit der Gateway-Aktivierung 285
Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt .. 286
Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen Amazon VPC-Endpunkt 289
Beheben Sie Fehler, wenn Sie Ihr Gateway über einen öffentlichen Endpunkt aktivieren und es in derselben VPC einen Storage Gateway Gateway-VPC-Endpunkt gibt 294

Fehlerbehebung bei lokalen Gateway-Problemen 294
Aktivierung Support zur Unterstützung bei der Fehlerbehebung Ihres Gateways 299
Fehlerbehebung bei Problemen mit der Einrichtung von Microsoft Hyper-V 301
Behebung von Problemen mit Amazon EC2 Gateway 305
Die Aktivierung des Gateways ist nach einigen Momenten nicht erfolgt. 306
Sie können die EC2 Gateway-Instanz nicht in der Instanzliste finden 306
Es kann kein Amazon EBS-Volume an die EC2 Gateway-Instance angehängt werden 307
Beim Hinzufügen von Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind 307
So entfernen Sie einen als Upload-Pufferspeicher zugewiesenen Datenträger, um die Größe des Upload-Pufferspeichers zu reduzieren 307
Der Durchsatz zum oder vom EC2 Gateway sinkt auf Null 307
Aktivierung Support zur Unterstützung der Fehlerbehebung am Gateway 308
Stellen Sie über die serielle Konsole eine Verbindung zu Ihrem EC2 Amazon-Gateway her 310
Fehlerbehebung bei Hardware-Appliance-Problemen 310
So ermitteln Sie die Service-IP-Adresse 310
So führen Sie eine Zurücksetzung auf die Werkseinstellungen durch 310
So führen Sie einen Remote-Neustart durch 310
So erhalten Sie Support für Dell iDRAC 311
So finden Sie die Seriennummer der Hardware-Appliance 311
So erhalten Sie Hardware-Appliance-Support 311
Beheben von Problemen mit virtuellen Bändern 312
Wiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway 312
Fehlerbehebung bei nicht wiederherstellbaren Bändern 316
High Availability-Zustandsbenachrichtigungen 318
Beheben von Problemen mit Hochverfügbarkeit 318
Zustandsbenachrichtigungen 318
Metriken 320
Bewährte Methoden 321
Bewährte Methoden: Wiederherstellung Ihrer Daten 321
Wiederherstellung nach dem unerwarteten Herunterfahren einer VM 322
Wiederherstellen von Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM 322
Wiederherstellung von Daten von einem nicht wiederherstellbaren Band 323
Wiederherstellen von Daten von einem fehlerhaften Cache-Datenträger 323

Wiederherstellen von Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann ... 324
Säuberung unnötiger Ressourcen ... 324
Weitere Ressourcen ... 326
Host-Setup ... 327
Stellen Sie einen EC2 Amazon-Standardhost für Tape Gateway bereit ... 328
Stellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit ... 330
Metadatenoptionen für EC2 Amazon-Instances ändern ... 335
Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Hostzeit ... 335
Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit ... 336
Konfigurieren Sie paravirtualisierte Festplattencontroller ... 338
Netzwerkadapter für Ihr Gateway konfigurieren ... 338
VMware Hochverfügbarkeit mit Storage Gateway verwenden ... 344
Arbeiten mit Tape Gateway-Speicherressourcen ... 350
Entfernen von Datenträgern aus dem Gateway ... 350
EBS-Volumes für Gateways EC2 ... 352
Arbeiten mit VTL-Geräten ... 353
Arbeiten mit Bändern ... 357
Den Aktivierungsschlüssel erhalten ... 359
Linux (curl) ... 360
Linux (bash/zsh) ... 361
Microsoft Windows PowerShell ... 362
Verwenden der lokalen Konsole ... 362
Verbinden von iSCSI-Initiatoren ... 363
VTL-Geräte mit einem Windows-Client verbinden ... 364
VTL-Geräte mit einem Linux-Client verbinden ... 367
Anpassen von iSCSI-Einstellungen ... 369
Konfigurieren der CHAP-Authentifizierung ... 374
Verwendung AWS Direct Connect mit Storage Gateway ... 380
Die Gateway-IP-Adresse abrufen ... 381
Eine IP-Adresse von einem EC2 Amazon-Host abrufen ... 382
Ressourcen und Ressourcen verstehen IDs ... 383
Mit Resource arbeiten IDs ... 384
Markieren Ihrer Ressourcen ... 385
Arbeiten mit Tags ... 385
Open-Source-Komponenten ... 387

Storage-Gateway-Kontingente 387
Kontingente für Bänder 388
Empfohlene Kapazität für die lokalen Datenträger des Gateways 388
API-Referenz 390
Erforderliche Abfrage-Header 390
Signieren von Anforderungen 393
Signatur-Berechnungsbeispiel 394
Fehlermeldungen 396
Ausnahmen 396
Operationsfehlercodes 399
Fehlermeldungen 418
Operationen 420
Dokumentverlauf 421
Frühere Aktualisierungen 441
Versionshinweise 461
..... cdlxviii

Was ist Tape Gateway?

AWS Storage Gateway verbindet eine lokale Software-Appliance mit cloudbasiertem Speicher, um eine nahtlose Integration von Datensicherheitsfunktionen zwischen Ihrer lokalen IT-Umgebung und der AWS Speicherinfrastruktur zu gewährleisten. 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.

Sie können Storage Gateway entweder lokal als VM-Appliance VMware ESXi, die auf einem KVM- oder Microsoft Hyper-V-Hypervisor läuft, als Hardware-Appliance oder als Amazon-Instance bereitstellen. AWS EC2 Sie können auf EC2 Instances gehostete Gateways für Disaster Recovery, Datenspiegelung und Bereitstellung von Speicher für auf Amazon gehostete Anwendungen verwenden. EC2

Eine Vielzahl von Anwendungsfällen, die dies AWS Storage Gateway ermöglicht, finden Sie unter. AWS Storage Gateway Aktuelle Informationen zu den Preisen finden Sie unter Preise auf der AWS Storage Gateway -Detailseite.

AWS Storage Gateway bietet dateibasierte (S3 File Gateway und FSx File Gateway), volumebasierte (Volume Gateway) und bandbasierte (Tape Gateway) Speicherlösungen an.

Dieses Benutzerhandbuch enthält Informationen zu Tape Gateway.

Tape Gateway bietet Cloud-gestützten virtuellen Bandspeicher. Mit Tape Gateway können Sie Backup-Daten kostengünstig und dauerhaft in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archivieren. Tape Gateway bietet eine virtuelle Bandinfrastruktur, die sich nahtlos an Ihre Geschäftsanforderungen anpassen lässt und den betrieblichen Aufwand für die Bereitstellung, Skalierung und Wartung einer physischen Bandinfrastruktur überflüssig macht.

Eine Übersicht über die Architektur finden Sie unter So funktioniert Tape Gateway.

In diesem Benutzerhandbuch finden Sie einen Abschnitt „Erste Schritte“, der Informationen zur Einrichtung enthält, die für alle Gateway-Typen gelten. Dort finden Sie auch die Setup-Anforderungen für Tape Gateway und Abschnitte, in denen beschrieben wird, wie Sie Ihr Tape Gateway bereitstellen, aktivieren, konfigurieren und verwalten.

Die Verfahren in diesem Benutzerhandbuch konzentrieren sich hauptsächlich auf die Durchführung von Gateway-Vorgängen mithilfe von AWS Management Console. Informationen zum

programmgesteuerten Ausführen dieser Operationen finden Sie in der AWS Storage Gateway -API-Referenz.

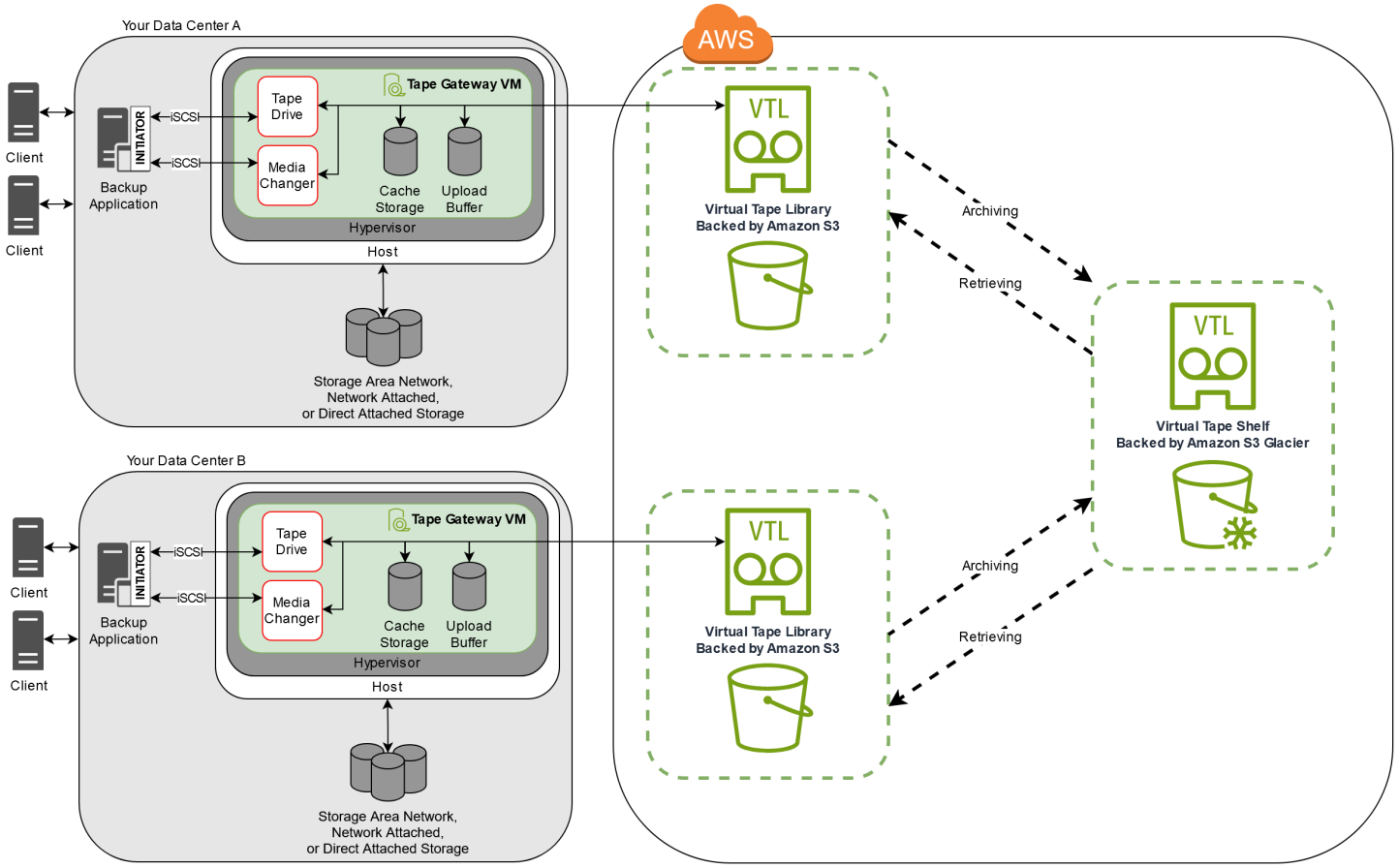
So funktioniert Tape Gateway

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

Tape Gateways

Tape Gateway bietet eine zuverlässige, kostengünstige Lösung zum Archivieren von Daten in der Amazon Web Services Cloud. Mit seiner Virtual Tape Library (VTL)-Schnittstelle können Sie mit der vorhandenen Infrastruktur für bandbasierte Sicherungsanwendungen Daten auf virtuellen Bandkassetten speichern, die Sie auf Ihrem Tape Gateway erstellen. Jedes Tape Gateway ist mit einem Medienwechsler und Bandlaufwerken vorkonfiguriert. Diese werden als iSCSI-Geräte für Ihre Client-Sicherungsanwendungen verfügbar gemacht. Bei Bedarf fügen Sie Bandkassetten zum Archivieren von Daten hinzu.

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



Das folgende Diagramm veranschaulicht die Komponenten von Tape Gateway:

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

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

  - Bandlaufwerk – Ein VTL-Bandlaufwerk entspricht einem physischen Bandlaufwerk, das E/A- und Suchoperationen auf einem Band ausführen kann. Jede VTL verfügt über eine Gruppe von 10 Bandlaufwerken, die für die Sicherungsanwendung als iSCSI-Geräte verfügbar sind.
  - Medienwechsler – Ein VTL-Medienwechsler entspricht einem Roboter, der Bänder in den Speicherslots einer physischen Bandbibliothek und auf Bandlaufwerken verschiebt. Jede VTL verfügt über einen Medienwechsler, der für die Sicherungsanwendung als iSCSI-Gerät verfügbar ist.
- Archivierung – Ein Archiv entspricht einem externen Aufbewahrungsort für Bänder. Sie können Bänder aus der zu archivierenden VTL des Gateways archivieren und bei Bedarf Bänder aus dem Archiv in die Gateway-VTL abrufen.
  - Archivierung von Bändern – Wenn Ihre Sicherungssoftware ein Band auswirft, verschiebt das Gateways dieses Band in das Archiv, wo es langfristig gespeichert wird. Das Archiv befindet sich in der AWS -Region, in der Sie das Gateway aktiviert haben. Bänder im Archiv werden im virtuellen Bandregal (Virtual Tape Shelf, VTS) gespeichert. Das VTS wird von S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive gesichert, einem kostengünstigen Speicherservice für die Datenarchivierung, Sicherung und langfristige Aufbewahrung von Daten.
  - Abrufen von Bändern – Archivierte Bänder können nicht direkt gelesen werden. Wenn Sie ein archiviertes Band lesen möchten, müssen Sie es zuerst von Ihrem Tape Gateway abrufen. Hierzu verwenden Sie die Storage-Gateway-Konsole oder die Storage Gateway API.

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

Nachdem Sie ein Tape Gateway bereitgestellt und aktiviert haben, mounten Sie die virtuellen Bandlaufwerke und den Medienwechsler als iSCSI-Geräte auf Ihren lokalen Anwendungsservern. Sie erstellen virtuelle Bänder nach Bedarf und verwenden dann die bestehende Sicherungssoftwareanwendung, um Daten auf die virtuellen Bänder zu schreiben. Der Medienwechsler lädt und entlädt die virtuellen Bänder für Lese- und Schreiboperationen in die virtuellen Bandlaufwerke.

Zuweisen von lokalen Datenträgern für die Gateway-VM

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

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

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

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

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

Erste Schritte mit AWS Storage Gateway

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

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

Topics

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

Melde dich an für AWS Storage Gateway

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

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

Um sich für eine anzumelden AWS-Konto

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

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

   Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontoserstellt. 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.

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

Erstellen Sie einen IAM-Benutzer mit Administratorrechten

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

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

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

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

Zugreifen AWS Storage Gateway

Sie können die AWS Storage Gateway Konsole verwenden, um verschiedene Gateway-Konfiguration und Wartungsaufgaben durchzuführen, darunter das Aktivieren oder Entfernen von Storage Gateway Gateway-Hardware-Appliances aus Ihrer Bereitstellung, das Erstellen, Verwalten und Löschen der verschiedenen Gateway-Typen, das Erstellen, Verwalten und Löschen von Bändern auf den Ihrer virtuellen Bandbibliothek sowie die Überwachung des Zustands und Status verschiedener Elemente des Storage Gateway Gateway-Dienstes. Aus Gründen der Einfachheit und Benutzerfreundlichkeit konzentriert sich dieses Handbuch auf die Ausführung von Aufgaben über die Weboberfläche der Storage Gateway Gateway-Konsole. Sie können über Ihren Webbrowser auf die Storage Gateway Gateway-Konsole zugreifen unter:https://console.aws.amazon.com/storagegateway/home/.

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

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

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

AWS-Regionen die Storage Gateway unterstützen

An AWS-Region ist ein physischer Standort auf der Welt, an dem es AWS mehrere Availability Zones gibt. Availability Zones bestehen aus einem oder mehreren diskreten AWS Rechenzentren, die

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

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

Voraussetzungen für die Einrichtung von Tape Gateway

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

Themen

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

Hardware- und Speicheranforderungen

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

Hardwareanforderungen für VMs

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

- 4 virtuelle Prozessoren für die VM
- Für ein Tape Gateway sollte Ihre Hardware die folgenden RAM-Mengen reservieren:
  - 16 GiB reservierter RAM für Gateways mit einer Cache-Größe von bis zu 16 TiB
  - 32 GiB reservierter RAM für Gateways mit einer Cache-Größe von 16 TiB bis 32 TiB
  - 48 GiB reservierter RAM für Gateways mit einer Cache-Größe von 32 TiB bis 64 TiB
- 80 GiB Festplattenspeicher zur Installation des VM-Abbilds sowie für die Systemdaten

Weitere Informationen finden Sie unter Optimierung 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 EC2 Amazon-Instance-Typen

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

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

Für Tape Gateway sollte Ihre EC2 Amazon-Instance je nach der Cachegröße, die Sie für Ihr Gateway verwenden möchten, 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

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

Für Tape Gateway Volumes empfohlen

- Allzweck-Instance-Familie: Instance-Typ m4, m5 oder m6.
- Für die Datenverarbeitung optimierte Instance-Familie — Instance-Typen c4, c5, c6 oder c7. Wählen Sie die Instance-Größe 2xlarge oder höher aus, um die erforderlichen RAM-Anforderungen zu erfüllen.
- Speicheroptimierte Instance-Familie — Instance-Typen r3, r5, r6 oder r7.
- Speicheroptimierte Instance-Familie — Instance-Typen i3, i4 oder i7.

Speicheranforderungen

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

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

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

> **Note**
>
> Sie können ein oder mehrere lokale Laufwerke für Ihren Cache und Upload-Puffer konfigurieren, bis die maximale Kapazität erreicht ist.
> Wenn Sie einem vorhandenen Gateway Cache oder Upload-Puffer hinzufügen, ist es wichtig, neue Festplatten in Ihrem Host (Hypervisor oder EC2 Amazon-Instance) zu erstellen. 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 bereitstellen EC2 oder andere Bereitstellungsarten (einschließlich lokal) mit Netzwerksicherheitsrichtlinien verwenden, die AWS IP-Adressbereiche einschränken. In diesen Fällen kann es bei Ihrem Gateway zu Problemen mit der Dienstkonnektivität kommen, wenn sich die AWS IP-Bereichswerte ändern. Die Werte für den AWS IP-Adressbereich, die Sie verwenden müssen, gehören zur Amazon-Servicesubmenge für die AWS Region, in der Sie Ihr Gateway aktivieren.

Informationen zu den aktuellen IP-Bereichswerten finden Sie unter AWS IP-Adressbereiche im Allgemeine AWS-Referenz.

> **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 bereitstellen EC2 oder andere Bereitstellungstypen verwenden

Themen

- Port-Anforderungen
- Netzwerk- und Firewall-Anforderungen für das Storage-Gateway-Hardwaregerät
- Ermöglicht AWS Storage Gateway den Zugriff über Firewalls und Router
- Konfiguration von Sicherheitsgruppen für Ihre Amazon EC2 Gateway-Instance

Port-Anforderungen

Tape Gateway setzt voraus, dass für eine erfolgreiche Implementierung und einen erfolgreichen Betrieb bestimmte Ports durch Ihre Netzwerksicherheit zugelassen werden. Einige Ports sind für alle Gateways erforderlich, während andere nur für bestimmte Konfigurationen erforderlich sind, z. B. beim Herstellen einer Verbindung zu VPC-Endpunkten.

Netzwerkelement	Aus	Bis	Protokoll	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
Webbrowser	Ihr Webbrowser	Storage-Gateway-VM	TCP HTTP	80	✓	✓	✓	Wird von lokalen Systemen verwendet

Netzwerkelement	Aus	Bis	Protokoll	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								, um den Storage Gateway Gateway-Aktivierungsschlüssel zu erhalten. Port 80 wird nur während der Aktivierung einer Storage-Gateway-Appliance verwendet. Für eine Storage-Gateway-VM ist es nicht erforderlich, dass Port 80 öffentlic

Netzwerkelement	Aus	Bis	Protokoll	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								h zugänglich ist. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie Ihr Gateway von der Storage Gateway Management Console aus aktivieren, muss der Host, von dem aus Sie eine

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

Netzwerkelement	Aus	Bis	Protokoll	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
DNS	Storage-Gateway-VM	Domain Name Service (DNS)-Server	TCP- und UDP-DNS	53	✓	✓	✓	Wird für die Kommunikation zwischen einer Storage Gateway Gateway-VM und dem DNS-Server für die IP-Namensauflösung verwendet.

Netzwerkelement	Aus	Bis	Protokoll	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
NTP	Storage-Gateway-VM	Network Time Protocol (NTP)-Server	TCP & UDP NTP	123	✓	✓	✓	Wird von lokalen Systemen verwendet, um die VM-Zeit mit der Host-Zeit zu synchronisieren. Eine Storage-Gateway-VM ist so konfiguriert, dass die folgenden NTP-Server verwendet werden: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org

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

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

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

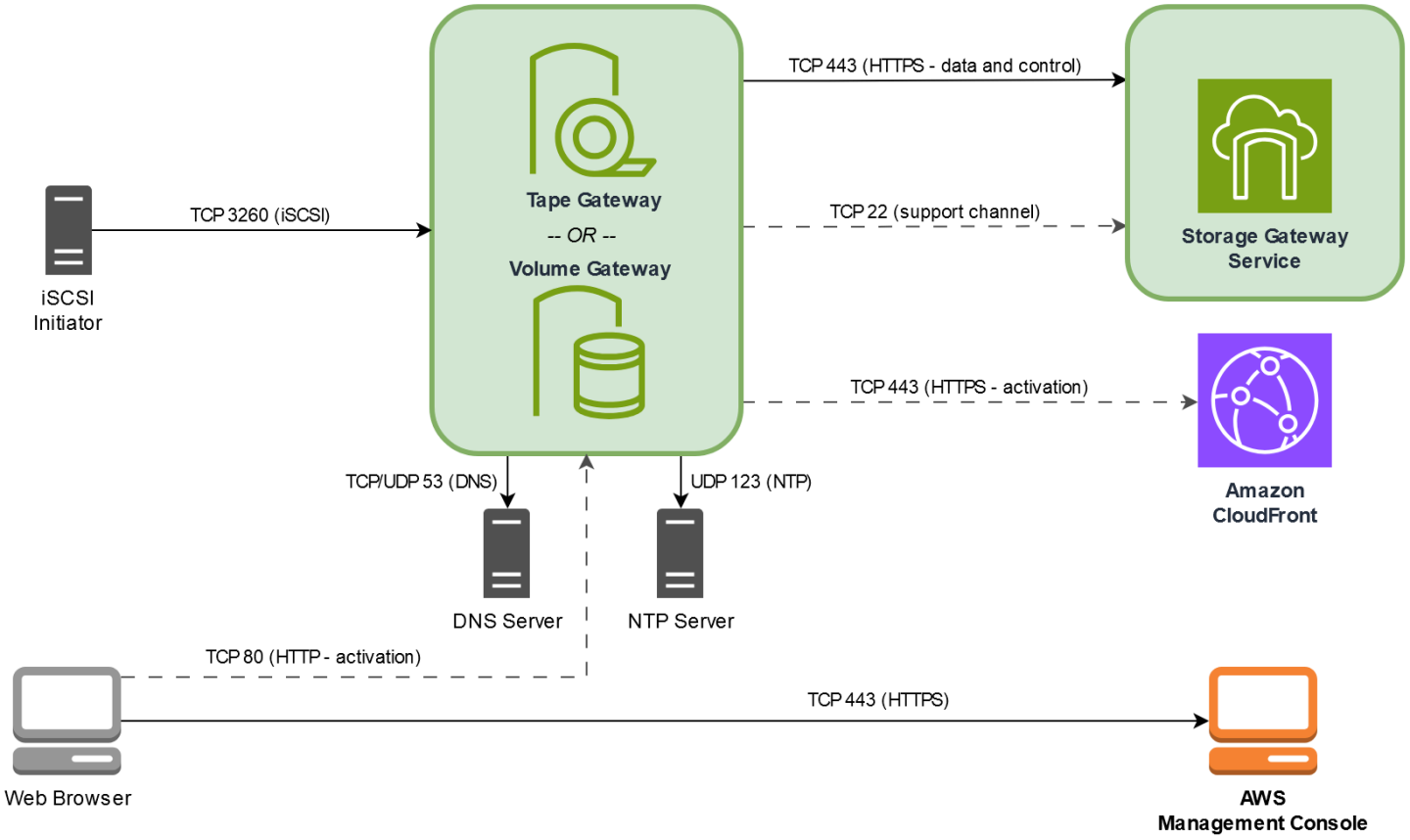
Netzwerkelement	Aus	Bis	Protokoll	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓*	Managementkontrolle *Nur erforderlich, wenn VPC-Endpoints verwendet werden
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	1026		✓	✓*	Endpunkt der Kontrollebene *Nur erforderlich, wenn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

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

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

Netzwerkelement	Aus	Bis	Protokoll	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓*	Managementkontrolle *Nur erforderlich, wenn VPC-Endpoints verwendet werden
iSCSI-Client	iSCSI-Client	Storage-Gateway-VM	TCP	3260	✓	✓	✓	Damit lokale Systeme eine Verbindung zu iSCSI-Zielen herstellen können, die vom Gateway verfügbar gemacht werden.

Die folgende Abbildung zeigt den Netzwerkdatenverkehr für eine grundlegende .



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

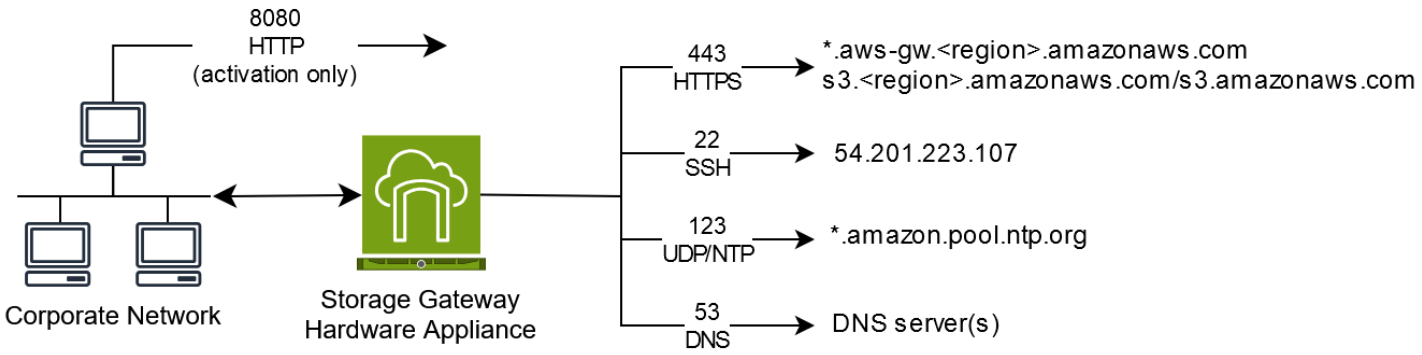
Jedes Storage-Gateway-Hardwaregerät benötigt die folgenden Netzwerkdienste:

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

Auf der Rückseite des Dell PowerEdge R640-Servers befinden sich fünf physische Netzwerkanschlüsse. Bei diesen Ports handelt es sich von links nach rechts (zur Rückseite des Servers hin) um:

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

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



Eine Hardware-Appliance benötigt die folgenden Ports.

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

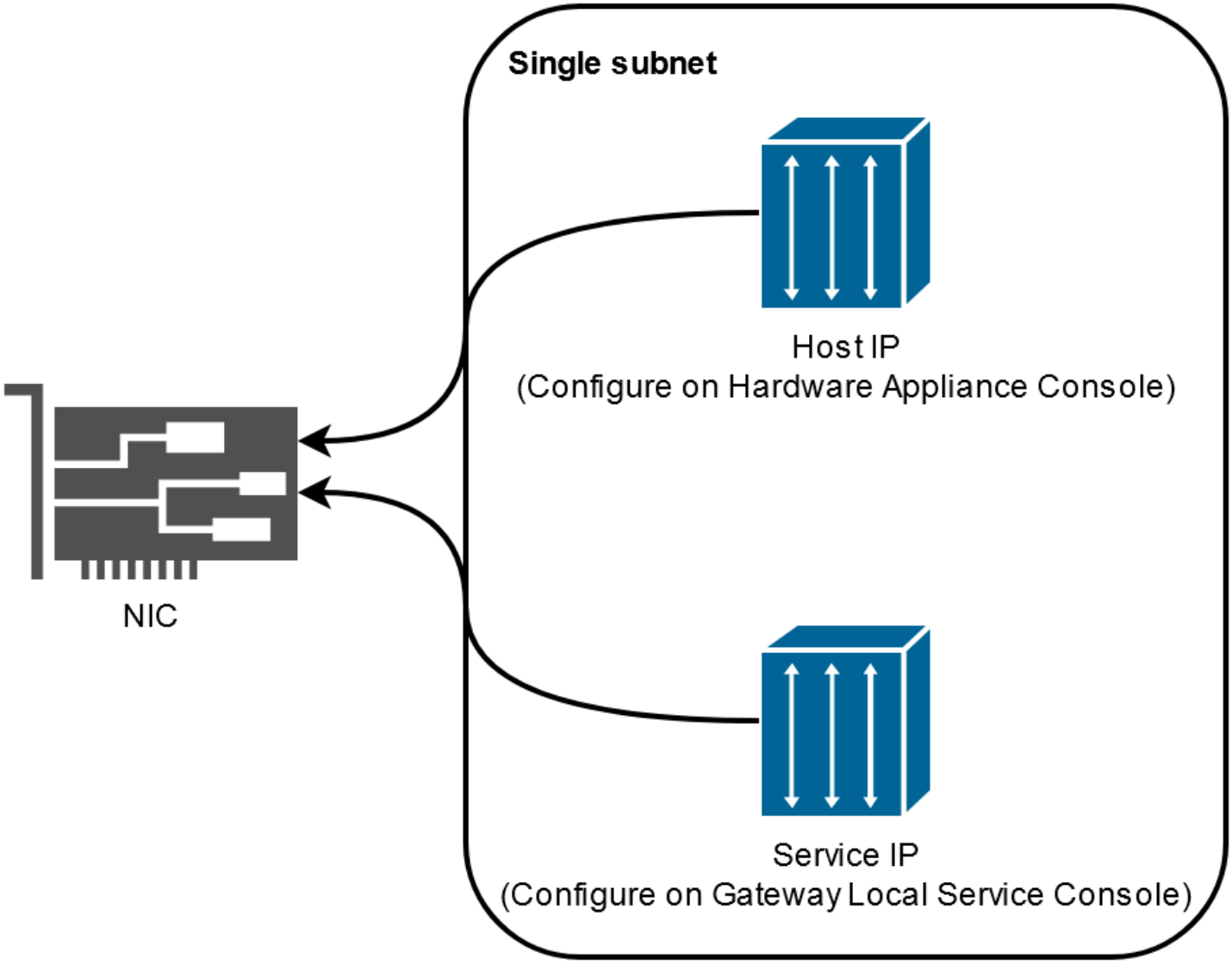
Protokoll	Port	Richtung	Quelle	Ziel	Verwendung
HTTP	8080	Eingehend	AWS	Hardware-Appliance	Aktivierung (nur kurz)

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

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

> **Note**
>
> Eine Abbildung der Rückseite des Servers mit seinen Ports finden Sie unter Physische Installation Ihrer Hardware-Appliance

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



Weitere Informationen zur Aktivierung und Konfiguration einer Hardware-Appliance finden Sie unter Verwenden der Storage-Gateway-Hardware-Appliance.

Ermöglicht AWS Storage Gateway den Zugriff über Firewalls und Router

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

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

> **Important**
>
> Ersetzen *region* Sie je nach AWS Region Ihres Gateways den Service-Endpunkt durch die richtige Regionszeichenfolge.

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

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

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

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

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

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

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 in der. Allgemeine AWS-Referenz
- Storage Gateway Hardware Appliance — Informationen zu unterstützten AWS Regionen, die Sie mit der Hardware-Appliance verwenden können, finden Sie unter Regionen der Storage Gateway Gateway-Hardware-Appliance in der. Allgemeine AWS-Referenz

Konfiguration von Sicherheitsgruppen für Ihre Amazon EC2 Gateway-Instance

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

- Die Sicherheitsgruppe sollte keine eingehenden Verbindungen aus dem externen Internet zulassen. Sie sollte festlegen, dass ausschließlich Instances innerhalb der Gateway-Sicherheitsgruppe mit dem Gateway kommunizieren dürfen. Müssen Instances von außerhalb der Gateway-Sicherheitsgruppe eine Verbindung mit dem Gateway herstellen, empfehlen wir, solche Verbindungen ausschließlich auf Port 3260 (iSCSI-Verbindungen) und Port 80 (Aktivierung) zuzulassen.
- Wenn Sie Ihr Gateway von einem EC2 Amazon-Host außerhalb der Gateway-Sicherheitsgruppe aus aktivieren möchten, lassen Sie eingehende Verbindungen auf Port 80 von der IP-Adresse dieses Hosts aus zu. Falls Sie die IP-Adresse des zur Aktivierung verwendeten Hosts nicht kennen, können Sie Port 80 öffnen, Ihr Gateway aktivieren und Port 80 nach der Aktivierung wieder für Zugriffe schließen.
- Erlauben Sie den Zugriff auf Port 22 nur, wenn Sie Support ihn zur Fehlerbehebung verwenden. Weitere Informationen finden Sie unter Sie Support möchten bei der Fehlerbehebung Ihres EC2 Gateways helfen.

In einigen Fällen können Sie eine EC2 Amazon-Instance als Initiator verwenden (d. h. um eine Verbindung zu iSCSI-Zielen auf einem Gateway herzustellen, das Sie auf Amazon bereitgestellt haben). EC2 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 lokal entweder als virtuelle Maschine (VM) -Appliance oder als physische Hardware-Appliance oder AWS als EC2 Amazon-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) — Für dieses Setup benötigen Sie auch einen VMware vSphere-Client, um eine Verbindung zum Host herzustellen.
- 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 kernelbasierte virtuelle Maschine (KVM): Eine kostenlose Open-Source-Virtualisierungstechnologie. KVM ist in allen Versionen von Linux Version 2.6.20 und neuer enthalten. Storage Gateway wurde für die Distributionen CentOS/RHEL 7.7, 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.
- EC2 Amazon-Instance — Storage Gateway stellt ein Amazon Machine Image (AMI) bereit, das das Gateway-VM-Image enthält. Bei Amazon EC2 können nur die Typen Datei, zwischengespeichertes Volume und Tape Gateway bereitgestellt werden. Informationen zur Bereitstellung eines Gateways bei Amazon EC2 finden Sie unterStellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit.

- Storage-Gateway-Hardware-Appliance: Storage Gateway bietet eine physische Hardware-Appliance als On-Premises-Bereitstellungsoption für Standorte mit eingeschränkter Infrastruktur für virtuelle Maschinen.

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

Unterstützte iSCSI-Initiatoren

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

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

- Microsoft Windows Server 2022
- RedHat Enterprise Linux 8
- RedHat Enterprise Linux 9
- VMware ESX Initiator, der eine Alternative zur Verwendung von Initiatoren in den Gastbetriebssystemen Ihres VMs

> **Important**
>
> Storage Gateway bietet keine Unterstützung für Microsoft Multipfad-E/A (MPIO) über Windows-Clients.
> Storage Gateway unterstützt jetzt Verbindungen zwischen mehreren Hosts und ein und demselben Volume, wenn die Hosts den Zugriff über Windows Server Failover Clustering

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

Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway

Sie verwenden eine Sicherungsanwendung, um Bänder mit einem Tape Gateway zu lesen, auf die Bänder zu schreiben und sie zu verwalten. Welchen Medienwechslertyp Sie wählen, hängt von der Sicherungsanwendung ab, die Sie verwenden möchten.

AWS hat die Backup-Anwendungen von Drittanbietern in der folgenden Tabelle getestet, um die Kompatibilität mit diesen Tape Gateway-Features und -Funktionen sicherzustellen:

- Erkennungsfunktionen, einschließlich iSCSI-Initiatorkonnektivität, Medienwechsler, Rescan, automatische und manuelle Gerätezuweisung.
- Bandfunktionen wie Erstellen, Löschen, Importieren, Exportieren, Inventarisieren und Barcode-Sichtbarkeit.
- Löschung des Bandinhalts und Überprüfung, dass nachfolgende Wiederherstellungen keine Daten enthalten.
- Datensicherung auf einzelne oder mehrere Bänder, Überprüfung, ob Backup-Aufträge, die die Bandkapazität überschreiten, angehalten werden, um auf weitere Bänder zu warten.
- Wiederherstellung vollständiger und teilweiser Daten von Bändern und Überprüfung der Datenintegrität.
- Überprüfung der Funktionalität und Datenintegrität nach dem Herunterfahren und Neustarten des Gateways bei Backup-Vorgängen.

Sicherungsanwendung	Version	Medienwechslertyp	Gateway-Version getestet
Arcserve Backup	19	AWS-Gateway-VTL	2.12.3
Bacula Enterprise	15.0.2	AWS-Gateway-VTL oder STK-L700	2.12.3

Sicherungsanwendung	Version	Medienwechslertyp	Gateway-Version getestet
Commvault	2024E/11,36,35	STK-L 700	2.12.3
Dell EMC NetWorker	19,10	AWS-Gateway-VTL	2.12.3
IBM Storage Protect	8.1.10	IBM-03584L32-0402	Alle
Micro Focus Datenschützer	24.4	AWS-Gateway-VTL	2.12.3
Microsoft System Center Manager	2025	STK-L 700	2.12.3
NovaStor DataCenter	9.5.3	STK-L 700	2.12.3
NetVault Quest-Backup	13.3	STK-L 700	2.12.3
Veeam Backup & Replicon	12	AWS-Gateway-VTL	Alle
Veritas Backup Exec	24	AWS-Gateway-VTL	Alle
Veritas NetBackup	10.5	AWS-Gateway-VTL	2.12.3

Important

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

Verwenden der Storage-Gateway-Hardware-Appliance

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

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

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

Eine Liste der unterstützten Regionen, AWS-Regionen in denen die 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.

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

Themen

- Einrichtung Ihrer Storage Gateway Gateway-Hardware-Appliance
- Physische Installation Ihrer Hardware-Appliance

- Zugreifen auf die Hardware-Appliance-Konsole
- Netzwerkparameter der Hardware-Appliance konfigurieren
- Aktivierung Ihrer Storage Gateway Gateway-Hardware-Appliance
- Erstellen eines Gateways auf Ihrer Hardware-Appliance
- Konfiguration einer Gateway-IP-Adresse auf der Hardware-Appliance
- Gateway-Software von Ihrer Hardware-Appliance entfernen
- Löschen Ihrer Storage Gateway Gateway-Hardware-Appliance

Einrichtung Ihrer Storage Gateway Gateway-Hardware-Appliance

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

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

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

1. Mounten Sie die Appliance in einem Rack und schließen Sie Strom- und Netzwerkkabel an. Weitere Informationen finden Sie unter Physische Installation Ihrer Hardware-Appliance.
2. Stellen Sie die Internetprotokolladressen der Version 4 (IPv4) für die Hardware-Appliance (den Host) ein. Weitere Informationen finden Sie unter Netzwerkparameter der Hardware-Appliance konfigurieren.

3. Aktivieren Sie die Hardware-Appliance auf der Konsolen-Übersichtsseite der Hardware-Appliance in der AWS Region Ihrer Wahl. Weitere Informationen finden Sie unter Aktivierung Ihrer Storage Gateway Gateway-Hardware-Appliance.
4. Erstellen Sie ein Gateway auf Ihrer Hardware-Appliance. Weitere Informationen finden Sie unter Ein Tape Gateway erstellen und aktivieren.

   Sie richten Gateways auf Ihrer Hardware-Appliance genauso ein wie Gateways auf Microsoft Hyper-V VMware ESXi, Linux Kernel-based Virtual Machine (KVM) oder Amazon. EC2

Erweiterung des nutzbaren Cache-Speichers

Sie können den nutzbaren Speicher auf der Hardware-Appliance von 5 TB auf 12 TB erhöhen. Dadurch wird ein größerer Cache für den Zugriff auf eingehende Daten mit geringer Latenz bereitgestellt. AWS Wenn Sie das 5-TB-Modell bestellt haben, können Sie den nutzbaren Speicher auf 12 TB erhöhen, indem Sie fünf 1,92-TB-Laufwerke SSDs (Solid-State-Laufwerke) kaufen.

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

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

Optionen für Netzwerkschnittstellenkarte

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

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

Physische Installation Ihrer Hardware-Appliance

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

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

Voraussetzungen

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

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

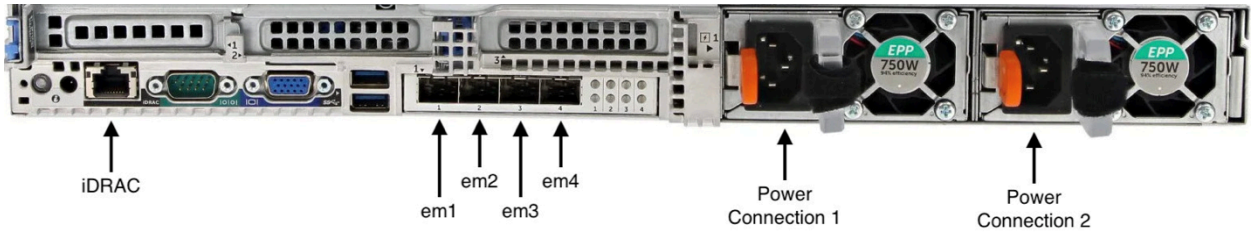
> **Note**
>
> Stellen Sie vor Ausführung der folgenden Schritte sicher, dass Sie alle Anforderungen für die Storage-Gateway-Hardware-Appliance erfüllen wie in Netzwerk- und Firewall-Anforderungen für das Storage-Gateway-Hardwaregerät beschrieben.

Um Ihre Hardware-Appliance physisch zu installieren

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

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

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



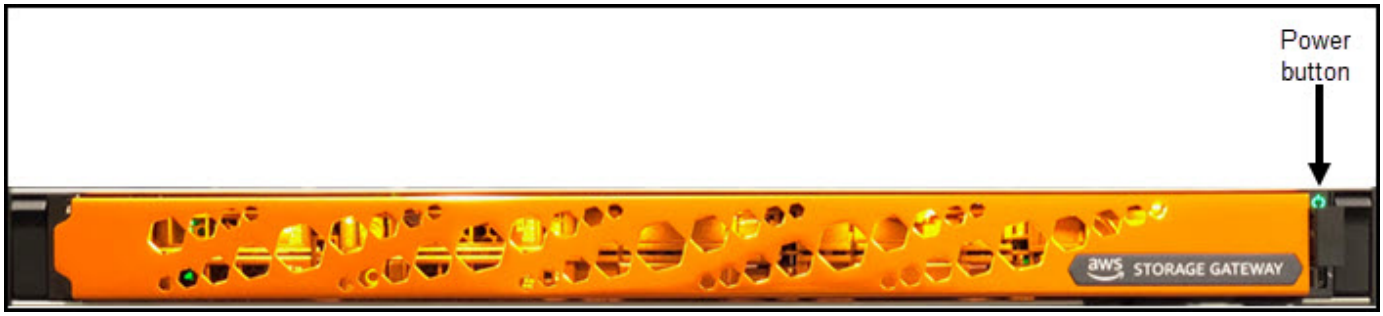
Hardware-Gerät auf einer Rückseite mit Netzwerk- und Stromanschlussetiketten.

2. Schließen Sie an beide Netzteile ein Stromkabel an. Es ist möglich, nur einen Stromanschluss anzuschließen, aus Redundanzgründen empfehlen wir jedoch, beide Netzteile mit Strom zu verbinden.
3. Schließen Sie ein Ethernet-Kabel an den `em1`-Port an, um eine stets verfügbare Internetverbindung bereitzustellen. Der `em1`-Port ist der erste der vier physischen Netzwerkports an der Rückseite, von links nach rechts betrachtet.

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

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

Vorderseite der Hardware-Appliance mit Netzschalter-Etikett.



Vorderseite der Hardware-Appliance mit Netzschalter-Etikett.

Nächster Schritt

Zugreifen auf die Hardware-Appliance-Konsole

Zugreifen auf die Hardware-Appliance-Konsole

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

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

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

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

Um ein Admin-Passwort festzulegen

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

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

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

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

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

Nächster Schritt

Netzwerkparameter der Hardware-Appliance konfigurieren

Netzwerkparameter der Hardware-Appliance konfigurieren

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

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

So richten Sie eine Netzwerkadresse ein

1. Wählen Sie auf der Startseite die Option Netzwerk konfigurieren aus und drücken Sie dann auf`Enter`. Die Seite „Netzwerk konfigurieren“ wird angezeigt. Auf der Seite „Netzwerk konfigurieren“ werden IP- und DNS-Informationen für jede der vier Netzwerkschnittstellen auf der

Hardware-Appliance angezeigt. Sie enthält auch Menüoptionen zur Konfiguration von DHCP - oder statischen Adressen für jede dieser Schnittstellen.

2. Führen Sie für die em1-Schnittstelle einen der folgenden Schritte aus:

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

     Notieren Sie sich diese Adresse für die spätere Verwendung im Aktivierungsschritt.

   - Wählen Sie Statisch und drücken Sie`Enter`, um eine statische IPv4 Adresse zu konfigurieren.

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

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

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

So melden Sie sich von der Hardwarekonsole ab

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

Nächster Schritt

[Aktivierung Ihrer Storage Gateway Gateway-Hardware-Appliance]

Aktivierung Ihrer Storage Gateway Gateway-Hardware-Appliance

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

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

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

So aktivieren Sie Ihre 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 auf Ihrer Hardware-Appliance

Erstellen eines Gateways auf Ihrer Hardware-Appliance

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

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

So erstellen Sie einen Gateway auf Ihrer Hardware-Appliance

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

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

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

Nächster Schritt

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

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

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

Bevor Sie Ihre Hardware-Appliance aktiviert haben, haben Sie ihrer physischen Netzwerkschnittstelle eine IP-Adresse zugewiesen. Nachdem Sie die Appliance aktiviert und Ihr Storage Gateway darauf gestartet haben, müssen Sie der virtuellen Storage-Gateway-Maschine, die auf der Hardware-Appliance ausgeführt wird, eine weitere IP-Adresse zuweisen. Um einem auf Ihrer Hardware-Appliance installierten Gateway eine statische IP-Adresse zuzuweisen, konfigurieren Sie die IP-Adresse über die lokale Gateway-Konsole für dieses Gateway. Ihre Anwendungen (wie Ihr NFS- oder SMB-Client) stellen eine Verbindung zu dieser IP-Adresse her. Mit der Option Open Service Console können Sie von der Hardware-Appliance-Konsole aus auf die lokale Gateway-Konsole zugreifen.

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

1. Wählen Sie auf der Hardwarekonsole Open Service Console aus und drücken Sie dann`Enter`, um die Anmeldeseite für die lokale Gateway-Konsole zu öffnen.
2. Auf der Anmeldeseite der AWS Storage Gateway lokalen Konsole werden Sie aufgefordert, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

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

   > **Note**
   >
   > Wir empfehlen, das Standardpasswort zu ändern, indem Sie im Hauptmenü AWS Geräteaktivierung – Konfiguration die entsprechende Zahl für die Gateway-Konsole eingeben und dann den Befehl `passwd` ausführen. Weitere Informationen zum Ausführen des Befehls finden Sie unter Storage-Gateway-Befehle in der lokalen Konsole für ein lokales Gateway ausführen. Sie können das Passwort auch von der Storage Gateway Gateway-Konsole aus festlegen. Weitere Informationen finden Sie unter Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole.

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

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

- Eingabeaufforderung

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

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

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

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

   > **Note**
   >
   > Die IP-Adresse, die Sie hier angeben, muss sich im selben Subnetz befinden wie die IP-Adresse, die bei der Aktivierung der Hardware-Appliance verwendet wurde.

So verlassen Sie die lokale Konsole des Gateways

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

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

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

Gateway-Software von Ihrer Hardware-Appliance entfernen

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

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

So entfernen Sie einen Gateway von einer Hardware-Appliance

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

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

> **Note**
>
> Nachdem Sie die Gateway-Software entfernt haben, können Sie die Aktion nicht rückgängig machen. Bei bestimmten Gateway-Typen können Daten beim Löschen verlorengehen, insbesondere zwischengespeicherte Daten. Weitere Informationen zum Löschen eines Gateways finden Sie unter Löschen Ihres Gateways und Entfernen der zugehörigen Ressourcen.

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

Löschen Ihrer Storage Gateway Gateway-Hardware-Appliance

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

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

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

So löschen Sie Ihre Hardware-Appliance

1. Wenn Sie ein Gateway auf der Hardware-Appliance installiert haben, müssen Sie zunächst das Gateway entfernen, bevor Sie die Appliance löschen können. Anweisungen zum Entfernen eines Gateways von der Hardware-Appliance finden Sie unter Gateway-Software von Ihrer Hardware-Appliance entfernen.
2. Wählen Sie auf der Hardware-Seite der Storage-Gateway-Konsole die Hardware-Appliance, die Sie löschen möchten.
3. Wählen Sie unter Aktionen die Option Appliance löschen aus. Das Bestätigungsdialogfeld wird angezeigt.
4. Vergewissern Sie sich, dass Sie die angegebene Hardware-Appliance löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen.

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

Erstellen Sie Ihr Gateway

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

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

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

Überblick – Gateway-Aktivierung

Bei der Gateway-Aktivierung müssen Sie Ihr Gateway einrichten, eine Verbindung herstellen AWS, anschließend Ihre Einstellungen überprüfen und es 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 einsetzen, die Sie bei Ihrem bevorzugten Händler bestellen, oder als EC2 Amazon-Instanz in Ihrer AWS Cloud-Umgebung. Wenn Sie die Gateway-Appliance bereitstellen, weisen Sie lokalen physischen Festplattenspeicher auf dem Virtualisierungshost zu.

Verbinden mit AWS

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

Überprüfen und aktivieren

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

Überblick – Gateway-Konfiguration

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

Überblick – Speicherressourcen

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

Ein Tape Gateway erstellen und aktivieren

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

Themen

- Einrichten eines Tape Gateways
- Connect Ihr Tape Gateway mit AWS
- Überprüfen von Einstellungen und Aktivieren Ihres Tape Gateways
- Konfigurieren von Tape Gateway

Einrichten eines Tape Gateways

So richten Sie ein neues Tape Gateway ein

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

    a. Geben Sie in Gateway-Name einen Namen für Ihren Gateway ein. Sie können nach diesem Namen suchen, um Ihr Gateway auf Listenseiten in der Storage-Gateway-Konsole zu finden.

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

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

        - VMware ESXi- Laden Sie die virtuelle Gateway-Maschine herunter, stellen Sie sie bereit und konfigurieren Sie sie mithilfe von VMware ESXi.
        - Microsoft Hyper-V – Laden Sie die virtuelle Gateway-Maschine mit Microsoft Hyper-V herunter, stellen Sie sie bereit und konfigurieren Sie sie.

- Linux KVM – Laden Sie die virtuelle Gateway-Maschine mit Linux KVM herunter, stellen Sie sie bereit und konfigurieren Sie sie.
- Amazon EC2 — Konfigurieren und starten Sie eine EC2 Amazon-Instance zum Hosten Ihres Gateways. Diese Option ist für Gateways für gespeicherte Volumes nicht verfügbar.
- Hardware-Appliance — Bestellen Sie eine dedizierte physische Hardware-Appliance AWS , um Ihr Gateway zu hosten.

b. Aktivieren Sie für Einrichten des Gateways bestätigen das entsprechende Kontrollkästchen, um zu bestätigen, dass Sie die Bereitstellungsschritte für die von Ihnen gewählte Host-Plattform ausgeführt haben. Dieser Schritt gilt nicht für die Hostplattform der Hardware-Appliance.

6. Wählen Sie im Abschnitt Sicherungsanwendungseinstellungen für Backup-Anwendung die Anwendung aus, mit der Sie Ihre Banddaten auf den virtuellen Bändern sichern möchten, die Ihrem Tape Gateway zugeordnet sind.
7. Wählen Sie Weiter aus, um fortzufahren.

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

Connect Ihr Tape Gateway mit AWS

Um ein neues Tape Gateway zu verbinden AWS

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

   - Öffentlich zugänglich — Ihr Gateway kommuniziert mit ihm 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 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. Weitere Informationen finden Sie unter Aktivierung Ihres Gateways in einer virtuellen privaten Cloud.

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 EC2 Amazon-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, mit welcher Verbindung Ihr Gateway verbunden werden soll AWS, müssen Sie das Gateway aktivieren. Anweisungen finden Sie unter Überprüfen von Einstellungen und Aktivieren Ihres Tape Gateways.

Überprüfen von Einstellungen und Aktivieren Ihres Tape Gateways

So aktivieren Sie ein neues Tape Gateway

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

   - Einrichten eines Tape Gateways
   - Connect Ihr Tape Gateway mit AWS

   Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Überprüfen und Aktivieren in der Storage-Gateway-Konsole zu öffnen.
2. Überprüfen Sie die anfänglichen Gateway-Details für jeden Abschnitt auf der Seite.
3. Wenn ein Abschnitt Fehler enthält, wählen Sie Bearbeiten, um zur entsprechenden Einstellungsseite zurückzukehren und Änderungen vorzunehmen.

   > **Note**
   >
   > Sie können die Gateway-Optionen oder Verbindungseinstellungen nicht ändern, nachdem Ihr Gateway aktiviert wurde.

4. Wählen Sie Gateway aktivieren, um fortzufahren.

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

Konfigurieren von Tape Gateway

So führen Sie die Erstkonfiguration auf einem neuen Tape Gateway durch

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

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

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

2. Verwenden Sie im Abschnitt Speicher konfigurieren die Dropdownmenüs, um mindestens eine Festplatte mit mindestens 165 GiB Kapazität für CACHE STORAGE und mindestens eine Festplatte mit mindestens 150 GiB Kapazität für UPLOAD BUFFER zuzuweisen. Die in diesem Abschnitt aufgeführten lokalen Festplatten entsprechen dem physischen Speicher, den Sie auf Ihrer Hostplattform bereitgestellt haben.
3. Wählen Sie im Abschnitt CloudWatch Protokollgruppe aus, wie Amazon CloudWatch Logs eingerichtet werden soll, 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 zur Überwachung Ihres Gateways.

> **Note**
>
> Um Storage Gateway Gateway-Integritätsprotokolle zu erhalten, müssen die folgenden Berechtigungen in Ihrer Protokollgruppen-Ressourcenrichtlinie vorhanden sein. Ersetzen Sie die *highlighted section* ResourceArn-Informationen für Ihre Bereitstellung durch die spezifische Protokollgruppe.

```
"Sid": "AWSLogDeliveryWrite20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "delivery.logs.amazonaws.com"
        ]
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
```

```
        "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

Das Element „Resource“ ist nur erforderlich, wenn Sie möchten, dass die Berechtigungen explizit für eine einzelne Protokollgruppe gelten.

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

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

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

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

5. (Optional) Wählen Sie im Abschnitt Tags die Option Neues Tag hinzufügen und geben Sie dann ein Schlüssel-Wert-Paar ein, bei dem Groß- und Kleinschreibung beachtet wird, damit Sie auf

Listenseiten in der Storage-Gateway-Konsole nach Ihrem Gateway suchen und filtern können. Wiederholen Sie diesen Schritt, um bei Bedarf weitere Tags hinzuzufügen.

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

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

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

Neue virtuelle Bänder für Tape Gateway erstellen

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

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

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

> **Note**
>
> Sie zahlen nur für die Datenmenge, die Sie auf das Band schreiben, nicht für die Bandkapazität.
> Sie können AWS Key Management Service (AWS KMS) verwenden, um Daten zu verschlüsseln, die auf ein virtuelles Band geschrieben wurden und in Amazon Simple Storage

Service (Amazon S3) gespeichert sind. Derzeit können Sie dies mithilfe der AWS Storage Gateway API oder AWS Command Line Interface (AWS CLI) tun. Weitere Informationen finden Sie unter CreateTapesoder erstellen von Bändern.

WORM-Bandschutz (Write Once, Read Many)

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

Daten, die auf virtuelle WORM-Bänder geschrieben wurden, können nicht überschrieben werden. Es können nur neue Daten an virtuelle WORM-Bänder angehängt werden, doch bestehende Daten können nicht gelöscht werden. Die Aktivierung des WORM-Schutzes für virtuelle Bänder hilft, diese Bänder während ihrer aktiven Nutzung zu schützen, bevor sie ausgeworfen und archiviert werden.

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

Manuelles Erstellen von Bändern

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

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

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.
3. Wählen Sie Bänder erstellen aus, um den Bereich Bänder erstellen zu öffnen.
4. Wählen Sie in Gateway (Gateway) einen Gateway aus. Das Band wird für dieses Gateway erstellt.

5. Wählen Sie als Bandtyp die Option Standard aus, um virtuelle Standardbänder zu erstellen. Wählen Sie WORM aus, um virtuelle WORM-Bänder (Write Once, Read Many) zu erstellen. Weitere Informationen finden Sie unter Write Once, Read Many (WORM)-Bandschutz.
6. Wählen Sie unter Number of tapes (Anzahl der Bänder) die Anzahl der Bänder aus, die Sie erstellen möchten. Weitere Hinweise zu Bandkontingenten finden Sie unter AWS Storage Gateway Kontingente.
7. Geben Sie unter Capacity (Kapazität) die Größe des virtuellen Bandes ein, das Sie erstellen möchten. Bänder müssen größer als 100 GiB sein. Hinweise zu Kapazitätskontingenten finden Sie unter AWS Storage Gateway Kontingente.
8. Geben Sie in Barcode-Präfix das Präfix an, das dem Barcode virtueller Bänder vorangestellt werden soll.

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

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

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

finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.

- Wählen Sie einen benutzerdefinierten Pool aus, sofern verfügbar. Sie konfigurieren benutzerdefinierte Bandpools so, dass sie entweder Deep Archive Pool oder Glacier Pool verwenden. Bänder werden in der konfigurierten Speicherklasse archiviert, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

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

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

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

Der Status der virtuellen Bänder wird zunächst auf CREATING (WIRD ERSTELLT) festgelegt, wenn die virtuellen Bänder erstellt werden. Nach der Erstellung der Bänder wird der Status in AVAILABLE geändert. Weitere Informationen finden Sie unter Grundlegendes zum Bandstatus.

Zulassen der automatischen Banderstellung

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

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

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

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

Wenn Sie ein Band auswerfen und es in den import/export slot, that tape does not count toward the minimum number of tapes specified in your automatic tape creation policy. Only tapes in the import/export Steckplatz gelangt, wird es als „verfügbar“ gewertet. Durch das Exportieren eines Bandes wird keine automatische Banderstellung ausgelöst. Nur Importe wirken sich auf die Anzahl der verfügbaren Bänder aus.

Ein Band mit demselben Barcode-Präfix aus dem import/export slot to a tape drive or storage slot reduces the number of tapes in the import/export Steckplatz entfernen. Das Gateway erstellt neue Bänder, um die Mindestanzahl verfügbarer Bänder für dieses Barcode-Präfix beizubehalten.

So lassen Sie die automatische Banderstellung zu

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.
3. Wählen Sie das Gateway aus, für das Sie automatisch Bänder erstellen möchten.

4. Wählen Sie im Menü Aktionen die Option Automatische Banderstellung konfigurieren.

   Die Seite Band automatisch erstellen wird angezeigt. Hier können Sie Optionen für die automatische Banderstellung konfigurieren, ändern oder löschen.

5. Um die automatische Banderstellung zuzulassen, wählen Sie Neues Element hinzufügen und konfigurieren dann die Einstellungen für die automatische Banderstellung.

6. Wählen Sie als Bandtyp die Option Standard aus, um virtuelle Standardbänder zu erstellen. Wählen Sie WORM, um virtuelle write-once-read-many(WORM-) Bänder zu erstellen. Weitere Informationen finden Sie unter Write Once, Read Many (WORM)-Bandschutz.

7. Geben Sie unter Mindestanzahl von Bändern die Mindestanzahl von virtuellen Bändern ein, die auf dem Tape Gateway jederzeit verfügbar sein sollen. Der gültige Bereich für diesen Wert ist mindestens 1 und maximal 10.

8. Geben Sie unter Capacity (Kapazität) die Kapazität der virtuellen Bänder in Byte an. Der gültige Bereich reicht von mindestens 100 GiB bis maximal 15 TiB.

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

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

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

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

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

- Wählen Sie einen benutzerdefinierten Pool aus, sofern verfügbar. Sie konfigurieren benutzerdefinierte Bandpools so, dass sie entweder Deep Archive Pool oder Glacier Pool verwenden. Bänder werden in der konfigurierten Speicherklasse archiviert, wenn sie von Ihrer Sicherungssoftware ausgeworfen werden.

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

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

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

    Der Status der verfügbaren virtuellen Bänder wird zunächst auf CREATING gesetzt, wenn die virtuellen Bänder erstellt werden. Nach der Erstellung der Bänder wird der Status in AVAILABLE geändert. Weitere Informationen finden Sie unter Grundlegendes zum Bandstatus.

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

Nächster Schritt

Verwenden von Tape Gateway

Erstellen eines benutzerdefinierten Bandpools

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

Themen

- Auswahl eines Bandpool-Typs
- Verwenden der Bandaufbewahrungssperre
- Erstellen eines benutzerdefinierten Bandpools

Auswahl eines Bandpool-Typs

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

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

Sie können die in S3 Glacier Flexible Retrieval archivierten Bänder zu einem späteren Zeitpunkt zu S3 Glacier Deep Archive verschieben. Weitere Informationen finden Sie unter Bänder in die Speicherklasse S3 Glacier Deep Archive verschieben.

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

Verwenden der Bandaufbewahrungssperre

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

Sie können die Bandaufbewahrungssperre in einem von zwei Modi konfigurieren:

- Governance-Modus — Bei der Konfiguration im Governance-Modus `storagegateway:BypassGovernanceRetention` können nur AWS Identity and Access Management (IAM-) Benutzer, die über die entsprechenden Berechtigungen verfügen, Bänder aus dem Pool entfernen. Wenn Sie die AWS Storage Gateway API zum Entfernen des Bandes verwenden, müssen Sie auch `BypassGovernanceRetention` auf `true` einstellen.
- Compliance-Modus – Wenn der Schutz im Compliance-Modus konfiguriert ist, kann er von keinem Benutzer entfernt werden, auch nicht vom AWS-Konto-Root-Benutzer.

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

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

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

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

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

Erstellen eines benutzerdefinierten Bandpools

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

So erstellen Sie einen benutzerdefinierten Bandpool

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

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

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

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

Ihre VTL-Geräte anschließen

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

Themen

- Herstellen einer Verbindung mit einem Microsoft Windows-Client
- Herstellen einer Verbindung mit einem 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.

So verbinden Sie VTL-Geräte mit einem Windows-Client

1. Starten `iscsicpl.exe`.

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

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

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

So überprüfen und aktualisieren Sie Treiber und Anbieter

1. Starten Sie auf Ihrem Windows-Client den Geräte-Manager.
2. Erweitern Sie Tape drives (Bandlaufwerke), öffnen Sie mit das Kontextmenü (Rechtsklick) eines der Bandlaufwerke und wählen Sie Properties (Eigenschaften) aus.
3. Überprüfen Sie auf der Registerkarte Driver (Treiber) des Dialogfelds Device Properties (Geräteeigenschaften), ob Microsoft der Driver Provider (Treiberanbieter) ist.
4. Wenn Microsoft nicht der Driver Provider (Treiberanbieter) ist, legen Sie den Wert wie folgt fest:
    a. Wählen Sie Update Driver (Treiber aktualisieren) aus.
    b. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Browse my computer for driver software (Auf dem Computer nach Treibersoftware suchen) aus.

c. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Let me pick from a list of device drivers on my computer (Aus einer Liste von Gerätetreibern auf dem Computer auswählen) aus.

d. Wählen Sie LTO Tape drive (LTO-Bandlaufwerk) und dann Next (Weiter) aus.

5. Wählen Sie Close (Schließen) aus, um das Fenster Update Driver Software (Treibersoftware aktualisieren) zu schließen, und überprüfen Sie, ob nun Microsoft als Wert für Driver Provider (Treiberanbieter) festgelegt ist.

6. Wiederholen Sie die Schritte zum Aktualisieren von Treiber und Anbieter für alle Bandlaufwerke.

Herstellen einer Verbindung mit einem Linux-Client

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

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

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

   Verwenden Sie den folgenden Befehl zum Installieren des Pakets.

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

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

   Verwenden Sie für RHEL 8 oder 9 den folgenden Befehl.

   ```
   sudo service iscsid status
   ```

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

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

   Die Ausgabe des Erkennungsbefehls gleicht der folgenden Beispielausgabe.

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

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

4. Stellen Sie eine Verbindung mit einem Ziel her.

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

   Verwenden Sie den folgenden -Befehl.

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

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

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

   Die Ausgabe des Befehls sollte der folgenden Beispielausgabe gleichen.

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

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

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

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

   Die Ausgabe des Befehls sollte der folgenden Beispielausgabe gleichen.

   ```
   total 0
   lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
   iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
   lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
   iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
   lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
   iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
   lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
   iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
   ```

```
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-lun-0
 -> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-
lun-0-nst -> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-lun-0
 -> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-
lun-0-nst -> ../../nst1
```

```
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-lun-0
 -> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-
lun-0-nst -> ../../nst2
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-lun-0
 -> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-
lun-0-nst -> ../../nst5
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-lun-0
 -> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-
lun-0-nst -> ../../nst3
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-lun-0
 -> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-
lun-0-nst -> ../../nst4
```

Nächster Schritt

Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung

Verwenden Sie Ihre Backup-Software, um Ihr Gateway-Setup zu testen

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

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

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

2. Sichern Sie Daten auf einem Band.
3. Archivieren Sie das Band.

4. Rufen Sie das Band aus dem Archiv ab.
5. Wiederherstellen von Daten von einem Band

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

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

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

Topics

- Testen Sie Ihr Setup mit Arcserve Backup
- Testen Ihrer Konfiguration mithilfe von Bacula Enterprise
- Testen Ihrer Konfiguration mithilfe von Commvault
- Testen Ihres Setups mithilfe von Dell EMC NetWorker
- Testen Sie Ihr Setup mithilfe von IBM Data Protect
- Testen Sie Ihr Setup mit OpenText Data Protector
- Testen Ihres Setups mithilfe von Microsoft System Center DPM
- Testen Sie Ihr Setup mit NovaStor DataCenter
- Testen Sie Ihr Setup mithilfe von Quest NetVault Backup
- Testen Sie Ihr Setup mithilfe von Veeam Backup and Replication
- Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec
- Testen Sie Ihr Setup mithilfe von Veritas NetBackup

Testen Sie Ihr Setup mit Arcserve Backup

Mit Arcserve Backup können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL) -Geräte verwalten. In diesem Thema finden Sie eine

grundlegende Anleitung für die Konfiguration von Arcserve Backup mit einem Tape Gateway und die Ausführung von Sicherungs- und Wiederherstellungsoperationen. Ausführliche Informationen zur Verwendung von Arcserve Backup finden Sie in der Arcserve Backup-Dokumentation.

Themen

- Konfigurieren von Arcserve für das Arbeiten mit VTL-Geräten
- Laden von Bändern in einen Medienpool
- Sichern von Daten auf einem Band
- Archivieren eines Bandes
- Wiederherstellen von Daten von einem Band

Konfigurieren von Arcserve für das Arbeiten mit VTL-Geräten

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

So suchen Sie nach VTL-Geräten

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

Laden von Bändern in einen Medienpool

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

So starten Sie die Band-Engine

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

5. Wählen Sie Quick Inventory (Schnellinventarisierung) aus, um Medieninformationen aus der Datenbank abzurufen.

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

So importieren Sie Bänder

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

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

Sichern von Daten auf einem Band

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

So sichern Sie Daten auf einem Band

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

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

Archivieren eines Bandes

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

So archivieren Sie ein Band

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

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

Wiederherstellen von Daten von einem Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

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

2. Verwenden Sie ArcServer, um die Daten wiederherzustellen. Der Vorgang ist identisch mit dem Vorgang zur Wiederherstellung von Daten von physischen Bändern. Anweisungen finden Sie in der Arcserve Backup-Dokumentation.

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

So stellen Sie Daten von einem Band wieder her

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

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Ihrer Konfiguration mithilfe von Bacula Enterprise

Mit Bacula Enterprise können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL) -Geräte verwalten. In diesem Thema finden Sie eine grundlegende Dokumentation für die Konfiguration der Bacula 10-Sicherungsanwendung für ein Tape Gateway und die Ausführung von Sicherungen und Wiederherstellungen. Ausführliche Informationen zur Verwendung von Bacula finden Sie in den Handbüchern und der Dokumentation zu Bacula Systems oder wenden Sie sich an Bacula Systems.

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

Einrichten von Bacula Enterprise

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

Einrichten von Bacula

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

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

Konfigurieren von Bacula für das Arbeiten mit VTL-Geräten

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

Konfigurieren von Bacula

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

Sichern von Daten auf einem Band

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

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

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

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

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

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

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

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

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

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

Archivieren eines Bandes

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

So archivieren Sie ein Band

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

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

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

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

Wiederherstellen von Daten von einem archivierten und abgerufenen Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

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

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

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

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

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

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

Testen Ihrer Konfiguration mithilfe von Commvault

Mit Commvault können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre VTL-Geräte (Virtual Tape Library) verwalten. In diesem Thema finden Sie eine grundlegende Anleitung zur Konfiguration der Commvault-Sicherungsanwendung für ein Tape Gateway, zur Ausführung eines Sicherungsarchivs und zum Abrufen Ihrer Daten von archivierten Bändern. Ausführliche Informationen zur Verwendung von Commvault finden Sie in der Commvault-Dokumentation.

Themen

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

Konfigurieren von Commvault für das Arbeiten mit VTL-Geräten

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

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

So konfigurieren Sie Commvault

1. Wählen Sie im Hauptmenü der CommCell Konsole Storage und anschließend Expert Storage Configuration, um das MediaAgents Dialogfeld „Auswählen“ zu öffnen.
2. Wählen Sie den verfügbaren Medienagenten, den Sie verwenden möchten, Add (Hinzufügen) und dann OK (OK) aus.
3. Wählen Sie im Dialogfeld Expert Storage Configuration (Fortgeschrittene Speicherkonfiguration) die Option Start (Starten) und dann die Option Detect/Configure Devices (Geräte entdecken/konfigurieren) aus.
4. Lassen Sie die Optionen in Device Type (Gerätetyp) ausgewählt und wählen Sie Exhaustive Detection (Ausführliche Erkennung) und dann OK (OK) aus.
5. Wählen Sie im Bestätigungsfeld Confirm Exhaustive Detection (Ausführliche Erkennung bestätigen) die Option Yes (Ja) aus.
6. Wählen Sie im Dialogfeld Device Selection (Geräteauswahl) Ihre Bibliothek und alle zugehörigen Laufwerke und dann OK (OK) aus. Warten Sie, bis Ihre Geräte erkannt werden, und wählen Sie dann die Option Close (Schließen) aus, um den Protokollbericht zu schließen.
7. Rechtsklicken Sie auf Ihre Bibliothek und wählen Sie die Option Configure (Konfigurieren) und dann Yes (Ja) aus. Schließen Sie das Dialogfeld für die Konfiguration.
8. Wählen Sie im Dialogfeld Does this library have a barcode reader? (Besitzt diese Bibliothek einen Strichcodeleser?) die Option Yes (Ja) und dann als Gerätetyp IBM ULTRIUM V5 (IBM ULTRIUM V5) aus.
9. Wählen Sie im CommCell Browser „Speicherressourcen“ und anschließend „Bibliotheken“, um Ihre Bandbibliothek anzuzeigen.
10. Um Ihre Bänder in der Bibliothek anzuzeigen, öffnen Sie das Kontextmenü (Rechtsklick) für die Bibliothek und wählen dann Discover Media (Medien entdecken), Media location (Medienspeicherort) und Media Library (Medienbibliothek) aus.
11. Um Ihre Bänder zu mounten, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre Medien und wählen Load (Laden) aus.

Erstellen einer Speicher-Richtlinie und eines Subclient

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

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

So erstellen Sie eine Speicher-Richtlinie

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

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

So erstellen sie eine Subclient-Richtlinie

1. Wählen Sie im CommCell Browser Client-Computer und dann Ihren Client-Computer aus. Wählen Sie Dateisystem und dann defaultBackupSet.
2. Klicken Sie mit der rechten Maustaste defaultBackupSet, wählen Sie Alle Aufgaben und dann Neuer Subclient.
3. Geben Sie im Feld Eigenschaften des Subclients einen Namen in SubClient das Feld Name ein, und klicken Sie dann auf OK.
4. Wählen Sie Browse (Durchsuchen) aus, navigieren Sie zu den Dateien, die Sie sichern möchten, wählen Sie Add (Hinzufügen) aus und schließen Sie dann das Dialogfeld.
5. Wählen Sie im Eigenschaftsfeld Subclient (Unterclient) die Registerkarte Storage Device (Speichergerät), unter Storage policy (Speicherrichtlinie) eine Speicherrichtlinie und dann OK (OK) aus.
6. Verknüpfen Sie im nun angezeigten Fenster Backup Schedule (Sicherungszeitplan) den neuen Unterclient mit einem Sicherungszeitplan.
7. Wählen Sie Do Not Schedule (Nicht planen) für eine einmalige Sicherung oder für On-Demand-Sicherungen und dann OK (OK) aus.

   Sie sollten jetzt Ihren Subclient auf der defaultBackupSetRegisterkarte sehen.

Sichern von Daten auf einem Band in Commvault

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

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

Archivieren eines Bandes in Commvault

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

So archivieren Sie ein Band

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

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

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

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

Wiederherstellen von Daten von einem Band

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

- Wiederherstellen durch Subclient
- Wiederherstellen durch Auftrags-ID

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

1. Wählen Sie im CommCell Browser Client-Computer und dann Ihren Client-Computer aus. Wählen Sie Dateisystem und dann defaultBackupSet.

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

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

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

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

1. Wählen Sie im CommCell Browser Speicherressourcen, dann Bibliotheken und anschließend Ihre Bibliothek aus. Wählen Sie Medien nach Speicherort und dann Medien in Bibliothek aus.
2. Rechtsklicken Sie auf das abgerufene Band. Wählen Sie All Tasks (Alle Aufgaben) und dann Catalog (Katalog) aus.
3. Wählen Sie im Dialogfeld Catalog Media (katelogmedien) die Option Catalog only (Nur Katalog) und dann OK (OK) aus.
4. Wählen Sie CommCell Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.

5. Öffnen Sie nach erfolgreichem Abschluss des Auftrags das Kontextmenü (Rechtsklick) für Ihr Band. Wählen Sie View (Anzeigen) und dann View Catalog Contents (Kataloginhalt anzeigen) aus. Notieren Sie zur späteren Verwendung die Job ID (Auftrags-ID).
6. Wählen Sie die Option Recatalog/Merge (Neu katalogisieren/Zusammenführen) aus. Stellen Sie sicher, dass im Dialogfeld Catalog Media (Katalogmedien) die Option Merge only (Nur zusammenführen) ausgewählt ist.
7. Wählen Sie Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.
8. Wenn der Job erfolgreich war, wählen Sie CommCell Home, dann Systemsteuerung und anschließend. Browse/Search/Recovery
9. Wählen Sie Show aged data during browse and recovery (Veraltete Daten während Durchsuchen und Wiederherstellen anzeigen) und dann OK (OK) aus. Schließen Sie dann Control Panel (Steuerungsbereich).
10. Klicken Sie im CommCell Browser mit der rechten Maustaste auf Client-Computer und wählen Sie dann Ihren Client-Computer aus. Wählen Sie View (Anzeigen) und dann Job History (Auftragsverlauf) aus.
11. Wählen Sie im Dialogfeld Job History Filter (Auftragsverlaufsfilter) die Option Advanced (Erweitert) aus.
12. Wählen Sie Include Aged Data (Veraltete Daten einschließen) und dann OK (OK) aus.
13. Wählen Sie im Dialogfeld Job History (Auftragsverlauf) OK (OK) aus, um die Registerkarte history of jobs (Verlauf von Aufträgen) zu öffnen.
14. Suchen Sie den Auftrag, den Sie wiederherstellen möchten, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie dann Browse and Restore (Durchsuchen und Wiederherstellen) aus.
15. Wählen Sie im Dialogfeld Browse and Restore (Durchsuchen und Wiederherstellen) die Option View Content (Inhalt anzeigen) aus.
16. Wählen Sie die Dateien aus, die Sie wiederherstellen möchten, und ann Recover All Selected (Alle ausgewählten Dateien wiederherstellen) aus.
17. Wählen Sie Startseite und dann Auftrags-Controller aus, um den Status des Wiederherstellungsauftrags zu überwachen.

Testen Ihres Setups mithilfe von Dell EMC NetWorker

Mit Dell EMC NetWorker können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL) -Geräte verwalten. In diesem Thema finden Sie grundlegende Dokumentation zur Konfiguration der Dell EMC NetWorker Software für die Verwendung mit einem Tape Gateway und zur Durchführung von Backups, einschließlich der Konfiguration von Speichergeräten, dem Schreiben von Daten auf ein Band, der Archivierung eines Bandes und der Wiederherstellung von Daten von einem Band.

Ausführliche Informationen zur Installation und Verwendung der Dell EMC NetWorker Software finden Sie in der NetWorker Dokumentation.

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

Themen

- Konfigurieren der Arbeit mit VTL-Geräten
- Zulassen des Imports von WORM-Bändern in Dell EMC NetWorker
- Daten auf einem Band in Dell EMC sichern NetWorker
- Archivieren eines Bandes in Dell EMC NetWorker
- Wiederherstellen von Daten von einem archivierten Band in Dell EMC NetWorker

Konfigurieren der Arbeit mit VTL-Geräten

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

Die Software erkennt Tape-Gateway-Geräte nicht automatisch. Um Ihre VTL-Geräte mit der NetWorker Software vertraut zu machen und sie von der Software erkennen zu lassen, konfigurieren Sie die Software manuell. Im Folgenden nehmen wir an, dass Sie die Software ordnungsgemäß installiert haben und mit der Management Console vertraut sind. Weitere Informationen zur Management Console finden Sie im Abschnitt zur NetWorker Management Console-Schnittstelle im Dell EMC NetWorker Administration Guide.

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

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

    a. Geben Sie an der Menüaufforderung die entsprechende Zahl ein, um Configure an Autodetected SCSI Jukebox auszuwählen.

    b. Wenn Sie aufgefordert werden, einen Namen für das Jukebox-Gerät einzugeben, geben Sie einen Namen wie ein. `AWSVTL`

    c. Wenn Sie aufgefordert werden, die NetWorker automatische Reinigung einzuschalten, geben Sie einno.

    d. Wenn Sie aufgefordert werden, die automatische Konfiguration zu umgehen, geben Sie einno.

    e. Wenn Sie aufgefordert werden, eine weitere Jukebox zu konfigurieren, geben Sie ein. no
7. Wenn „jbconfig“ abgeschlossen ist, kehren Sie zur Networker-GUI zurück und drücken Sie F5, um den Vorgang zu aktualisieren.
8. Wählen Sie Ihre Bibliothek aus, um Ihre Bänder im linken Bereich und die entsprechende Liste der leeren Volume-Slots im rechten Fensterbereich anzuzeigen.
9. Wählen Sie in der Volume-Liste die Volumes aus, die Sie aktivieren möchten (ausgewählte Volumes werden hervorgehoben), öffnen Sie das Kontextmenü (Rechtsklick) für die ausgewählten Volumes und wählen Sie dann Ablegen aus. Mit dieser Aktion wird das Band vom E/A-Slot in den Volume-Slot verschoben.

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

Zulassen des Imports von WORM-Bändern in Dell EMC NetWorker

Sie sind jetzt bereit, Bänder von Ihrem Tape Gateway in die Dell EMC NetWorker Bibliothek zu importieren.

Bei den virtuellen Bändern handelt es sich um WORM-Bänder (Write Once Read Many), aber Dell EMC NetWorker erwartet Bänder, die keine WORM-Bänder sind. Damit Dell EMC NetWorker mit Ihren virtuellen Bändern arbeiten kann, müssen Sie den Import von Bändern in Medienpools aktivieren, die keine WORM-Programme sind.

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

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

Daten auf einem Band in Dell EMC sichern NetWorker

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

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

   Erstellen Sie einen Medienpool und schreiben Sie Daten auf ein virtuelles Band indem Sie dieselben Verfahren wie bei physischen Bändern verwenden. Ausführliche Informationen finden Sie im Abschnitt zum Sichern von Daten im Dell EMC NetWorker Administration Guide.
2. Schreiben Sie Daten auf das Band. Sie sichern Daten, indem Sie die Dell EMC NetWorker Benutzeranwendung anstelle der Dell EMC NetWorker Management Console verwenden. Die Dell EMC NetWorker Benutzeranwendung wird als Teil der NetWorker Installation installiert.

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

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

Archivieren eines Bandes in Dell EMC NetWorker

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

Um ein Band mit Dell EMC zu archivieren NetWorker

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

Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS angezeigt. Wenn die Archivierung gestartet wird, wird der Status

in ARCHIVING geändert. Nach Abschluss der Archivierung wird das Band nicht mehr in der VTL aufgeführt.

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

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

Wiederherstellen von Daten von einem archivierten Band in Dell EMC NetWorker

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig:

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

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Sie Ihr Setup mithilfe von IBM Data Protect

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

Dieses Thema enthält grundlegende Informationen zur Konfiguration der IBM Data Protect-Backup-Software für ein Tape Gateway. Es enthält auch grundlegende Informationen zur Durchführung von Sicherungs- und Wiederherstellungsvorgängen mit IBM Data Protect. Weitere Informationen zur Verwaltung der IBM Data Protect-Backup-Software finden Sie in der IBM Data Protect-Dokumentation.

Die IBM Data Protect-Backup-Software unterstützt AWS Storage Gateway die folgenden Betriebssysteme.

- Microsoft Windows Server

- Red Hat Linux

Informationen zu den von IBM Data Protect unterstützten Geräten für Windows finden Sie unter IBM Data Protect (ehemals Tivoli Storage Manager) Unterstützte Geräte für AIX, HP-UX, Solaris und Windows.

Informationen zu Geräten, die von IBM Data Protect für Linux unterstützt werden, finden Sie unter Von IBM Data Protect (ehemals Tivoli Storage Manager) unterstützte Geräte für Linux.

Themen

- IBM Data Protect einrichten
- IBM Data Protect für die Verwendung mit VTL-Geräten konfigurieren
- In IBM Data Protect Daten auf ein Band schreiben
- Daten von einem in IBM Data Protect archivierten Band wiederherstellen

IBM Data Protect einrichten

Nachdem Sie Ihre VTL-Geräte mit Ihrem Client verbunden haben, konfigurieren Sie die IBM Data Protect-Software so, dass sie sie erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit Ihrem Client verbinden, finden Sie unter Ihre VTL-Geräte anschließen.

Um IBM Data Protect einzurichten

1. Besorgen Sie sich eine lizenzierte Kopie der IBM Data Protect-Software von IBM.
2. Installieren Sie die IBM Data Protect-Software in Ihrer lokalen Umgebung oder Ihrer EC2 Amazon-In-Cloud-Instanz. Weitere Informationen finden Sie in der IBM Dokumentation zur Installation und Aktualisierung von IBM Data Protect.

   Weitere Informationen zur Konfiguration der IBM Data Protect-Software finden Sie unter Konfiguration virtueller AWS Bandbibliotheken von Tape Gateway für einen IBM Data Protect-Server.

IBM Data Protect für die Verwendung mit VTL-Geräten konfigurieren

Als Nächstes konfigurieren Sie IBM Data Protect so, dass es mit Ihren VTL-Geräten funktioniert. Sie können IBM Data Protect so konfigurieren, dass es mit VTL-Geräten auf Microsoft Windows Server oder Red Hat Linux funktioniert.

IBM Data Protect für Windows konfigurieren

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

So konfigurieren Sie IBM Data Protect für Microsoft Windows

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

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

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

Konfigurieren Sie IBM Data Protect für Linux

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

Um IBM Data Protect für Linux zu konfigurieren

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

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

In IBM Data Protect Daten auf ein Band schreiben

Beim Schreiben von Daten auf ein virtuelles Band auf einem Tape Gateway verwenden Sie das gleiche Verfahren und die gleichen Sicherungsrichtlinien wie beim Schreiben auf physische Bänder. Erstellen Sie die erforderliche Konfiguration für Sicherungs- und Wiederherstellungsaufträge. Weitere Informationen zur Konfiguration von IBM Data Protect finden Sie unter Überblick über die Verwaltungsaufgaben für IBM Data Protect.

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe einen Fehler aufweist, schlägt die Backup-Aufgabe möglicherweise fehl. Wenn der Backup-Job fehlschlägt, ändert sich der Bandstatus in IBM Data Protect auf ReadOnly. Wenn Sie wissen, dass das Band nicht vollständig genutzt wurde, können Sie den Bandstatus manuell wieder auf ReadWriteändern und den Backup-Job entweder fortsetzen oder mit demselben Band erneut starten. IBM Data Protect setzt den fehlgeschlagenen Backup-Job möglicherweise auf einem anderen Band fort, wenn andere Bänder mit ReadWriteStatus verfügbar sind.

Daten von einem in IBM Data Protect archivierten Band wiederherstellen

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Detaillierte Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Stellen Sie die Daten mithilfe der IBM Data Protect-Backup-Software wieder her. Dazu erstellen Sie einen Wiederherstellungspunkt, ganz wie bei der Wiederherstellung von Daten von physischen Bändern. Weitere Informationen zur Konfiguration von IBM Data Protect finden Sie unter Überblick über die Verwaltungsaufgaben für IBM Data Protect.

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Sie Ihr Setup mit OpenText Data Protector

Mit Data Protector können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL) OpenText -Geräte verwalten. In diesem Thema finden Sie grundlegende Dokumentation zur Konfiguration der OpenText Data Protector-Software für ein Tape Gateway und zur Durchführung von Sicherungs- und Wiederherstellungsvorgängen. Ausführliche Informationen zur Verwendung der OpenText Data Protector-Software finden Sie in der OpenText Data Protector-Dokumentation. Weitere Informationen zu kompatiblen Sicherungsanwendungen finden Sie unter Unterstützte Sicherungsanwendungen von Drittanbietern für ein Tape Gateway.

Themen

- OpenText Data Protector für die Verwendung mit VTL-Geräten konfigurieren
- Virtuelle Bänder für die Verwendung mit Data Protector vorbereiten
- Laden von Bändern in einen Medienpool
- Sichern von Daten auf einem Band
- Archivieren eines Bandes
- Wiederherstellen von Daten von einem Band

OpenText Data Protector für die Verwendung mit VTL-Geräten konfigurieren

Nachdem Sie die VTL-Geräte (Virtual Tape Library) mit dem Client verbunden haben, konfigurieren Sie OpenText Data Protector so, dass es Ihre Geräte erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Client verbinden können, finden Sie unter Ihre VTL-Geräte anschließen.

Die OpenText Data Protector-Software erkennt Tape Gateway-Geräte nicht automatisch. Damit die Software diese Geräte erkennt, fügen Sie die VTL-Geräte manuell hinzu und lassen Sie sie anschließend wie folgt erkennen.

So fügen Sie VTL-Geräte hinzu

1. Wählen Sie im Hauptfenster von OpenText Data Protector in der Liste oben links die Ablage Geräte und Medien aus.

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

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

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

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

      - Barcode reader support (Strichcode-Leser-Unterstützung)
      - Automatically discover changed SCSI address (Geänderte SCSI-Adressen automatisch entdecken)
      - SCSI Reserve/Release (robotic control) (SCSI reservieren/freigeben (Robotiksteuerung)

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

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

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

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

Virtuelle Bänder für die Verwendung mit Data Protector vorbereiten

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

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

In den folgenden Abschnitten finden Sie Anleitungen für diesen Prozess.

Laden virtueller Bänder in eine Bandbibliothek

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

So laden Sie virtuelle Bänder in Ihre Bandbibliothek

1. Wählen Sie das Pluszeichen neben Ihrer Bandbibliothek, um die Knoten für Robotik-Pfade, Laufwerke und Slots anzuzeigen.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für Drives (Laufwerke), wählen Sie Add Drive (Laufwerk hinzufügen) aus, geben Sie einen Namen für Ihr Band ein und wählen Sie dann Next (Weiter) aus, um fortzufahren.

3. Wählen Sie das Bandlaufwerk, das Sie in SCSI address of data drive (SCSI-Adresse des Datenlaufwerks) hinzufügen möchten. Wählen Sie anschließend Automatically discover changed SCSI address (Geänderte SCSI-Adressen automatisch entdecken) und dann Next (Weiter) aus.
4. Wählen Sie im nächsten Bildschirm Advanced (Erweitert) aus. Das Popup-Fenster Advanced Options (Erweiterte Optionen) wird angezeigt.

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

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

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

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

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

Laden virtueller Bänder in Slots

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

So Laden Sie ein Band in einen Slot

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

Erstellen eines Medienpools

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

So erstellen Sie einen Medienpool

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

Laden von Bändern in einen Medienpool

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

So laden Sie ein virtuelles Band in einen Medienpool

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

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

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

Zu diesem Zeitpunkt sollten Sie alles konfiguriert haben, damit Sie Ihre virtuelle Bandbibliothek mit Data Protector verwenden können. Prüfen Sie anhand des folgenden Verfahrens, dass dem so ist.

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

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

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

Sichern von Daten auf einem Band

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

So sichern Sie Daten auf einem Band

1. Wählen Sie im Drop-down-Menü in der oberen linken Ecke des Fensters die Option Backup aus.
2. Erweitern Sie den Backup-Navigationsbaum im linken Bereich.
3. Klicken Sie mit der rechten Maustaste auf Dateisystem, um das Kontextmenü zu öffnen, und wählen Sie dann Backup hinzufügen.
4. Wählen Sie im Bildschirm Create New Backup (Neue Sicherung erstellen) unter File system (Dateisystem) die Option Blank File System Backup (Leere Dateisystemsicherung) und dann OK (OK) aus.

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

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

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

Archivieren eines Bandes

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

So prüfen Sie den Inhalt eines Bands vor dem Archivieren

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

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

So werfen Sie ein Band aus und archivieren es

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

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

Wiederherstellen von Daten von einem Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

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

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

So stellen Sie Daten von einem Band wieder her

1. Wählen Sie im Drop-down-Menü in der oberen linken Ecke des Fensters die Option Wiederherstellen aus.

2. Wählen Sie in der linken Navigationsstruktur das Datei- oder Datenbanksystem aus, das Sie wiederherstellen möchten. Achten Sie darauf, dass das Kontrollkästchen für die wiederherzustellende Sicherung ausgewählt ist. Wählen Sie Restore (Wiederherstellen) aus.
3. Wählen Sie im Fenster Start Restore Session (Wiederherstellungssitzung starten) die Option Needed Media (Benötigte Medien) aus. Wählen Sie All media (Alle Medien) aus. Anschließend sollte Ihnen das Band angezeigt werden, das ursprünglich für die Sicherung verwendet wurde. Wählen Sie dieses Band und dann Close (Schließen) aus.
4. Akzeptieren Sie im Fenster Start Restore Session (Wiederherstellungssitzung starten) die Standardeinstellungen aus. Wählen Sie Next (Weiter) und dann Finish Beenden) aus.

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Ihres Setups mithilfe von Microsoft System Center DPM

Sie können Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre VTL-Geräte (Virtual Tape Library) verwalten, indem Sie Microsoft System Center Data Protection Manager (DPM) verwenden. In diesem Thema finden Sie eine grundlegende Anleitung zur Konfiguration der DPM-Sicherungsanwendung für ein Tape Gateway sowie zur Durchführung einer Sicherung und Wiederherstellung.

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

Themen

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

Konfigurieren von DPM zur Erkennung von VTL-Geräten

Sobald Sie die VTL (Virtual Tape Library)-Geräte mit dem Windows-Client verbunden haben, müssen Sie die DPM-Software so konfigurieren, dass sie Ihre Geräte erkennt. Weitere Informationen dazu,

wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Ihre VTL-Geräte anschließen.

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

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

Aktualisieren Sie die Treiber der VTL-Geräte wie folgt:

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

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

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

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

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

> **Note**
>
> Der Verzeichnispfad kann sich je nach Ihrer Version von System Center oder DPM ändern.

Wenn diese Datei vorhanden ist, wird sie DPMDrive MappingTool überschrieben. Soll die ursprüngliche Datei erhalten bleiben, müssen Sie eine Sicherungskopie erstellen.

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

> **Note**
>
> Der Verzeichnispfad kann sich je nach Ihrer Version von System Center oder DPM ändern.

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

Die Ausgabe dieses Befehls sieht wie folgt aus:

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

Importieren eines Bands in DPM

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

So importieren Sie Bänder in die Bibliothek der DPM-Sicherungsanwendung

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

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

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

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

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

   > **Note**
   >
   > Die Identifizierung eines Bandes kann einige Sekunden oder Minuten dauern.
   > Wenn Barcodes auf den Bändern nicht korrekt angezeigt werden, müssen Sie den Media Changer-Treiber auf Sun/ Library ändern. StorageTek Weitere Informationen finden Sie unter Anzeigen von Barcodes für Bänder in Microsoft System Center DPM.

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

Schreiben von Daten auf ein Band in DPM

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

Standardmäßig beträgt die Kapazität eines Bandes 30 GB. Wenn Sie Daten sichern, die größer als die Kapazität eines Bandes sind, tritt ein Geräte-E/A-Fehler auf. Wenn die Position, an der der Fehler aufgetreten ist, größer als die Größe des Bandes ist, behandelt Microsoft DPM den Fehler als Hinweis auf das Bandende. Wenn die Position, an der der Fehler aufgetreten ist, kleiner als

die Größe des Bandes ist, schlägt der Sicherungsauftrag fehl. Um dieses Problem zu beheben, ändern Sie den `TapeSize`-Wert im Registry-Eintrag, sodass er der Größe Ihres Bandes entspricht. Informationen zu diesem Verfahren finden Sie unter Fehler-ID: 30101 im Microsoft System Center.

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

Archivieren eines Bands mithilfe von DPM

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

Archivieren Sie ein Band wie folgt in DPM:

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

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

Wiederherstellen von Daten von einem in DPM archivierten Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

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

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Sie Ihr Setup mit NovaStor DataCenter

Mithilfe NovaStor DataCenter/Network. In this topic, you can find basic documentation on how to configure the NovaStor DataCenter/Network backup application for a Tape Gateway and perform backup and restore operations. For detailed information about how to use NovaStor DataCenter/Network, refer to the NovaStor DataCenter/Network der Dokumentation können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre VTL-Geräte (Virtual Tape Library) verwalten.

/Netzwerk einrichten NovaStor DataCenter

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

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

Konfiguration von NovaStor DataCenter /Network für die Verwendung mit VTL-Geräten

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

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

Um NovaStor DataCenter /Network so zu konfigurieren, dass es mit VTL-Geräten funktioniert

1. Wählen Sie in der NovaStor DataCenter /Network Admin-Konsole Media Management und dann Storage Management aus.
2. Öffnen Sie im Menü Storage Targets (Speicherziele) das Kontextmenü (Rechtsklick) für Media Management Servers (Medienverwaltungsserver). Wählen Sie New (Neu) und OK (OK) aus, um einen storage (Speicher)-Knoten zu erstellen und vorab auszufüllen.

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

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

3. Öffnen Sie das Kontextmenü (Rechtsklick) für den erstellten storage (Speicher)-Knoten und wählen Sie New Library (Neue Bibliothek) aus.
4. Wählen Sie den Bibliotheksserver aus der Liste aus. Die Bibliotheksliste wird automatisch gefüllt.
5. Geben Sie der Bibliothek einen Namen und wählen Sie dann OK (OK) aus.
6. Wählen Sie die Bibliothek zur Anzeige aller Eigenschaften der virtuellen Storage-Gateway-Bandbibliothek aus.
7. Erweitern Sie im Menü Storage Targets (Speicherziele) die Option Backup Servers (Sicherungsserver), öffnen Sie das Kontextmenü (Rechtsklick) für den Server und wählen Sie Attach Library (Bibliothek anfügen) aus.
8. Wählen Sie im daraufhin angezeigten Dialogfeld „Bibliothek anhängen“ den LTO5Medientyp aus, und klicken Sie dann auf OK.

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

Erstellen eines Bandpools

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

Ein Bandpool kann in drei Schritten erstellt werden:

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

So erstellen Sie einen Scratch-Pool.

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

Sie weisen Sie dem Scratch-Pool Bänder zu

1. Wählen Sie im linken Navigationsmenü Tape Library Management (Bandbibliothekverwaltung) aus.
2. Wählen Sie die Registerkarte Library (Bibliothek) aus, um den Bibliotheksbestand anzuzeigen.
3. Wählen Sie die Bänder aus, die Sie dem Scratch-Pool zuweisen möchten. Stellen Sie sicher, dass für die Bänder der korrekte Medientyp festgelegt ist.

4. Öffnen Sie das Kontextmenü (Rechtsklick) für die Bibliothek und wählen Sie Add to Scratch Pool (Zum Scratch-Pool hinzufügen) aus.

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

So erstellen Sie einen Band-Pool

1. Wählen Sie im linken Navigationsmenü Tape Library Management (Bandbibliothekverwaltung) aus.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für die Registerkarte Media Pools (Medienpools) und wählen Sie Create Media Pool (Medienpool erstellen) aus.
3. Geben Sie dem Medienpool einen Namen und wählen Sie Backup Server (Sicherungsserver) aus.
4. Wählen Sie eine Bibliothekspartition für den Medienpool aus.
5. Wählen Sie den Scratch-Pool aus, aus dem der Pool die Bänder erhalten soll.
6. Wählen Sie in Schedule (Plan) die Option Not Scheduled (Nicht geplant) aus.

Konfigurieren des Medienimports und -exports zum Archivieren von Bändern

NovaStor DataCenter/Network can use import/exportSteckplätze, wenn sie Teil des Media Wechslers sind.

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

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

So konfigurieren Sie den Medienimport- und export

1. Navigieren Sie zu Tape Library Management (Bandbibliothekverwaltung). Wählen Sie einen Server als Media Management Server (Medienverwaltungsserver) und dann Library (Bibliothek) aus.
2. Wählen Sie die Registerkarte Off-site Locations (Speicherort außerhalb) aus.

3. Öffnen Sie das Kontextmenü (Rechtsklick) für den weißen Bereich und wählen Sie Add (Hinzufügen) aus, um einen neuen Bereich zu öffnen.
4. Geben Sie im Bereich **`S3 Glacier Flexible Retrieval`** oder **`S3 Glacier Deep Archive`** ein und fügen Sie im Textfeld optional eine Beschreibung hinzu.

Sichern von Daten auf einem Band

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

> **Note**
>
> Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, schlägt die Backup-Aufgabe fehl, und das Band kann nicht mehr beschrieben werden. Sie können das Band archivieren oder weiterhin Daten daraus lesen. Um die fehlgeschlagenen Backup-Aufgabe abzuschließen, müssen Sie sie erneut auf ein neues Band übermitteln.

Archivieren eines Bandes

Wenn Sie ein Band archivieren, wirft Tape Gateway das Band aus der Bandbibliothek in den Speicherschacht aus. Anschließend exportiert es das Band mithilfe Ihrer Backup-Anwendung, d. h. / Network, aus dem Steckplatz in das Archiv. NovaStor DataCenter

So archivieren Sie ein Band

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

Es kann einige Zeit dauern, bis die Archivierung abgeschlossen ist. Als Status des Bands wird zunächst IN TRANSIT TO VTS angezeigt. Wenn die Archivierung gestartet wird, wird der Status

in ARCHIVING geändert. Nach Abschluss der Archivierung wird das Band nicht mehr in der VTL aufgeführt.

Stellen Sie unter NovaStor DataCenter /Network sicher, dass sich das Band nicht mehr im Speichersteckplatz befindet.

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

Wiederherstellen von Daten von einem archivierten und abgerufenen Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Detaillierte Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie die NovaStor DataCenter /Network-Software, um die Daten wiederherzustellen. Dazu aktualisieren Sie den E-Mail-Slot und verschieben genau wie beim Wiederherstellen von Daten von physischen Bändern jedes abzurufende Band in einen leeren Slot. Informationen zum Wiederherstellen von Daten finden Sie in der Dokumentation NovaStor DataCenter /Network.

Gleichzeitiges Schreiben von mehreren Sicherungsaufträgen auf ein Bandlaufwerk

In der NovaStor Software können Sie mithilfe der Multiplexfunktion mehrere Jobs gleichzeitig auf ein Bandlaufwerk schreiben. Diese Funktion ist verfügbar, wenn ein Multiplexer für einen Medienpool verfügbar ist. Informationen zur Verwendung von Multiplexing finden Sie unter Documentation / Network. NovaStor DataCenter

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

Wenn Sie Ihre VTL-Geräte so konfigurieren, dass sie mit NovaStor DataCenter /Network funktionieren, wird möglicherweise eine Fehlermeldung angezeigt, die lautet. `External Program did not exit correctly` Dieser Fehler tritt auf, weil der Elementzuweisungsbereich von Storage Gateway für Speicherlaufwerke und Bandlaufwerke die Anzahl überschreitet, die NovaStor DataCenter /Network zulässt.

Storage Gateway gibt 3200 Speicher und import/export slots, which is more than the 2400 limit that NovaStor DataCenter/Network allows. To resolve this issue, you add a configuration file that activates

the NovaStor software to limit the number of storage and import/export Steckplätze zurück und konfiguriert den Elementzuweisungsbereich vorkonfiguriert.

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

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

```
port:12001
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. Fügen Sie die Bibliothek zum Medienverwaltungsserver hinzu.
5. Verschieben Sie mithilfe des folgenden Befehls ein Band aus dem Import-/Export-Steckplatz in die Bibliothek. Ersetzen Sie den Namen der Beispielbibliothek durch den Namen der Bibliothek in Ihrer Einrichtung.

   ```
   C:\Program Files\NovaStor\DataCenter\Hitback\tape\ophijacc.exe -c VTL-ec2amaz-uko8jfj-ec2amaz-uko8jfj.lcfg
   ```

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

Testen Sie Ihr Setup mithilfe von Quest NetVault Backup

Mit Quest (ehemals Dell) NetVault Backup können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL) -Geräte verwalten.

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

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

Themen

- Konfiguration von Quest NetVault Backup für die Arbeit mit VTL-Geräten
- Daten im Quest NetVault Backup auf einem Band sichern
- Archivieren eines Bandes mithilfe von Quest NetVault Backup
- Daten von einem in Quest NetVault Backup archivierten Band wiederherstellen

Konfiguration von Quest NetVault Backup für die Arbeit mit VTL-Geräten

Nachdem Sie die VTL-Geräte (Virtual Tape Library) mit dem Windows-Client verbunden haben, konfigurieren Sie Quest NetVault Backup so, dass es Ihre Geräte erkennt. Weitere Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Ihre VTL-Geräte anschließen.

Die Quest NetVault Backup-Anwendung erkennt Tape Gateway-Geräte nicht automatisch. Sie müssen die Geräte manuell hinzufügen, um sie der Quest NetVault Backup-Anwendung zugänglich zu machen, und dann die VTL-Geräte erkennen.

Hinzufügen von VTL-Geräten

So fügen Sie VTL-Geräte hinzu

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

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

   Quest NetVault Backup zeigt all Ihre Laufwerke und die 10 Schächte an, zu denen Sie Ihre Laufwerke hinzufügen können. Die Schächte werden nacheinander angezeigt.
8. Wählen Sie das Laufwerk aus, das Sie dem angezeigten Schacht hinzufügen möchten, und dann Next (Weiter) aus.

   > **Important**
   >
   > Wenn Sie ein Laufwerk einem Schacht hinzufügen, müssen die Laufwerks- und Schachtnummern übereinstimmen. Wenn beispielsweise Schacht 1 angezeigt wird, müssen Sie Laufwerk 1 hinzufügen. Wenn ein Laufwerk nicht angeschlossen ist, lassen Sie den entsprechenden Schacht leer.
9. Wenn Ihre Client-Maschine angezeigt wird, wählen Sie diese und dann Next (Weiter) aus. Der Client-Computer kann mehrfach angezeigt werden.
10. Wenn die Laufwerke angezeigt werden, wiederholen Sie die Schritte 7 bis 9, um alle Laufwerke den Schächten hinzuzufügen.
11. Wählen Sie auf der Registerkarte Configuration (Konfiguration) die Option Manage devices (Geräte verwalten) aus. Erweitern Sie auf der Seite Manage Devices (Geräte verwalten) den Medienwechsler, um die hinzugefügten Geräte anzuzeigen.

Daten im Quest NetVault Backup auf einem Band sichern

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

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

Archivieren eines Bandes mithilfe von Quest NetVault Backup

Wenn Sie ein Band archivieren, wirft Tape Gateway das Band aus der Bandbibliothek in den Speicherschacht aus. Anschließend exportiert es das Band mithilfe Ihrer Backup-Anwendung, d. h. Quest NetVault Backup, aus dem Steckplatz in das Archiv.

Um ein Band in Quest NetVault Backup zu archivieren

1. Wählen Sie auf der Registerkarte Quest NetVault Backup-Konfiguration Ihren Medienwechsler aus und erweitern Sie ihn, um Ihre Bänder zu sehen.
2. Wählen Sie das Einstellungssymbol für Slots, um den Slots-Browser für den Medienwechsler zu öffnen.
3. Wählen Sie in den Steckplätzen das Band aus, das Sie archivieren möchten, und klicken Sie dann auf Exportieren.

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

Stellen Sie in der Quest NetVault Backup-Software sicher, dass sich das Band nicht mehr im Speichersteckplatz befindet.

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

Daten von einem in Quest NetVault Backup archivierten Band wiederherstellen

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

1. Rufen Sie das archivierte Band aus dem Archiv auf ein Tape Gateway ab. Detaillierte Anweisungen finden Sie unter Abrufen archivierter Bänder.
2. Verwenden Sie die Quest NetVault Backup-Anwendung, um die Daten wiederherzustellen. Dazu erstellen Sie einen Wiederherstellungsordner, wie bei der Wiederherstellung von Daten von physischen Bändern. Anweisungen zum Erstellen eines Wiederherstellungsauftrags finden Sie im Quest NetVault Backup — Administrationshandbuch.

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Sie Ihr Setup mithilfe von Veeam Backup and Replication

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

Themen

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

Konfigurieren von Veeam für das Arbeiten mit VTL-Geräten

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

VTL-Gerätetreiber aktualisieren

Um die Software so zu konfigurieren, dass sie mit den Tape-Gateway-Geräten zusammenarbeitet, aktualisieren Sie die Gerätetreiber für die VTL Geräte um Sie der Veeam Software zur Verfügung zu stellen und ermitteln Sie anschließend die VTL-Geräte. Aktualisieren Sie im Geräte-Manager den Treiber des Medienwechslers. Detaillierte Anweisungen finden Sie unter Aktualisieren des Gerätetreibers für den Medienwechsler.

Erkennen von VTL-Geräten

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

So ermitteln Sie VTL-Geräte

1. Wählen Sie in der Veeam-Software Tape Infrastructure aus. Wenn das Tape Gateway verbunden ist, werden die virtuellen Bänder auf der Registerkarte Backup Infrastructure aufgelistet.
2. Erweitern Sie die Struktur Tape (Band), um die Bandlaufwerke und den Medienwechsler anzuzeigen.
3. Erweitern Sie den Medienwechsler-Baum. Wenn Ihre Bandlaufwerke dem Medienwechsler zugeordnet sind, werden die Laufwerke unter Drives (Laufwerke) angezeigt. Andernfalls werden die Bandbibliothek und die Bandlaufwerke als separate Geräte erscheinen.

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

Importieren eines Bands in Veeam

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

Importieren eines Bands in die Veeam-Software-Bibliothek

1. Öffnen Sie das Kontextmenü (Rechtsklick) für den Medienwechsler und wählen Sie Import (Importieren) aus, um die Bänder in die I/E Steckplätze zu importieren.
2. Öffnen Sie das Kontextmenü (Rechtsklick) für den Medienwechsler und wählen Sie Inventory Library (Inventarbibliothek) aus, um nicht erkannte Bänder zu identifizieren. Wenn Sie

das erste Mal ein neues virtuelles Band in ein Bandlaufwerk laden, wird das Band von der Veeam-Sicherungs-Anwendung nicht erkannt. Um das nicht erkannte Band zu identifizieren, inventarisieren Sie die Bänder in der Bandbibliothek.

Sichern von Daten auf einem Band in Veeam

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

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

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

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

Archivieren eines Bands mithilfe von Veeam

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

Archivieren eines Bands in die Veeam-Bibliothek

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

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

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

Wiederherstellen von Daten von einem in Veeam archivierten Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

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

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec

Sie können Veritas Backup Exec verwenden, um Ihre Daten auf virtuellen Bändern zu sichern, diese Bänder zu archivieren und Ihre Virtual Tape Library(VTL)-Geräte zu verwalten. In diesem Thema finden Sie grundlegende Dokumentation, die für die Durchführung von Sicherungs- und Wiederherstellungsvorgängen mit Backup Exec erforderlich ist.

Ausführlichere Informationen zur Verwendung von Backup Exec, einschließlich der Erstellung sicherer Backups, Software- und Hardwarekompatibilitätslisten und Administratorhandbücher, finden Sie auf der Support-Website von Veritas.

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

Themen

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

Konfigurieren von Speicher in Backup Exec

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

Konfigurieren Sie den Speicher wie folgt:

1. Starten Sie die Backup Exec-Software und klicken Sie links oben in der Symbolleiste auf das gelbe Symbol.
2. Klicken Sie auf Configuration and Settings (Konfiguration und Einstellungen) und anschließend auf Backup Exec Services (Backup Exec-Services), um den Backup Exec Service Manager zu öffnen.
3. Klicken Sie auf Restart All Services (Alle Services neu starten). Backup Exec erkennt nun die VTL-Geräte (also den Medienwechsler und die Bandlaufwerke). Der Neustart kann einige Minuten dauern.

> **Note**
>
> Tape Gateway stellt 10 Bandlaufwerke bereit. Möglicherweise ist in Ihrem Backup-Exec-Lizenzvertrag jedoch festgeschrieben, dass Sie mit Ihrer Sicherungsanwendung

nicht so viele Bandlaufwerke verwenden dürfen. In diesem Fall müssen Sie in der automatisierten Bibliothek (Wechsler) von Backup Exec die entsprechende Zahl von Bandlaufwerken deaktivieren. Es darf nur die laut Ihrem Lizenzvertrag zulässige Anzahl von Bandlaufwerken aktiviert sein. Detaillierte Anweisungen finden Sie unter Deaktivieren eines Bandlaufwerks in Backup Exec .

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

Importieren eines Bands in Backup Exec

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

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

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

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

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

3. Öffnen Sie das Kontextmenü (Rechtsklick) eines leeren Slots und wählen Sie Import (Importieren) und dann Import media now (Medien jetzt importieren) aus. Sie können im Rahmen einer einzigen Importoperation mehrere Schächte auswählen und mehrere Bänder importieren.
4. Wählen Sie im nun angezeigten Fenster Media Request (Medienanforderung) auf View details (Details anzeigen).
5. Wählen Sie im Fenster Action Alert: Media Intervention (Aktionsalarm: Medienintervention) auf Respond OK (Mit OK antworten), um das Medium in den Slot einzufügen.

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

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

Schreiben von Daten auf ein Band in Backup Exec

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

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

Archivieren eines Bands mithilfe von Backup Exec

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

Archivieren Sie Ihr Band wie folgt:

1. Wählen Sie im Menü Storage (Speicher) die Option Slots (Slots) aus, öffnen Sie das Kontextmenü (Rechtsklick) des Slots, aus dem Sie das Band exportieren möchten. Wählen Sie die Option Export media (Medien exportieren) und dann auf Export media now (Medien jetzt exportieren) aus. Sie können im Rahmen einer einzigen Exportoperation mehrere Schächte auswählen und mehrere Bänder exportieren.
2. Klicken Sie im Pop-up-Fenster Media Request auf View details. Klicken Sie anschließend im Fenster Alert: Media Intervention auf Respond OK.

   In der Storage-Gateway-Konsole können Sie den Status des Bands überprüfen, das archiviert wird. Das Hochladen der Daten in AWS kann einige Zeit dauern. Während des Hochladens wird in der VTL des Tape Gateway als Status für das exportierte Band IN TRANSIT TO VTS angezeigt. Wenn die Dateien hochgeladen wurden und die Archivierung gestartet wird, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach dem Archivieren der Daten wird das exportierte Band nicht mehr in der VTL aufgeführt, aber in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert.
3. Wählen Sie Ihr Gateway und anschließend VTL Tape Cartridges (VTL-Bandkartuschen) aus. Stellen Sie sicher, dass das virtuelle Band nicht mehr imGateway aufgelistet wird.
4. Klicken Sie im Navigationsbereich der Storage-Gateway-Konsole auf Bänder. Überprüfen Sie, ob als Status für das Band ARCHIVIERT angezeigt wird.

Wiederherstellen von Daten von einem in Backup Exec archivierten Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

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

Deaktivieren eines Bandlaufwerks in Backup Exec

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

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

Nächster Schritt

Säuberung unnötiger Ressourcen

Testen Sie Ihr Setup mithilfe von Veritas NetBackup

Mit Veritas können Sie Ihre Daten auf virtuellen Bändern sichern, die Bänder archivieren und Ihre Virtual Tape Library (VTL) -Geräte verwalten. NetBackup In diesem Thema finden Sie grundlegende Dokumentation zur Konfiguration der NetBackup Anwendung für ein Tape Gateway und zur Durchführung von Sicherungs- und Wiederherstellungsvorgängen.

Ausführliche Informationen zur Verwendung NetBackup finden Sie auf der Seite Veritas Services and Operations Readiness Tools (SORT) auf der Veritas-Website.

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

Themen

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

Konfiguration von Speichergeräten NetBackup

Nachdem Sie die VTL-Geräte (Virtual Tape Library) mit dem Windows-Client verbunden haben, konfigurieren Sie den NetBackup Veritas-Speicher so, dass er Ihre Geräte erkennt. Weitere

Informationen dazu, wie Sie VTL-Geräte mit einem Windows-Client verbinden können, finden Sie unter Ihre VTL-Geräte anschließen.

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

1. Öffnen Sie die NetBackup Verwaltungskonsole als Administrator.
2. Wählen Sie Configure Storage Devices (Speichergeräte konfigurieren) aus, um den Assistenten für die Gerätekonfiguration zu öffnen.
3. Wählen Sie Weiter. Die NetBackup Anwendung erkennt Ihren Computer als Gerätehost.
4. Wählen Sie in der Spalte Device Hosts (Gerätehosts) Ihren Computer und dann Next (Weiter) aus. Die NetBackup Anwendung durchsucht Ihren Computer nach Geräten und erkennt alle Geräte.
5. Wählen Sie auf der Seite Scanning Hosts (Scanning-Hosts) auf Next (Weiter) und ein zweites Mal auf Next (Weiter). Die NetBackup Anwendung findet alle 10 Bandlaufwerke und den Medienwechsler auf Ihrem Computer.
6. Wählen Sie im Fenster Backup Devices (Sicherungsgeräte) Next (Weiter) aus.
7. Überprüfen Sie im Fenster Drag and Drop Configuration (Drag-and-Drop-Konfiguration), ob Ihr Medienwechsler ausgewählt ist. Wählen Sie dann Next (Weiter) aus.
8. Wählen Sie im nun angezeigten Dialogfeld Yes (Ja) aus, um die Konfiguration auf Ihrem Computer zu speichern. Die NetBackup Anwendung aktualisiert die Gerätekonfiguration.
9. Wenn das Update abgeschlossen ist, wählen Sie Weiter, um die Geräte für die NetBackup Anwendung verfügbar zu machen.
10. Wählen Sie im Fenster Finished! (Fertig!) die Option Finish (Beenden) aus.

Um Ihre Geräte in der NetBackup Anwendung zu verifizieren

1. Erweitern Sie in der NetBackup Verwaltungskonsole den Knoten Medien- und Geräteverwaltung und dann den Knoten Geräte. Wählen Sie Drives (Laufwerke) aus, um alle Bandlaufwerke anzuzeigen.
2. Wählen Sie im Knoten Devices (Geräte) Robots (Roboter) aus, um alle Medienwechsler anzuzeigen. In der NetBackup Anwendung wird der Medienwechsler als Roboter bezeichnet.
3. Öffnen Sie im Bereich All Robots (Alle Roboter) das Kontextmenü (Rechtsklick) für TLD(0) (d. h. Ihren Roboter) und wählen Sie dann Inventory Robot (Roboterinventar) aus.
4. Vergewissern Sie sich im Fenster Robot Inventory, dass in der Kategorie Select robot in der Liste Device Host Ihr Host ausgewählt ist.

5. Überprüfen Sie, ob in der Liste Robot (Roboter) Ihr Roboter ausgewählt ist.
6. Wählen Sie im Fenster Robot Inventory (Roboterinventar) die Option Update volume configuration (Volumekonfiguration aktualisieren), Preview changes (Änderungsvorschau anzeigen), Empty media access port prior to update (Medienzugriffsport vor Aktualisierung leeren) und dann Start (Starten) aus.

   Der Prozess inventarisiert dann Ihren Medienwechsler und Ihre virtuellen Bänder in der NetBackup Enterprise Media Management (EMM) -Datenbank. NetBackup speichert Medieninformationen, Gerätekonfiguration und Bandstatus im EMM.
7. Wählen Sie nach Abschluss der Inventarisierung im Fenster Robot Inventory (Roboterinventar) Yes (Ja) aus. Durch die Wahl von Yes (Ja) an dieser Stelle werden die Konfiguration aktualisiert und die virtuellen Bänder in den Import/Export-Slots zur virtuellen Bandbibliothek verschoben.
8. Schließen Sie das Fenster Robot Inventory (Roboterinventar).
9. Erweitern Sie im Knoten Media (Medien) den Knoten Robots (Roboter) und wählen Sie TLD(0) aus, um alle virtuellen Bänder anzuzeigen, die für Ihren Roboter (Medienwechsler) verfügbar sind.

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

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

Sichern von Daten auf einem Band

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

> **Note**
>
> - Im Rahmen dieser Erste-Schritte-Übung sollten Sie nur eine kleine Menge Daten sichern, da sowohl die Speicherung und die Archivierung der Daten als auch der Datenabruf

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

- Wenn Ihr Tape Gateway während einer laufenden Backup-Aufgabe aus irgendeinem Grund neu gestartet wird, wird die Backup-Aufgabe unterbrochen. Die unterbrochene Backup-Aufgabe wird automatisch wieder aufgenommen, wenn Ihr Gateway den Neustart abgeschlossen hat.

Erstellen Sie wie folgt einen Volume-Pool:

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

1. Starten Sie die NetBackup Verwaltungskonsole.
2. Erweitern Sie den Knoten Media (Medien), öffnen Sie das Kontextmenü (Rechtsklick) für Volume Pool (Volume-Pool) und wählen Sie dann New (Neu) aus. Anschließend wird das Dialogfeld New Volume Pool (Neuer Volume-Pool) angezeigt.
3. Geben Sie in das Feld Name (Name) einen Namen für den Volume-Pool ein.
4. Geben Sie in das Feld Description (Beschreibung) eine Beschreibung für den Volume-Pool ein und wählen Sie dann OK (OK) aus. Der Volume-Pool wird erstellt und der Volume-Pool-Liste hinzugefügt.

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

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

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

   Wenn Sie bereits zuvor einen Robot verbunden haben, hat Ihr Tape-Gateway-Robot möglicherweise einen anderen Namen.
2. Öffnen Sie in der Liste der virtuellen Bänder das Kontextmenü (Rechtsklick) des Bands, das Sie dem Volume-Pool hinzufügen möchten. Wählen Sie Change (Ändern) aus, um das Dialogfeld Change Volumes (Volumes ändern) zu öffnen.
3. Wählen Sie in Volume Pool (Volume-Pool) die Option New pool (Neuer Pool) aus.

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

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

Erstellen Sie wie folgt eine Backup-Richtlinie:

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

1. Wählen Sie Ihren Master-Server aus, um zur NetBackup Veritas-Konsole zurückzukehren.
2. Klicken Sie auf Create a Policy (Richtlinie erstellen), um das Fenster Policy Configuration Wizard (Assistent für die Richtlinienkonfiguration) zu öffnen.
3. Wählen Sie die Option File systems, databases, applications (Dateisysteme, Datenbanken, Anwendungen) aus und klicken Sie auf Next (Weiter).
4. Geben Sie in das Feld Policy Name einen Namen für Ihre Richtlinie ein und vergewissern Sie sich, dass in der Liste Select the policy type die Option MS-Windows ausgewählt ist. Klicken Sie dann auf Next.
5. Wählen Sie im Fenster Client List (Clientliste) die Option Add (Hinzufügen) aus. Geben Sie in der Spalte Name (Name) den Hostnamen Ihres Computers ein und wählen Sie Next (Weiter) aus. Die Richtlinie, die Sie gerade definieren, wird damit auf `localhost` (Ihren Client-Computer) angewendet.
6. Wählen Sie im Fenster Files (Dateien) zunächst Add (Hinzufügen) und anschließend das Ordnersymbol aus.
7. Navigieren Sie im Fenster Browse (Durchsuchen) zum Ordner oder zu den Dateien, den oder die Sie sichern möchten, und wählen Sie OK (OK) aus. Klicken Sie dann auf Next (Weiter).
8. Akzeptieren Sie im Fenster Backup Types (Sicherungstypen) die Standardeinstellungen und wählen Sie dann Next (Weiter) aus.

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

9. Legen Sie im Fenster Frequency and Retention (Häufigkeit und Aufbewahrung) fest, wie häufig die Sicherung ausgeführt werden soll und welche Aufbewahrungsrichtlinie für die Sicherung gelten soll. Für diese Übung können Sie alle Standardeinstellungen akzeptieren und Weiter wählen.
10. Wählen Sie im Fenster Start (Starten) die Option Off hours (Außerhalb der Geschäftszeiten) und dann Next (Weiter) aus. Mit dieser Auswahl legen Sie fest, dass Ihr Ordner nur außerhalb der Geschäftszeiten gesichert werden soll.
11. Wählen Sie im Policy Configuration Wizard (Assistent für Richtlinienkonfiguration) die Option Finish (Beenden) aus.

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

Führen Sie wie folgt eine manuelle Sicherung durch:

1. Erweitern Sie im Navigationsbereich der NetBackup Konsole den Knoten NetBackup Management.
2. Erweitern Sie den Knoten Policies (Richtlinien).
3. Öffnen Sie das Kontextmenü (Rechtsklick) für Ihre Richtlinie und wählen Sie Manual Backup (Manuelle Sicherung) aus.
4. Wählen Sie im Fenster Manual Backup (Manuelle Sicherung) einen Zeitplan, einen Client und dann OK (OK) aus.
5. Wählen Sie im nun angezeigten Dialogfeld Manual Backup Started (Manuelle Sicherung gestartet) OK (OK) aus.
6. Wählen Sie im Navigationsbereich Activity Monitor (Aktivitätsüberwachung) aus, um in der Spalte Job ID (Auftrags-ID) den Status der Sicherung anzuzeigen.

Um den Barcode des virtuellen Bandes zu finden, auf das die Dateidaten während der Sicherung NetBackup geschrieben wurden, schauen Sie im Fenster Auftragsdetails nach, wie im folgenden Verfahren beschrieben. Sie benötigen diesen Barcode für die Anleitung im nächsten Abschnitt, mit der Sie das Band archivieren.

Ermitteln Sie wie folgt den Barcode des Bands:

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

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

Archivieren eines Bands

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

Archivieren Sie wie folgt ein virtuelles Band:

1. Erweitern Sie in der NetBackup Verwaltungskonsole den Knoten Medien- und Geräteverwaltung und erweitern Sie den Knoten Medien.
2. Erweitern Sie Robots (Roboter) und wählen Sie TLD(0) aus.
3. Öffnen Sie das Kontextmenü (Rechtsklick) für das virtuelle Band, das Sie archivieren möchten, und wählen Sie Eject Volume From Robot (Volume aus Roboter auswerfen) aus.
4. Stellen Sie im Fenster Eject Volumes (Volumes auswerfen) sicher, dass der Wert in der Spalte Media ID (Medien-ID) mit der ID des virtuellen Bands übereinstimmt, das Sie auswerfen möchten, und wählen Sie dann Eject (Auswerfen) aus.
5. Wählen Sie im Dialogfeld Yes (Ja) aus.

   Wenn der Auswurfvorgang abgeschlossen ist, zeigt der Status des Bands im Dialogfeld Eject Volumes (Volumes auswerfen) an, dass das Auswerfen erfolgreich war.
6. Wählen Sie Close (Schließen) aus, um das Fenster Eject Volumes (Volumes auswerfen) zu schließen.

7. Überprüfen Sie in der Storage-Gateway-Konsole in der VTL des Gateways den Status des Bands, das Sie archivieren. Das Hochladen der Daten in AWS kann einige Zeit dauern. Während des Hochladens wird in der VTL des Gateways als Status für das ausgeworfene Band IN TRANSIT TO VTS (WIRD ZU VTS ÜBERTRAGEN) angezeigt. Wenn die Archivierung beginnt, wird der Status in ARCHIVING (WIRD ARCHIVIERT) geändert. Nach dem Hochladen der Daten wird das ausgeworfene Band nicht mehr in der VTL aufgeführt, aber in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert.
8. Wählen Sie Ihr Gateway und dann VTL Tape Cartridges (VTL-Bandkartuschen) aus und überprüfen Sie, ob das virtuelle Band nicht mehr im Gateway aufgeführt wird.
9. Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Tapes aus. Überprüfen Sie, ob für das archivierte Band der Status ARCHIVED angezeigt wird.

Wiederherstellen von Daten von einem Band

Zur Wiederherstellung archivierter Daten sind zwei Schritte notwendig.

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

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

Nächster Schritt

Säuberung unnötiger Ressourcen

Wie geht es weiter?

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

Sie können einige der Tape Gateway-Wartungsaufgaben auf dem ausführen AWS Management Console, z. B. die Konfiguration der Bandbreitenbegrenzungen Ihres Gateways und die Verwaltung von Gateway-Softwareupdates. Wenn Ihr Tape Gateway On-Premises bereitgestellt wird, können Sie einige dieser Wartungsaufgaben mit der lokalen Gateway-Konsole ausführen. Hierzu gehört das Routing Ihres Tape Gateway über einen Proxy und das Konfigurieren Ihres Gateways für die Verwendung einer statischen IP-Adresse. Wenn Sie Ihr Gateway als EC2 Amazon-Instance ausführen, können Sie auf der EC2 Amazon-Konsole bestimmte Wartungsaufgaben ausführen, z. B. Amazon EBS-Volumes hinzufügen und entfernen. Weitere Informationen zur Verwaltung Ihres Tape Gateway finden Sie unter Verwaltung Ihres Tape Gateways.

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

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 es ihm zu ermöglichen, Daten an AWS Speicherdienste zu übertragen, ohne über das öffentliche Internet zu kommunizieren. Mit dem Amazon VPC-Service können Sie AWS Ressourcen, einschließlich privater Netzwerkschnittstellen-Endpunkte, in einer benutzerdefinierten Virtual Private Cloud (VPC) starten. Eine VPC gibt Ihnen die Kontrolle über Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways. Weitere Informationen finden Sie VPCs unter Was ist Amazon VPC? im Amazon VPC-Benutzerhandbuch.

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 Connect Sie Ihr Tape Gateway 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 Endpunkt erstellen aus. Der Anfangsstatus des Endpunkts ist pending (ausstehend). Wenn der Endpunkt erstellt wurde, notieren Sie die ID des VPC-Endpunkts, den Sie gerade erstellt haben.
9. Wenn der Endpunkt erstellt wurde, wählen Sie Endpoints (Endpunkte) und dann den neuen VPC-Endpunkt aus.
10. Verwenden Sie auf der Registerkarte Details des ausgewählten Storage-Gateway-Endpunkts unter DNS-Namen den ersten DNS-Namen, der keine Verfügbarkeitszone angibt. Ihr DNS-Name sieht ungefähr wie folgt aus: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

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

Verwaltung Ihres Tape Gateways

Die Verwaltung Ihres Gateways umfasst Aufgaben wie die Konfiguration des Cache-Speichers und des Upload-Pufferspeichers, die Arbeit mit virtuellen und die allgemeine Wartung. Falls Sie noch kein Gateway erstellt haben, lesen Sie Erste Schritte mit AWS Storage Gateway.

Im Folgenden finden Sie Informationen zur Verwaltung Ihrer .

Topics

- Bearbeiten grundlegender Gateway-Informationen- Erfahren Sie, wie Sie die Storage Gateway Gateway-Konsole verwenden, um grundlegende Informationen für ein vorhandenes Gateway zu bearbeiten, darunter den Gateway-Namen, die Zeitzone und die CloudWatch Protokollgruppe.
- Verwalten der automatischen Banderstellung- Erfahren Sie, wie Sie Tape Gateway so konfigurieren, dass neue virtuelle Bänder automatisch erstellt werden, sodass die von Ihnen angegebene Mindestanzahl verfügbarer Bänder beibehalten wird.
- Archivierung virtueller Bänder- Erfahren Sie, wie Sie die Archivierung Ihrer Bänder entweder für die Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive konfigurieren, wenn Sie ein neues Band erstellen.
- Bänder in die Speicherklasse S3 Glacier Deep Archive verschieben- Erfahren Sie, wie Sie Ihre Bänder von S3 Glacier Flexible Retrieval auf S3 Glacier Deep Archive migrieren können, um Daten langfristig und kostengünstig digital aufzubewahren.
- Abrufen archivierter Bänder- Erfahren Sie, wie Sie auf Daten zugreifen können, die auf einem archivierten virtuellen Band gespeichert sind, indem Sie das Band zunächst auf Ihr Tape Gateway abrufen.
- Statistiken zur Bandnutzung anzeigen- Erfahren Sie, wie Sie mit der Storage Gateway Gateway-Konsole die auf einem Band gespeicherte Datenmenge anzeigen können.
- Virtuelle Bänder von Ihrem Tape Gateway löschen- Erfahren Sie, wie Sie mithilfe der Storage Gateway-Konsole virtuelle Bänder von Ihrem Tape Gateway löschen.
- Löschen von benutzerdefinierten Bandpools- Erfahren Sie, wie Sie einen benutzerdefinierten Bandpool mithilfe der Storage Gateway Gateway-Konsole löschen.
- Deaktivieren Ihres Tape Gateways- Erfahren Sie, wie Sie ein Tape Gateway deaktivieren, wenn das Gateway ausgefallen ist und Sie die Bänder vom ausgefallenen Gateway auf ein anderes Gateway wiederherstellen möchten.

- Grundlegendes zum Bandstatus- Erfahren Sie mehr über die verschiedenen Bandstatuswerte, die Storage Gateway meldet, um festzustellen, ob ein Band normal funktioniert oder ob ein Problem vorliegt, das möglicherweise Maßnahmen Ihrerseits erfordert.
- Verschieben Ihrer Daten auf ein neues Gateway- Erfahren Sie, wie Sie Daten zwischen Gateways verschieben können, wenn Ihre Daten- und Leistungsanforderungen steigen oder wenn Sie eine AWS Benachrichtigung zur Migration Ihres Gateways erhalten.

Bearbeiten grundlegender Gateway-Informationen

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

So bearbeiten Sie grundlegende Informationen für ein vorhandenes Gateway

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

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

5. Wählen Sie Gateway-Zeitzone die lokale Zeitzone für den Teil der Welt aus, in dem Sie Ihr Gateway einsetzen möchten.

6. Wählen Sie unter Wählen Sie, wie Sie die Protokollgruppe einrichten möchten, aus, wie Amazon CloudWatch Logs eingerichtet werden soll, um den Zustand Ihres Gateways zu überwachen. Sie können aus den folgenden Optionen 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 der entsprechenden Dropdownliste aus.
   - Protokollierung deaktivieren — Verwenden Sie Amazon CloudWatch Logs nicht zur Überwachung Ihres Gateways.

7. Wenn Sie mit der Änderung der Einstellungen, die Sie ändern möchten, fertig sind, wählen Sie Änderungen speichern.

Verwalten der automatischen Banderstellung

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

So ändern oder löschen Sie die Richtlinie für die automatische Banderstellung

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

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

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

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

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

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

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

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

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

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

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

   Der Status der verfügbaren virtuellen Bänder wird zunächst auf CREATING gesetzt, wenn die virtuellen Bänder erstellt werden. Nach der Erstellung der Bänder wird der Status in AVAILABLE geändert. Weitere Informationen finden Sie unter Grundlegendes zum Bandstatus.

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

Archivierung virtueller Bänder

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

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

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

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

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

Bänder in die Speicherklasse S3 Glacier Deep Archive verschieben

Verschieben Sie Ihre Bänder für die langfristige Datenaufbewahrung und Erhaltung digitaler Daten zu sehr niedrigen Kosten von „S3 Glacier Flexible Retrieval“ zu „S3 Glacier Deep Archive“. „S3 Glacier Deep Archive“ wird für die langfristige Datenaufbewahrung und zur Erhaltung digitaler

Daten verwendet, wobei nur ein- oder zweimal im Jahr auf die Daten zugegriffen wird. Detaillierte Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten.

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

1. Wählen Sie im Navigationsbereich Bandbibliothek > Bänder aus, um Ihre Bänder anzuzeigen. Standardmäßig werden in dieser Liste bis zu 1 000 Bänder gleichzeitig angezeigt, aber die von Ihnen durchgeführten Suchvorgänge gelten für alle Ihre Bänder. Sie können die Suchleiste verwenden, um Bänder zu finden, die bestimmten Kriterien entsprechen, oder um die Liste auf weniger als 1 000 Bänder zu reduzieren. Wenn Ihre Liste 1.000 Bänder oder weniger enthält, können Sie die Bänder anschließend nach verschiedenen Eigenschaften auf- oder absteigend sortieren.
2. Aktivieren Sie die Kontrollkästchen für die Bänder, die Sie in „S3 Glacier Deep Archive“ verschieben möchten. In der Spalte Pool wird der Pool angezeigt, dem jedes Band zugeordnet ist.
3. Klicken Sie auf Pool zuweisen.
4. Überprüfen Sie im Dialogfeld „Band Pool zuweisen“ die Barcodes der Bänder, die Sie verschieben, und wählen Sie Zuweisen aus.

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

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

Abrufen archivierter Bänder

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

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

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

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

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

So rufen Sie ein archiviertes Band in ein Gateway ab

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

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

4. Prüfen Sie im Dialogfeld Retrieve tape (Band abrufen) unter Barcode, dass der Barcode das abzurufende virtuelle Band identifiziert.

5. Wählen Sie für Gateway das Gateway, in das das archivierte Band abgerufen werden soll. Wählen Sie dann Retrieve tape (Band abrufen).

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

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

Statistiken zur Bandnutzung anzeigen

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

So zeigen Sie die gespeicherte Datenmenge auf einem Band an

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

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

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

Virtuelle Bänder von Ihrem Tape Gateway löschen

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

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

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

So löschen Sie ein virtuelles Band

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

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

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

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

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

Löschen von benutzerdefinierten Bandpools

Das folgende Verfahren erklärt, wie Sie einen benutzerdefinierten Bandpool mithilfe der Storage Gateway Gateway-Konsole löschen. Informationen zum programmgesteuerten Ausführen dieser Aktion mithilfe der API finden Sie DeleteTapePoolin der Storage Gateway API-Referenz.

Sie können einen benutzerdefinierten Bandpool nur löschen, wenn sich keine archivierten Bänder im Pool befinden und dem Pool keine Richtlinien für die automatische Banderstellung zugeordnet sind. Informationen dazu, wie Sie Richtlinien für die automatische Banderstellung aus einem Bandpool löschen müssen, finden Sie unter Automatische Banderstellung verwalten.

So löschen Sie einen benutzerdefinierten Bandpool mit der Storage Gateway Gateway-Konsole

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Pools aus, um die verfügbaren Pools anzuzeigen.
3. Wählen Sie einen oder mehrere Bandpools aus, die gelöscht werden sollen.

   Wenn die Bandanzahl für die Bandpools, die Sie löschen möchten, 0 ist und es keine Richtlinien für die automatische Banderstellung gibt, die auf den benutzerdefinierten Bandpool verweisen, können Sie die Pools löschen.
4. Wählen Sie Löschen. Das Bestätigungsdialogfeld wird angezeigt.
5. Vergewissern Sie sich, dass Sie die angegebenen Bandpools löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen aus.

> **Warning**
>
> Dieses Verfahren löscht die ausgewählten Bandpools dauerhaft und kann nicht rückgängig gemacht werden.

Nachdem die Bandpools gelöscht wurden, werden sie aus der Bandbibliothek entfernt.

Deaktivieren Ihres Tape Gateways

Sie deaktivieren ein Tape Gateway wenn das Tape Gateway fehlgeschlagen ist und Sie die Bänder vom fehlgeschlagenen Gateway auf einem anderen Gateway wiederherstellen möchten.

Um die Bänder wiederherzustellen, müssen Sie zunächst das fehlgeschlagene Gateway deaktivieren. Deaktivieren eines Tape Gateway sperrt die virtuellen Bänder in diesem Gateway. Das bedeutet, dass alle Daten, die Sie auf diese Bänder schreiben, nachdem das Gateway deaktiviert wurde, nicht an AWS gesendet werden. Sie können ein Gateway nur über die Storage-Gateway-Konsole deaktivieren, und nur wenn das Gateway nicht mehr mit AWS verbunden ist. Wenn das Gateway mit verbunden ist AWS, können Sie das Tape Gateway nicht deaktivieren.

Sie deaktivieren ein Tape Gateway im Rahmen der Datenwiederherstellung. Weitere Informationen über die Wiederherstellung von Bändern finden Sie unter Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen..

So aktivieren Sie das Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das fehlgeschlagene Gateway.
3. Wählen Sie die Registerkarte Details für das Gateway, um die Meldung zur Deaktivierung des Gateways anzuzeigen.
4. Wählen Sie Wiederherstellungsbänder erstellen.
5. Wählen Sie Gateway deaktivieren.

Grundlegendes zum Bandstatus

Jedes Band verfügt über einen zugeordneten Status, aus dem sich auf einen Blick der Zustand des Bands ersehen lässt. In den meisten Fällen gibt der Status an, dass das Band ordnungsgemäß funktioniert und Sie keine Aktion durchzuführen brauchen. In einigen Fällen gibt der Status ein Problem mit dem Band an, das eventuell eine Aktion Ihrerseits erforderlich macht. Die folgenden Informationen können Sie bei der Entscheidung unterstützen, ob Sie handeln müssen.

Themen

- Grundlegendes zu Bandstatusinformationen in einer VTL
- Bestimmen des Bandstatus in einem Archiv

Grundlegendes zu Bandstatusinformationen in einer VTL

Der Status eines Bands muss AVAILABLE sein, damit Sie auf dem Band lesen oder schreiben können. In der folgenden Tabelle werden mögliche Statuswerte aufgelistet und beschrieben.

Status	Description	Banddaten sind gespeichert auf
WIRD ERSTELLT	Das virtuelle Band wird erstellt. Das Band kann nicht in ein Bandlaufwerk geladen werden, da das Band erstellt wird.	—
VERFÜGBAR	Das virtuelle Band ist erstellt und zum Laden in ein Bandlaufwerk bereit.	Amazon S3
IN TRANSIT TO VTS	Das virtuelle Band wurde ausgeworfen wird für die Archivierung hochgeladen. Zu diesem Zeitpunkt lädt Ihr Tape Gateway Daten auf AWS hoch. Wenn die Menge der hochgeladenen Daten gering ist, wird dieser Status möglicherweise nicht angezeigt. Nach Abschluss des Uploads wechselt der Status zu ARCHIVING.	Amazon S3
ARCHIVING	Das virtuelle Band wird vom Tape Gateway in das von „S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep	Daten werden von Amazon S3 in „S3 Glacier

Status	Description	Banddaten sind gespeichert auf
	Archive“ gestützte Archiv verschoben. Dieser Vorgang findet statt, nachdem der Datenupload abgeschlossen AWS ist.	Flexible Retrieval“ oder „S3 Glacier Deep Archive“ verschoben.
WIRD GELÖSCHT	Das virtuelle Band wird gelöscht.	Daten werden aus Amazon S3 gelöscht
GELÖSCHT	Das virtuelle Band wurde erfolgreich gelöscht.	—
RETRIEVING	Das virtuelle Band wird aus dem Archiv auf Ihr Tape Gateway abgerufen. **Note** Das virtuelle Band kann nur auf ein Tape Gateway abgerufen werden.	Daten werden von „S3 Glacier Flexible Retrieval “ oder „S3 Glacier Deep Archive“ nach Amazon S3 verschoben
RETRIEVED	Das virtuelle Band wurde aus dem Archiv abgerufen. Das abgerufene Band ist schreibgeschützt.	Amazon S3
RECOVERED	Das virtuelle Band wurde wiederhergestellt und ist schreibgeschützt. Wenn aus irgend einem Grund nicht auf Ihr Tape Gateway zugegriffen werden kann, können Sie mit diesem Tape Gateway verknüpfte virtuelle Bänder auf einem anderen Tape Gateway wiederherstellen. Sie müssen das unzugängliche Tape Gateway deaktivie ren, bevor Sie virtuelle Bänder wiederherstellen können.	Amazon S3
IRRECOVERABLE	Das virtuelle Band kann weder gelesen noch beschrieben werden. Dieser Status zeigt einen Fehler in Ihrem Tape Gateway an.	Amazon S3

Bestimmen des Bandstatus in einem Archiv

Sie können das folgende Verfahren verwenden, um den Status eines virtuellen Bands in einem Archiv zu ermitteln.

So bestimmen Sie den Status eines virtuellen Bands

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Tapes (Bänder).
3. Prüfen Sie in der Spalte Status des Bandbibliothek-Rasters den Status des Bands.

   Der Bandstatus wird auch auf der Registerkarte Details jedes virtuellen Bands angezeigt.

Im Folgenden finden Sie eine Beschreibung der möglichen Statuswerte.

Status	Description
ARCHIVED	Das virtuelle Band wurde ausgeworfen und an das Archiv hochgeladen.
RETRIEVING	Das virtuelle Band wird aus dem Archiv abgerufen. **Note** Das virtuelle Band kann nur auf ein Tape Gateway abgerufen werden.
RETRIEVED	Das virtuelle Band wurde aus dem Archiv abgerufen. Das abgerufene Band ist schreibgeschützt.

Weitere Informationen zum Arbeiten mit Bänder und VTL-Geräten finden Sie unter Bänder in Ihrer virtuellen Bandbibliothek verwalten.

Verschieben Ihrer Daten auf ein neues Gateway

Sie können Daten zwischen Gateways verschieben, wenn Ihre Daten- und Leistungsanforderungen steigen oder wenn Sie eine AWS Benachrichtigung zur Migration Ihres Gateways erhalten. Nachfolgend sind einige Gründe für diesen Vorgang ausgeführt:

- Verschieben Sie Ihre Daten auf bessere Hostplattformen oder neuere EC2 Amazon-Instances.
- Aktualisieren der zugrunde liegenden Hardware für Ihren Server

Welche Schritte Sie befolgen müssen, um Ihre Daten auf ein neues Gateway zu verschieben, hängt von Ihrem Gateway-Typ ab.

> **Note**
>
> Daten können nur zwischen den gleichen Gateway-Typen verschoben werden.

Verschieben virtueller Bänder auf ein neues Tape Gateway

So verschieben Sie ein virtuelles Band auf ein neues Tape Gateway

1. Verwenden Sie Ihre Sicherungsanwendung, um alle Ihre Daten auf einem virtuellen Band zu sichern. Warten Sie, bis die Sicherung erfolgreich abgeschlossen ist.
2. Verwenden Sie Ihre Sicherungsanwendung, um das Band auszuwerfen. Das Band wird in einer Amazon-S3-Speicherklasse gespeichert. Ausgeworfene Bänder werden in „S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep Archive“ archiviert und sind schreibgeschützt.

   Bevor Sie fortfahren, vergewissern Sie sich, dass die ausgeworfenen Bänder archiviert wurden:

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

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

   c. Prüfen Sie in der Spalte Status der Liste den Status des Bands.

      Der Bandstatus wird auch auf der Registerkarte Details jedes virtuellen Bands angezeigt.

Weitere Informationen zum Ermitteln des Bandstatus in einem Archiv finden Sie unter Bestimmen des Bandstatus in einem Archiv.

3. Stellen Sie mit Ihrer Sicherungsanwendung sicher, dass keine aktiven Sicherungsaufträge an das vorhandene Tape Gateway gesendet werden, bevor Sie es beenden. Falls aktive Sicherungsaufträge vorhanden sind, warten Sie, bis diese abgeschlossen sind, und werfen Sie die Bänder aus (siehe vorherigen Schritt), bevor Sie das Gateway beenden.
4. Führen Sie die folgenden Schritte aus, um das vorhandene Tape Gateway zu beenden:

   a. Wählen Sie im Navigationsbereich Gateways und anschließend das alte Tape Gateway aus, das Sie beenden möchten. Der Status des Gateways lautet In Ausführung.

   b. Wählen Sie unter Aktionen die Option Gateway anhalten aus. Überprüfen Sie die ID des Gateways im Dialogfeld und wählen Sie dann Gateway anhalten aus.

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

   Weitere Informationen zum Anhalten von Gateways finden Sie unter Starten und Anhalten eines Tape Gateways.
5. Erstellen Sie ein Tape Gateway. Detaillierte Anweisungen finden Sie unter Erstellen von Gateways.
6. Führen Sie die folgenden Schritte aus, um neue Bänder zu erstellen:

   a. Wählen Sie im Navigationsbereich die Registerkarte Gateways aus.

   b. Wählen Sie Bänder erstellen aus, um das Dialogfeld Band erstellen zu öffnen.

   c. Wählen Sie in Gateway (Gateway) einen Gateway aus. Das Band wird für dieses Gateway erstellt.

   d. Wählen Sie unter Number of tapes (Anzahl der Bänder) die Anzahl der Bänder aus, die Sie erstellen möchten. Weitere Informationen zu den Limits für Bänder finden Sie unter AWS Storage Gateway Kontingente.

      Sie können an dieser Stelle auch die automatische Banderstellung einrichten. Weitere Informationen finden Sie unter Automatisches Erstellen von Bändern.

e. Geben Sie unter Capacity (Kapazität) die Größe des virtuellen Bandes ein, das Sie erstellen möchten. Bänder müssen größer als 100 GiB sein. Weitere Informationen zu den Kapazitätslimits finden Sie unter AWS Storage Gateway Kontingente.

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

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

g. Wählen Sie für Pool entweder Glacier Pool oder Deep Archive Pool aus. Dieser Pool stellt die Speicherklasse dar, in der Ihr Band gespeichert wird, wenn es von Ihrer Sicherungssoftware ausgeworfen wird.

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

   Wählen Sie Deep Archive Pool, wenn Sie das Band in „S3 Glacier Deep Archive“ archivieren möchten. Wenn Ihre Sicherungssoftware das Band auswirft, wird es automatisch in „S3 Glacier Deep Archive“ archiviert. „S3 Glacier Deep Archive“ wird für die langfristige Datenaufbewahrung und zur Erhaltung digitaler Daten verwendet, wo nur ein- oder zweimal im Jahr auf die Daten zugegriffen wird. Sie können ein in „S3 Glacier Deep Archive“ archiviertes Band in der Regel innerhalb von 12 Stunden abrufen. Weitere Informationen finden Sie unter Speicherklassen für die Archivierung von Objekten im Benutzerhandbuch für den Amazon Simple Storage Service.

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

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

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

i. Wählen Sie Create tapes (Bänder erstellen) aus.

7. Starten Sie mit Ihrer Sicherungsanwendung einen Sicherungsauftrag und sichern Sie Ihre Daten auf dem neuen Band.

8. (Optional) Wenn Ihr Band archiviert worden ist und Sie darauf vorhandene Daten wiederherstellen müssen, rufen Sie diese auf dem neuen Tape Gateway ab. Das Band befindet sich im schreibgeschützten Modus. Weitere Informationen zum Abrufen archivierter Bänder finden Sie unter Abrufen archivierter Bänder.

> **Note**
>
> Es können Gebühren für ausgehende Daten anfallen.

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

b. Wählen Sie das virtuelle Band aus, das Sie abrufen möchten. Wählen Sie unter Aktionen die Option Band abrufen aus.

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

c. Prüfen Sie im Dialogfeld Retrieve tape (Band abrufen) unter Barcode, dass der Barcode das abzurufende virtuelle Band identifiziert.

d. Wählen Sie für Gateway das neue Tape Gateway aus, in das das archivierte Band abgerufen werden soll. Wählen Sie anschließend Band abrufen aus.

Wenn Sie sich vergewissert haben, dass Ihr neues Tape Gateway ordnungsgemäß funktioniert, können Sie das alte Tape Gateway löschen.

> **Important**
>
> Bevor Sie ein Gateway löschen, stellen Sie sicher, dass derzeit keine Anwendungen in die Volumes dieses Gateways schreiben. Wenn Sie ein Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten.

9. Gehen Sie folgendermaßen vor, um das alte Tape Gateway zu löschen:

> **Warning**
>
> Wenn ein Gateway gelöscht worden ist, gibt es keine Möglichkeit, es wiederherzustellen.

a. Wählen Sie im Navigationsbereich zunächst Gateways und anschließend das Gateway aus, das Sie löschen möchten.

b. Wählen Sie für Aktionen die Option Gateway löschen aus.

Vergewissern Sie sich im daraufhin angezeigten Bestätigungsdialogfeld, dass die angegebene Gateway-ID das alte Tape Gateway bezeichnet, das Sie löschen möchten, geben Sie **`delete`** in das Bestätigungsfeld ein, und wählen Sie dann Löschen.

c. Löschen Sie die VM. Weitere Informationen zum Löschen einer VM finden Sie in der Dokumentation für Ihren Hypervisor.

Überwachen von Storage Gateway

In diesem Abschnitt wird beschrieben, wie Sie ein Storage Gateway mithilfe von Amazon überwachen, einschließlich der Überwachung der mit dem Gateway verknüpften Ressourcen 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, mit Ausnahme von hochauflösenden Alarmen, ohne zusätzliche Kosten. Weitere Informationen zur CloudWatch Preisgestaltung finden Sie unter CloudWatch Amazon-Preise. Weitere Informationen zu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Spezifische Informationen zur Überwachung eines Tape Gateways und der zugehörigen Ressourcen finden Sie unter Monitoring your Tape Gateway.

Themen

- Grundlagen zu Gateway-Metriken
- Überwachen des Upload-Puffers
- Überwachen des Cache-Speichers
- CloudWatch Alarme verstehen
- Empfohlene CloudWatch Alarme für Ihr Gateway erstellen
- Einen benutzerdefinierten CloudWatch Alarm für Ihr Gateway erstellen
- Überwachen von Tape Gateway

Grundlagen zu Gateway-Metriken

Für die Diskussion in diesem Thema definieren wir Gateway-Metriken als Metriken, die sich auf das Gateway beziehen – das heißt, sie messen einen bestimmten Aspekt des Gateways. Da ein Gateway ein oder mehrere Volumes enthält, steht eine Gateway-spezifische Metrik stellvertretend für alle Volumes auf dem Gateway. Die `CloudBytesUploaded`-Metrik stellt beispielsweise die Gesamtanzahl der Bytes dar, die das Gateway im Berichtszeitraum an die Cloud gesendet hat. Diese Metrik enthält die Aktivitäten aller Volumes auf dem Gateway.

Bei der Verwendung von Gateway-Metrikdaten geben Sie die eindeutige Identifikation des Gateways an, für das Sie Metriken anzeigen möchten. Zu diesem Zweck geben Sie die Werte `GatewayId` und `GatewayName` an. Wenn Sie mit einer Metrik für ein Gateway arbeiten möchten, geben Sie die Gateway-Dimension im Metrik-Namespace an, der eine Gateway-spezifische Metrik von einer Volume-spezifischen Metrik unterscheidet. Weitere Informationen finden Sie unter Amazon CloudWatch Metrics verwenden.

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

Metrik	Beschreibung
`AvailabilityNotifications`	Anzahl der vom Gateway generierten Zustandsbenachrichtigungen im Zusammenhang mit der Verfügbarkeit. Verwenden Sie diese Metrik zusammen mit der Statistik `Sum`, um zu beobachten, ob Ereignisse im Zusammenhang mit der Verfügbarkeit im Gateway auftreten. Einzelheiten zu den Ereignissen finden

Metrik	Beschreibung
	Sie in Ihrer konfigurierten CloudWatch Protokollgruppe. Einheit: Zahl
`CacheHitPercent`	Prozentsatz der Lesevorgänge einer Anwendung, die aus dem Cache abgearbeitet wurden. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheit: Prozent
`CachePercentDirty`	Der Gesamtprozentsatz des Gateway-Cache, bis zu AWS dem noch keine Persistenz besteht. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Verwenden Sie diese Metrik zusammen mit der `Sum` Statistik. Idealerweise sollte diese Kennzahl niedrig bleiben. Einheit: Prozent

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

Metrik	Beschreibung	
QueuedWrites	Normalerweise steht dieser Wert für die Anzahl der lokal gespeicherten Byte, die darauf warten, geschrieben zu werden AWS, aber er spiegelt auch den Synchronisationsprozess wider, der zwischen lokalen Daten und Cloud-Daten während des „Bootstrappings“ stattfindet, das bei jedem Neustart eines Gateways stattfindet. Einheit: Byte	
TotalCacheSize	Die Gesamtgröße des Cache in Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheit: Byte	
UploadBufferPercentUsed	Prozentuale Nutzung des Gateway-Upload-Puffers. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Einheit: Prozent	

Metrik	Beschreibung
`UploadBufferUsed`	Gesamtanzahl der im Gateway-Upload-Puffer verwendeten Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen . Einheit: Byte
`UserCpuPercent`	Prozentsatz der CPU-Zeit, die für die Gateway-Verarbeitung aufgewendet wurde, gemittelt über alle Kerne. Einheit: Prozent

Dimensionen für Storage-Gateway-Metriken

Der CloudWatch Namespace für den Storage Gateway Gateway-Dienst lautet`AWS/StorageGateway`. Die Daten werden automatisch in 5-Minuten-Intervallen kostenlos zur Verfügung gestellt.

Dimension	Beschreibung
`GatewayId` , `GatewayName`	Diese Dimensionen filtern die angeforderten Daten nach Gateway-spezifischen Metriken. Sie können ein zu verwenden des Gateway anhand des Werts für `GatewayId` oder `GatewayName` identifizieren. Wenn das Gateways im Zeitraum, für den Sie Metriken anzeigen möchten, einen anderen Namen hatte, verwenden Sie die `GatewayId` . Die Durchsatz- und Latenzdaten eines Gateways basieren auf sämtlichen Volumes für dieses Gateway. Weitere Informati onen zur Verwendung von Gateway-Metriken finden Sie unter Messung der Leistung zwischen Ihrem Gateway und AWS.

Überwachen des Upload-Puffers

Im Folgenden finden Sie Informationen zur Überwachung des Gateway-Upload-Puffers und zum Erstellen eines Alarms, sodass Sie eine Benachrichtigung erhalten, wenn der Puffer einen bestimmten Grenzwert überschreitet. Mit diesem Ansatz können Sie einem Gateway Pufferspeicher hinzufügen, bevor er vollständig belegt ist und Ihre Speicheranwendung die Sicherung auf AWS stoppt.

Sie überwachen den Upload-Puffer in Cached-Volume- und Tape-Gateway-Architekturen auf dieselbe Weise. Weitere Informationen finden Sie unter So funktioniert Tape Gateway.

> **Note**
>
> Die Metriken `WorkingStoragePercentUsed`, `WorkingStorageUsed` und `WorkingStorageFree` stellen den Upload-Puffer für gespeicherte Volumes nur bis zur Freigabe der Cached-Volume-Funktion in Storage Gateway dar. Verwenden Sie jetzt die entsprechenden Upload-Puffer-Metriken `UploadBufferPercentUsed`, `UploadBufferUsed` und `UploadBufferFree`. Diese Metriken gelten für beide Gateway-Architekturen.

Interessierendes Element	Methode zum Messen
Nutzung des Upload-Puffers	Verwenden Sie die Metriken `UploadBufferPercentUsed` , `UploadBufferUsed` und `UploadBufferFree` mit der Statistik `Average`. Verwenden Sie z. B. `UploadBufferUsed` mit der `Average`-Statistik für die Analyse der Speichernutzung über einen Zeitraum.

So messen Sie den verwendeten Prozentsatz des Upload-Puffers.

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Gateway, mit dem Sie arbeiten möchten.
3. Wählen Sie die Metrik `UploadBufferPercentUsed` aus.
4. Wählen Sie einen Wert für Zeitraum aus.

5. Wählen Sie die `Average`-Statistik aus.
6. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

Die resultierende zeitlich sortierte Gruppe von Datenpunkten enthält die prozentuale Nutzung des Upload-Puffers.

Mit dem folgenden Verfahren können Sie mithilfe der CloudWatch Konsole einen Alarm erstellen. Weitere Informationen zu Alarmen und Schwellenwerten finden Sie unter CloudWatch Alarme erstellen im CloudWatch Amazon-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 GatewayName Dimension AWS/StorageGateway: GatewayId aus, und suchen Sie dann das Gateway, mit dem Sie arbeiten möchten.
   b. Wählen Sie die Metrik `UploadBufferPercentUsed` aus. Verwenden Sie die `Average`-Statistik und einen Zeitraum von 5 Minuten.
   c. Klicken Sie auf Weiter.
4. Definieren Sie den Namen, die Beschreibung und den Schwellenwert für den Alarm:
   a. Identifizieren Sie den Alarm auf der Seite Define Alarm (Alarm definieren) des Assistenten zum Erstellen von Alarmen, indem Sie in den Feldern Name und Description (Beschreibung) einen Namen und eine Beschreibung eingeben.
   b. Definieren Sie den Schwellenwert für den Alarm.
   c. Klicken Sie auf Weiter.
5. Konfigurieren Sie eine E-Mail-Aktion für den Alarm:
   a. Wählen Sie auf der Seite Configure Actions (Aktionen konfigurieren) des Assistenten zum Erstellen von Alarmen die Option Alarm für Alarm State (Alarmstatus) aus.
   b. Wählen Sie Choose or create email topic (E-Mail-Thema wählen oder erstellen) für Topic (Thema) aus.

Das Erstellen eines E-Mail-Themas bedeutet, dass Sie ein Amazon-SNS-Thema einrichten. Weitere Informationen zu Amazon SNS finden Sie unter Amazon SNS einrichten im CloudWatch Amazon-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.

   b. Bestätigen Sie Ihr Abonnement, indem Sie auf den Link in der E-Mail klicken.

      Eine Abonnement-Bestätigung wird angezeigt.

Überwachen des Cache-Speichers

Im Folgenden finden Sie Informationen zur Überwachung des Gateway-Cache-Speichers und zum Erstellen eines Alarms, sodass Sie eine Benachrichtigung erhalten, wenn Parameter des Caches bestimmte Schwellenwerte überschreiten. Durch diesen Alarm werden Sie benachrichtigt, wenn Sie einem Gateway Cache-Speicher hinzufügen sollten.

Cache-Speicher kann nur in der Cached-Volumes-Architektur überwacht werden. Weitere Informationen finden Sie unter So funktioniert Tape Gateway.

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

So messen Sie den Prozentsatz eines Caches mit geänderten Daten für ein Gateway und alle zugehörigen Volumes

1. Öffnen Sie die Konsole unter CloudWatch . 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.

CloudWatch Alarme verstehen

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

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

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

- Hohe E/A-Wartezeit: `IoWaitpercent` >= 20 für 3 Datenpunkte in 15 Minuten
- Cache-Prozent nicht korrekt: `CachePercentDirty` > 80 für 4 Datenpunkte innerhalb von 20 Minuten
- Zustandsbenachrichtigungen: `HealthNotifications` >= 1 für 1 Datenpunkt innerhalb von 5 Minuten Stellen Sie bei der Konfiguration dieses Alarms Fehlende Datenbehandlung auf notBreaching ein.

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

Für Gateways auf VMware Hostplattformen mit aktiviertem HA-Modus empfehlen wir außerdem 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 Einen benutzerdefinierten CloudWatch Alarm für Ihr Gateway erstellen.
Nicht verfügbar	Der Status des Alarms ist unbekannt. Wählen Sie Nicht verfügbar aus, um Fehlerinformationen auf der Registerkarte Überwachung anzuzeigen.

Empfohlene CloudWatch Alarme für Ihr Gateway erstellen

Wenn Sie mit der Storage Gateway-Konsole ein neues Gateway erstellen, können Sie festlegen, dass alle empfohlenen CloudWatch Alarme bei der Ersteinrichtung automatisch erstellt werden. Weitere Informationen finden Sie unter Konfigurieren von Tape Gateway . Wenn Sie empfohlene CloudWatch Alarme für ein vorhandenes Gateway hinzufügen oder aktualisieren möchten, gehen Sie wie folgt vor.

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

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

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

2. Wählen Sie im Navigationsbereich Gateways und anschließend 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.

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

Einen benutzerdefinierten CloudWatch Alarm für Ihr Gateway erstellen

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

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

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

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

Informationen zum Erstellen eines statischen Schwellenwerts finden Sie unter Erstellen eines CloudWatch Alarms auf der Grundlage eines statischen Schwellenwerts im CloudWatch Amazon-Benutzerhandbuch.

- Anomalieerkennungsalarm: Anomalieerkennung wertet Metrikdaten aus der Vergangenheit aus und erstellt ein Modell der erwarteten Werte. Sie legen einen Wert für den Schwellenwert für die Erkennung von Anomalien fest und CloudWatch verwenden diesen Schwellenwert zusammen mit dem Modell, um den „normalen“ Wertebereich für die Metrik zu bestimmen. Ein höherer Wert für den Schwellenwert erzeugt ein breiteres Band „normaler“ Werte. Sie können bestimmen, ob der Alarm ausgelöst werden soll, wenn der Metrikwert über der Bandbreite erwarteter Werte liegt, wenn er darunter liegt oder wenn er die Bandbreite über- oder unterschreitet.

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

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

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

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

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

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

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

- Wählen Sie im Navigationsbereich zunächst Gateways, dann das Gateway, für das Sie Alarme anzeigen möchten, und schließlich die Registerkarte Überwachung aus.

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

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

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

Überwachen von Tape Gateway

In den Themen dieses Abschnitts werden Verfahren und grundlegende Informationen zur Überwachung Ihres Tape Gateways beschrieben. Sie können die virtuellen Bänder, den Cache-Speicher und den Upload-Puffer überwachen, die Ihrem Tape Gateway zugeordnet sind. Sie verwenden den AWS Management Console , um Messwerte für Ihr Tape Gateway anzuzeigen. Mit Metriken können Sie den Zustand von Tape Gateway verfolgen und Alarme festlegen, sodass Sie benachrichtigt werden, wenn für eine oder mehrere Metriken ein festgelegter Schwellenwert überschritten wird.

Sie können Amazon CloudWatch Logs verwenden, um Informationen über den Zustand Ihres Tape Gateways und verwandter Ressourcen zu erhalten. Sie können die Protokolle verwenden, um Ihr Gateway auf auftretende Fehler zu überwachen. Darüber hinaus können Sie CloudWatch Amazon-Abonnementfilter verwenden, um die Verarbeitung der Protokollinformationen in Echtzeit zu automatisieren.

Storage Gateway stellt CloudWatch Metriken ohne zusätzliche Kosten bereit. Storage-Gateway-Metriken werden für einen Zeitraum von zwei Wochen aufgezeichnet. Mithilfe dieser Metriken können Sie auf Verlaufsinformationen zugreifen und sich einen besseren Überblick über die Leistung von

Tape Gateway und der virtuellen Bänder verschaffen. Ausführliche Informationen dazu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Datendurchsatz, Datenlatenz und Operationen pro Sekunde sind Messwerte, anhand derer Sie die Leistung Ihrer Speicheranwendungen mit Tape Gateway nachvollziehen können. Wenn Sie die richtige Aggregationsstatistik verwenden, können diese Werte mit den Storage-Gateway-Metriken gemessen werden, die für Sie bereitgestellt werden.

Themen

- Abrufen von Tape Gateway-Integritätsprotokollen mit CloudWatch Protokollgruppen
- Amazon CloudWatch Metrics verwenden
- Metriken für virtuelle Bänder verstehen
- Messung der Leistung zwischen Ihrem Tape Gateway und AWS

Abrufen von Tape Gateway-Integritätsprotokollen mit CloudWatch Protokollgruppen

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

Nehmen wir zum Beispiel an, dass Ihr Gateway in einem mit VMware HA aktivierten Cluster bereitgestellt wird und Sie über etwaige Fehler informiert sein müssen. Sie können eine CloudWatch Protokollgruppe so konfigurieren, dass Ihr Gateway überwacht wird und Sie benachrichtigt 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 zur Konfiguration einer CloudWatch Protokollgruppe bei der Aktivierung eines Gateways finden Sie unter Konfiguration Ihres Tape-Gateways. Allgemeine Informationen zu CloudWatch Protokollgruppen finden Sie unter Working with Log Groups and Log Streams im CloudWatch Amazon-Benutzerhandbuch.

Weitere Informationen zum Beheben von Fehlern dieser Art finden Sie unter Beheben von Problemen mit virtuellen Bändern.

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

So konfigurieren Sie eine CloudWatch Protokollgruppe für die Zusammenarbeit mit Ihrem File Gateway

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie die CloudWatch Protokollgruppe konfigurieren möchten.
3. Wählen Sie für Aktionen die Option Gateway-Informationen bearbeiten aus, oder wählen Sie auf der Registerkarte Details unter Integritätsprotokolle und Nicht aktiviert die Option Protokollgruppe konfigurieren aus, um das CustomerGatewayNameDialogfeld Bearbeiten zu öffnen.
4. Wählen Sie für Gateway-Zustandsprotokollgruppe eine der folgenden Optionen aus:

   - Deaktivieren Sie die Protokollierung, wenn Sie Ihr Gateway nicht mithilfe von CloudWatch Protokollgruppen überwachen möchten.
   - Erstellen Sie eine neue Protokollgruppe, um eine neue CloudWatch Protokollgruppe zu erstellen.
   - Verwenden Sie eine vorhandene Protokollgruppe, um eine bereits vorhandene CloudWatch Protokollgruppe zu verwenden.

     Wählen Sie eine Protokollgruppe aus der Liste der vorhandenen Protokollgruppen aus.
5. Wählen Sie Änderungen speichern aus.
6. Gehen Sie wie folgt vor, um die Zustandsprotokolle für Ihr Gateway anzuzeigen:

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

Im Folgenden finden Sie ein Beispiel für eine Tape Gateway-Ereignismeldung, die an gesendet wird CloudWatch. In diesem Beispiel wird eine `TapeStatusTransition`-Meldung angezeigt.

```
{
```

```
    "severity": "INFO",
    "source": "FZTT16FCF5",
    "type": "TapeStatusTransition",
    "gateway": "sgw-C51DFEAC",
    "timestamp": "1581553463831",
    "newStatus": "RETRIEVED"
    }
```

Amazon CloudWatch Metrics verwenden

Sie können Überwachungsdaten für Ihr Tape Gateway entweder mithilfe der API AWS Management Console oder der CloudWatch API abrufen. Die Konsole zeigt eine Reihe von Graphen an, die auf den unformatierten Daten aus der CloudWatch -API basieren. Die CloudWatch API kann auch über eines der Amazon AWS Software Development Kits (SDKs) oder die Amazon CloudWatch API-Tools verwendet werden. Je nach Anforderungen können Sie entweder die in der Konsole angezeigten oder die mit der API aufgerufenen Graphen verwenden.

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

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

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

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

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

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

Metriken für virtuelle Bänder verstehen

Im Folgenden finden Sie Informationen über die Storage-Gateway-Metriken, die virtuelle Bänder betreffen. Jedem Band ist eine Reihe von Metriken zugeordnet.

Einige bandspezifische Metriken können denselben Namen wie bestimmte Gateway-spezifische Metriken haben. Diese Metriken stellen die gleichen Messungsarten dar, beziehen sich jedoch auf ein Band anstatt auf ein Gateway. Geben Sie vor Beginn der Arbeit an, ob Sie mit einer Gateway-Metrik oder einer Bandmetrik arbeiten möchten. Geben Sie beim Arbeiten mit Bandmetriken die Band-ID für das Band an, für das Sie Metriken anzeigen möchten. Weitere Informationen finden Sie unter Amazon CloudWatch Metrics verwenden.

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

Die folgende Tabelle enthält die Storage-Gateway-Metriken, die Sie zum Abrufen von Informationen über Ihre Bänder verwenden können.

Metrik	Beschreibung
`CachePercentDirty`	Der Anteil des Bands am Gesamtprozentsatz des Gateway-Caches, der nicht dauerhaft in AWS gespeichert wird. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Verwenden Sie die Metrik `CachePercentDirty` des Gateways, um den Gesamtprozentsatz des Gateway-Caches anzuzeigen, der nicht dauerhaft in AWS gespeichert wird. Weitere Informationen finden Sie unter Grundlagen zu Gateway-Metriken. Einheiten: Prozent
`CloudTraffic`	Die Anzahl der hochgeladenen und von der Cloud auf das Band heruntergeladenen Bytes. Einheiten: Byte
`IoWaitPercent`	Der Prozentsatz der zugewiesenen IoWait Einheiten, die derzeit vom Band verwendet werden. Einheiten: Prozent
`HealthNotification`	Die Anzahl der vom Band gesendeten Zustandsbenachrichtigungen.

Metrik	Beschreibung
	Einheiten: Anzahl
`MemUsedBytes`	Der Prozentsatz des zugewiesenen Speichers, der gegenwärtig vom Band verwendet wird. Einheiten: Byte
`MemTotalBytes`	Der Prozentsatz des Gesamtspeichers, der gegenwärtig vom Band verwendet wird. Einheiten: Byte
`ReadBytes`	Die Gesamtzahl in Byte, die in Ihren On-Premises-Anwendungen im Berichtszeitraum für eine Dateifreigabe gelesen wurde. Verwenden Sie diese Metrik mit der `Sum`-Statistik, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die IOPS-Werte zu messen. Einheiten: Byte
`UserCpuPercent`	Der Prozentsatz der dem Benutzer zugewiesenen CPU-Datenverarbeitungseinheiten, die gegenwärtig vom Band verwendet werden. Einheiten: Prozent

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

Messung der Leistung zwischen Ihrem Tape Gateway und AWS

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

Eine Statistik ist eine Aggregation einer Metrik über einen bestimmten Zeitraum. Wenn Sie die Werte einer Metrik in anzeigen CloudWatch, verwenden Sie die `Average` Statistik für die Datenlatenz (Millisekunden) und die `Samples` Statistik für Eingabe-/Ausgabeoperationen pro Sekunde (IOPS). Weitere Informationen finden Sie unter Statistiken im CloudWatch Amazon-Benutzerhandbuch.

In der folgenden Tabelle werden die Metriken und die entsprechenden Statistiken zusammengefasst, mit denen Sie Durchsatz, Latenz und IOPS zwischen Ihrem Tape Gateway und AWS messen können.

Interessierendes Element	Methode zum Messen
Latency	Verwenden Sie die Metriken `ReadTime` und `WriteTime` mit der Statistik `Average` CloudWatch . Beispiel: Der `Average`-Wert der `ReadTime`-Metrik gibt die Latenz pro Operation über den Stichprobenzeitraum an.
Durchsatz bis AWS	Verwenden Sie die `CloudBytesUploaded` Metriken `CloudBytesDownloaded` und zusammen mit der `Sum` CloudWatch Statistik.

Interessierendes Element	Methode zum Messen
	Beispiel: Der `Sum` Wert der `CloudBytesDownloaded` Metrik über einen Probenzeitraum von 5 Minuten geteilt durch 300 Sekunden gibt Ihnen den Durchsatz vom Tape Gateway AWS zum Tape Gateway als Rate in Byte pro Sekunde.
Latenz der Daten bis AWS	Verwenden Sie die `CloudDownloadLatency` -Metrik mit der `Average`-Statistik. Beispiel: Die `Average`-Statistik der `CloudDownloadLatency` -Metrik gibt die Latenz pro Operation an.

Zur Messung des Upload-Datendurchsatzes von einem Tape Gateway zu AWS

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Registerkarte Metriken aus.
3. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudBytesUploaded` aus.
5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die `Sum`-Statistik aus.
7. Wählen Sie für Zeitraum einen Wert von 5 Minuten oder mehr.
8. Dividieren Sie in der resultierenden zeitlich sortierten Gruppe von Datenpunkten jeden Datenpunkt durch den Zeitraum (in Sekunden), um den Durchsatz in diesem Stichprobenzeitraum zu erhalten. Wenn der Durchsatz vom Tape Gateway zum Beispiel 555.544.576 Byte für einen bestimmten Datenpunkt AWS beträgt und der Zeitraum 300 Sekunden beträgt, dann würde der ungefähre Durchsatz 1,85 Megabyte pro Sekunde betragen.

Um die Datenlatenz von einem Tape Gateway zu messen AWS

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie die Registerkarte Metriken aus.
3. Wählen Sie die GatewayMetrics Dimension StorageGateway: und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudDownloadLatency` aus.

5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die `Average`-Statistik aus.
7. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

Die resultierende zeitlich sortierte Gruppe von Datenpunkten enthält die Latenz in Millisekunden.

Um einen Alarm für den oberen Schwellenwert für den Durchsatz eines Tape Gateways auf einzustellen AWS

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Alarm erstellen, um den Assistenten zum Erstellen von Alarmen zu starten.
3. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudBytesUploaded` aus.
5. Definieren Sie den Alarm durch Festlegen des Alarmstatus, wenn die `CloudBytesUploaded`-Metrik für eine bestimmte Zeit größer als oder gleich einem angegebenen Wert ist. Sie können beispielsweise einen Alarmstatus festlegen, wenn die `CloudBytesUploaded`-Metrik für 60 Minuten größer als 10 MB ist.
6. Konfigurieren Sie die auszuführenden Aktionen für den Alarmstatus. Sie können beispielsweise eine E-Mail-Benachrichtigung an sich selbst senden lassen.
7. Wählen Sie Alarm erstellen.

Um einen Alarm für den oberen Schwellenwert für das Lesen von Daten einzustellen AWS

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Alarm erstellen, um den Assistenten zum Erstellen von Alarmen zu starten.
3. Wählen Sie die Dimension StorageGateway: Gateway Metrics und suchen Sie das Tape Gateway, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudDownloadLatency` aus.
5. Definieren Sie den Alarm durch Festlegen des Alarmstatus, wenn die `CloudDownloadLatency`-Metrik für eine bestimmte Zeit größer als oder gleich einem angegebenen Wert ist. Sie können beispielsweise einen Alarmstatus definieren, wenn `CloudDownloadLatency` für mehr als 2 Stunden größer als 60.000 Millisekunden ist.

6. Konfigurieren Sie die auszuführenden Aktionen für den Alarmstatus. Sie können beispielsweise eine E-Mail-Benachrichtigung an sich selbst senden lassen.
7. Wählen Sie Alarm erstellen.

Warten eines Gateways

Die Wartung Ihres Tape Gateway umfasst Aufgaben wie die Dimensionierung und Konfiguration lokaler Festplatten für den Cache-Speicher und Upload-Pufferspeicher, die Verwaltung von Updates und die Festlegung eines Aktualisierungszeitplans, die Verwaltung der Bandbreitennutzung sowie das Herunterfahren oder Löschen Ihres Gateways und der zugehörigen Ressourcen, falls erforderlich. Diese Aufgaben sind für alle Gateway-Typen gleich. Falls Sie noch kein Gateway erstellt haben, lesen Sie Erstellen Sie Ihr Gateway.

Topics

- Verwaltung von lokalen Festplatten für Ihr Storage Gateway- Erfahren Sie, wie Sie die Anforderungen an die Festplattengröße einschätzen, Cache-Kapazität hinzufügen und die lokalen Festplatten verwalten, die Sie Ihrem Tape Gateway für Pufferung und Speicherung zuweisen.
- Verwaltung der Bandbreite für Ihr Tape Gateway- Erfahren Sie, wie Sie den Upload-Durchsatz von Ihrem Gateway begrenzen können AWS , um die vom Gateway verwendete Netzwerkbandbreite zu kontrollieren.
- Verwaltung von Gateway-Updates- Erfahren Sie, wie Sie Wartungsupdates ein- oder ausschalten und den Zeitplan für das Wartungsfenster für Ihr Tape Gateway ändern.
- Herunterfahren der Gateway-VM- Erfahren Sie, was zu tun ist, wenn Sie Ihre virtuelle Gateway-Maschine zu Wartungszwecken herunterfahren oder neu starten müssen, z. B. wenn Sie einen Patch auf Ihren Hypervisor anwenden.
- Löschen Ihres Gateways und Entfernen der zugehörigen Ressourcen- Erfahren Sie, wie Sie Ihr Gateway mithilfe der AWS Storage Gateway Konsole löschen und die zugehörigen Ressourcen bereinigen, um zu vermeiden, dass für deren weitere Nutzung Gebühren anfallen.

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. Auf EC2 Amazon-Instances erstellte Gateways verwenden Amazon EBS-Volumes als lokale Festplatten.

Themen

- Bestimmen der Größe des lokalen Festplattenspeichers
- 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 Speicherlösung, die Sie bereitstellen, benötigt das Gateway den folgenden zusätzlichen Speicher:

- Tape Gateways benötigen mindestens zwei Festplatten. Ein für die Verwendung als Cache, und eine als Upload-Puffer.

In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt. Nach dem Einrichten des Gateways können Sie entsprechend der steigenden Auslastung weiteren lokalen Speicher zuweisen.

Lokaler Speicher	Beschreibung
Upload-Puffer	Der Upload-Puffer stellt einen Staging-Bereich für die Daten bereit, bevor das Gateway die Daten an Amazon S3 hochlädt. Ihr Gateway lädt diese Pufferdaten über eine verschlüsselte Secure Sockets Layer (SSL)-Verbindung an AWS hoch.
Cache-Speicher	Der Cache-Speicher fungiert als dauerhafter On-Premises-Speicher für Daten mit ausstehen dem Upload an Amazon S3 aus dem Upload-Puffer. Wenn Ihre Anwendung einen E/A-Vorgang auf einem Volume oder Band ausführt, speichert das Gateway die Daten im Cache-Speicher, um einen Zugriff mit geringer Latenz zu ermöglich en. Wenn die Anwendung Daten von einem Volume oder Band

Lokaler Speicher	Beschreibung	
	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. Die zugrunde liegenden physischen Speicherressourcen werden als Datenspeicher in dargestellt VMware. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-Dateien. Wenn Sie eine lokale Festplatte bereitstellen (z. B. zur Verwendung als Cache-Speicher 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 es sich bei dem Backup um eine weniger leistungsstarke RAID-Konfiguration handelt, wie z. RAID1

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**
>
> Im Fall von Tape Gateways können die Anwendungen, wenn der Upload-Puffer seine Kapazität erreicht hat, weiter Daten aus Ihren Speicher-Volumes lesen und in diese Volumes schreiben. Das Tape Gateway schreibt jedoch keine Ihrer Volume-Daten in seinen Upload-Puffer und lädt auch keine dieser Daten hoch, AWS bis Storage Gateway die lokal gespeicherten Daten mit der Kopie der darin AWS gespeicherten Daten synchronisiert. Diese Synchronisation erfolgt, wenn die Volumes sich im Status BOOTSTRAPPING befinden.

Zur Schätzung der Menge des zuzuordnenden Upload-Puffers können Sie die erwarteten eingehenden und ausgehenden Datenraten bestimmen und in der folgenden Formel verwenden.

Rate der eingehenden Daten

Diese Rate bezieht sich auf den Anwendungsdurchsatz, die Rate, zu der die lokalen Anwendungen Daten in einem bestimmten Zeitraum an das Gateway schreiben.

Rate der ausgehenden Daten

Diese Rate bezieht sich auf die Netzwerkdurchsatz, die Rate, mit der das Gateway Daten an AWS hochladen kann. Diese Rate hängt von Ihrer Netzwerkgeschwindigkeit und der Auslastung sowie davon ab, ob Sie die Bandbreitendrosselung aktiviert haben. Diese Rate sollte unter Berücksichtigung der Komprimierung angepasst werden. Beim Hochladen von Daten in verwendet AWS das Gateway soweit möglich Datenkomprimierung. Wenn die Anwendungsdaten nur aus Text bestehen, können Sie eine effektive Komprimierungsrate von etwa 2:1 erhalten. Wenn Sie jedoch Videos schreiben, kann das Gateway möglicherweise gar keine Datenkomprimierung erzielen und benötigt mehr Upload-Puffer für das Gateway.

Es wird dringend empfohlen, dass Sie mindestens 150 GiB Upload-Pufferspeicher zuweisen, wenn einer der folgenden Punkte zutrifft:

- Ihre eingehende Rate ist höher als die ausgehende Rate.
- Die Formel gibt einen Wert kleiner als 150 GiB zurück.

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

Beispiel: Ihre Geschäftsanwendungen schreiben Textdaten mit einer Rate von 40 MB pro Sekunde während 12 Stunden täglich an das Gateway und der Netzwerkdurchsatz beträgt 12 MB pro Sekunde. Bei einem Komprimierungsfaktor von 2:1 für die Textdaten müssten Sie etwa 690 GiB Speicherplatz für den Upload-Puffer zuweisen.

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

Sie können diese Schätzung auch anfangs zur Bestimmung der Festplattengröße verwenden, die Sie dem Gateway als Upload-Pufferspeicherplatz zuweisen. Mithilfe der Storage-Gateway-Konsole können Sie nach Bedarf weiteren Upload-Pufferspeicherplatz hinzufügen. Außerdem können Sie die CloudWatch Betriebsmetriken von Amazon verwenden, um die Nutzung des Upload-Puffers zu überwachen und zusätzliche Speicheranforderungen zu ermitteln. Weitere Informationen zu Metriken und dem Festlegen von Alarmen finden Sie unter Überwachen des Upload-Puffers.

Bestimmen der Größe des zuzuordnenden Cache-Speichers

Ihr Gateway nutzt seinen Cache-Speicher, um Zugriff mit niedriger Latenz auf Daten bereitzustellen, auf die kürzlich zugegriffen wurde. Der Cache-Speicher fungiert als dauerhafter On-Premises-Speicher für Daten mit ausstehendem Upload an Amazon S3 aus dem Upload-Puffer. Normalerweise sollte die Größe des Cache-Speicher das 1,1-fache der Upload-Puffergröße betragen. Weitere Informationen dazu, wie Sie Ihre Cache-Speichergröße abschätzen können, finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.

Sie können anfänglich diese Schätzung für die Bereitstellung von Festplatten für den Cache-Speicher verwenden. Anschließend können Sie die CloudWatch Betriebsmetriken von Amazon verwenden, um die Cache-Speichernutzung zu überwachen und bei Bedarf mehr Speicherplatz über die Konsole bereitzustellen. Weitere Informationen zur Verwendung der Metriken und dem Einrichten von Alarmen finden Sie unter 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 der EC2 Amazon-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 Ihrer EC2 Amazon-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 EC2 Amazon-Instance finden Sie unter Amazon EBS-Volumes im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances. In den folgenden Schritten konfigurieren Sie diesen Datenträger als Upload-Puffer oder Cache-Speicher.
2. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
3. Wählen Sie im Navigationsbereich Gateways aus.
4. Suchen Sie nach Ihrem Gateway und wählen Sie es aus der Liste aus.
5. Wählen Sie im Menü Aktionen die Option 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 BUFFER oder CACHE STORAGE aus.
7. Wählen Sie Änderungen speichern aus, um die Konfigurationseinstellungen zu speichern.

Verwaltung der Bandbreite für Ihr Tape Gateway

Sie können den Upload-Durchsatz vom Gateway zu oder den Download-Durchsatz von AWS zu Ihrem Gateway begrenzen (AWS 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 mithilfe der AWS Management Console oder programmgesteuert mit der Storage Gateway Gateway-API (siehe UpdateBandwidthRateLimit) oder einem AWS Software Development Kit (SDK) angeben. Durch die programmgesteuerte Drosselung der Bandbreite können Sie die Limits im Laufe des Tages automatisch ändern, z. B. durch die Planung von Aufgaben zum Ändern der Bandbreite.

Sie können auch eine zeitplanbasierte Bandbreitendrosselung für Ihr Gateway definieren. Sie planen die Bandbreitendrosselung, indem Sie ein oder mehrere Intervalle definieren. bandwidth-rate-limit Weitere Informationen finden Sie unter Zeitplanbasierte Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole.

Die Konfiguration einer einzigen Einstellung für die Bandbreitendrosselung entspricht funktionell der Definition eines Zeitplans mit einem einzigen bandwidth-rate-limit Intervall für „Jeden Tag“ 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. Bandbreitenbegrenzungen 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
- Aktualisierung der Gateway-Bandbreitenbegrenzungen mithilfe der AWS SDK für Java
- Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem AWS SDK für .NET
- Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem 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 Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im linken Navigationsbereich erst Gateways und anschließend das Gateway aus, das Sie verwalten möchten.
3. Wählen Sie für Aktionen die Option Bandbreitenraten-Limit bearbeiten aus.
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 Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im linken Navigationsbereich erst Gateways und anschließend das Gateway aus, das Sie verwalten möchten.
3. Wählen Sie für Aktionen die Option Bandbreitenraten-Limit bearbeiten aus.

   Der bandwidth-rate-limit Zeitplan des Gateways wird im Dialogfeld Zeitplan für Bandbreitenratenbegrenzung bearbeiten angezeigt. Standardmäßig ist ein neuer bandwidth-rate-limit Gateway-Zeitplan leer.
4. Wählen Sie im Dialogfeld Zeitplan für Bandbreitenratenbegrenzung bearbeiten die Option Neues Element hinzufügen aus, um ein neues bandwidth-rate-limit Intervall hinzuzufügen. Geben Sie für jedes bandwidth-rate-limit Intervall die folgenden Informationen 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 am Anfang 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 geänderte Werte für die Intervallparameter eingeben.

Um Ihre bandwidth-rate-limit Intervalle zu entfernen, können Sie rechts neben dem zu löschenden Intervall die Option Entfernen auswählen.

Wenn Sie Ihre Änderungen abgeschlossen haben, wählen Sie Speichern aus.

5. Fügen Sie weitere bandwidth-rate-limit Intervalle hinzu, indem Sie „Neues Element hinzufügen“ wählen und den Tag, die Start- und Endzeit sowie die Beschränkungen für die Download- und Upload-Rate eingeben.

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

6. 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 Beschränkungen der Download- und Upload-Raten im Bereich „Details“ für das Gateway sehen.

Aktualisierung der Gateway-Bandbreitenbegrenzungen mithilfe der AWS SDK für 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 für Java aktualisieren. Wenn Sie den Beispielcode verwenden möchten, sollten Sie mit der Ausführung einer Java-Konsolenanwendung vertraut sein. Weitere Informationen finden Sie unter Erste Schritte im AWS SDK für Java -Entwicklerhandbuch.

Example : Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem AWS SDK für 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 Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;
```

```
public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

    // Rates
    static long uploadRate = 51200;  // Bits per second, minimum 51200
    static long downloadRate = 102400;   // Bits per second, minimum 102400

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

        // Create a Storage Gateway client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

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

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
 sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
 returnGatewayARN);
```

```
            System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
 second");
            System.out.println("Download bandwidth limit = " + downloadRate + " bits
 per second");
        }
        catch (AmazonClientException ex)
        {
            System.err.println("Error updating gateway bandwith.\n" + ex.toString());
        }
    }
}
```

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

Example : Aktualisierung der Gateway-Bandbreitenbegrenzungen mithilfe der AWS SDK für .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 Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

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

namespace AWSStorageGateway
{
    class UpdateBandwidthExample
```

```
    {
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

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

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

        // Rates
        static long uploadRate = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

        public static void Main(string[] args)
        {
            // Create a Storage Gateway client
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = serviceURL;
            sgClient = new AmazonStorageGatewayClient(sgConfig);

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

            Console.WriteLine("\nTo continue, press Enter.");
            Console.Read();
        }

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
```

```
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
 second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

Aktualisierung der Gateway-Bandbreitenbegrenzungen mit dem 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 für PowerShell -Benutzerhandbuch.

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

Das folgende PowerShell Skriptbeispiel aktualisiert die Bandbreitenbegrenzungen eines Gateways. Um dieses Beispielskript 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)
```

Verwaltung von Gateway-Updates

Storage Gateway besteht aus einer Komponente für verwaltete Cloud-Services und einer Gateway-Appliance-Komponente, die Sie entweder lokal oder auf einer EC2 Amazon-Instance in der AWS Cloud bereitstellen. Beide Komponenten werden regelmäßig aktualisiert. In den Themen in diesem Abschnitt wird der Rhythmus dieser Updates beschrieben, wie sie angewendet werden und wie Sie die Einstellungen für Updates auf den Gateways in Ihrer Bereitstellung konfigurieren.

> **Important**
>
> Sie sollten die Storage-Gateway-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 AWS Gateway-Aktualisierungsmechanismus (z. B. SSM oder Hypervisor-Tools) zu installieren oder zu aktualisieren, kann zu Fehlfunktionen des Gateways führen.

Aktualisierungshäufigkeit und erwartetes Verhalten

AWS aktualisiert die Cloud-Services-Komponente nach Bedarf, ohne dass die bereitgestellten Gateways unterbrochen werden. Ihre bereitgestellten Gateway-Appliances erhalten monatliche Wartungsupdates. Monatliche Wartungsupdates können Betriebssystem- und Software-Upgrades, Korrekturen zur Verbesserung der Stabilität, Leistung und Sicherheit sowie den Zugriff auf neue Funktionen beinhalten. Alle Updates sind kumulativ und aktualisieren Gateways auf die aktuelle Version, sobald sie installiert sind. Informationen zu den spezifischen Änderungen, die in den einzelnen Updates enthalten sind, finden Sie in den Versionshinweisen für die Tape Gateway-Gerätesoftware und den .

Monatliche Wartungsupdates können zu einer kurzzeitigen Betriebsunterbrechung führen. Der VM-Host des Gateways muss während der Updates nicht neu gestartet werden, aber das Gateway ist für kurze Zeit nicht verfügbar, solange das Gateway-Gerät aktualisiert und neu gestartet wird. 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.

Wenn Sie Ihr Gateway bereitstellen und aktivieren, wird ein standardmäßiger wöchentlicher Zeitplan für das Wartungsfenster festgelegt. Sie können den Zeitplan für das Wartungsfenster jederzeit ändern. Sie können die monatlichen Wartungsupdates auch deaktivieren, wir empfehlen jedoch, sie aktiviert zu lassen.

> **Note**
>
> Dringende Updates werden manchmal gemäß dem Zeitplan für das Wartungsfenster installiert, auch wenn die regelmäßigen Wartungsupdates ausgeschaltet sind.

Bevor ein Update auf Ihr Gateway angewendet wird, AWS benachrichtigt Sie mit einer Meldung auf der Storage Gateway Gateway-Konsole und Ihrem AWS Health Dashboard. Weitere Informationen finden Sie unter AWS Health Dashboard. Informationen zum Ändern der E-Mail-Adresse, an die Benachrichtigungen über Softwareupdates gesendet werden, finden Sie unter Aktualisieren der alternativen Kontakte für Ihr AWS Konto im Referenzhandbuch zur AWS Kontoverwaltung.

Wenn Updates verfügbar sind, wird auf der Registerkarte „Gateway-Details“ eine Wartungsmeldung angezeigt. Auf der Registerkarte Details können Sie auch das Datum und die Uhrzeit der Installation des letzten erfolgreichen Updates sehen.

Wartungsupdates ein- oder ausschalten

Wenn Wartungsupdates aktiviert sind, wendet Ihr Gateway diese Updates automatisch gemäß dem konfigurierten Zeitplan für das Wartungsfenster an. Weitere Informationen finden Sie unter .

Wenn Wartungsupdates deaktiviert sind, wendet das Gateway diese Updates nicht automatisch an. Sie können sie jedoch jederzeit manuell über die Storage Gateway Gateway-Konsole, API oder CLI anwenden. Dringende Updates werden manchmal unabhängig von dieser Einstellung während des konfigurierten Wartungsfensters installiert.

> **Note**
>
> Das folgende Verfahren beschreibt, wie Gateway-Updates mithilfe der Storage Gateway Gateway-Konsole ein- oder ausgeschaltet werden. Informationen zum programmgesteuerten Ändern dieser Einstellung mithilfe der API finden Sie UpdateMaintenanceStartTimein der Storage Gateway API-Referenz.

So schalten Sie Wartungsupdates mit der Storage Gateway Gateway-Konsole ein oder aus:

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie Wartungsupdates konfigurieren möchten.
3. Wählen Sie Aktionen und dann Wartungseinstellungen bearbeiten aus.
4. Wählen Sie für Wartungsupdates „Ein“ oder „Aus“.
5. Wählen Sie Änderungen speichern, wenn Sie fertig sind.

Sie können die aktualisierte Einstellung auf der Registerkarte Details für das ausgewählte Gateway in der Storage Gateway Gateway-Konsole überprüfen.

Ändern Sie den Zeitplan für das Gateway-Wartungsfenster

Wenn Wartungsupdates aktiviert sind, wendet Ihr Gateway diese Updates automatisch gemäß dem Zeitplan für das Wartungsfenster an. Dringende Updates werden manchmal während des konfigurierten Wartungsfensters installiert, unabhängig von der Einstellung für Wartungsupdates.

> **Note**
>
> Das folgende Verfahren beschreibt, wie Sie den Zeitplan für das Wartungsfenster mithilfe der Storage Gateway Gateway-Konsole ändern. Informationen zum programmgesteuerten Ändern dieser Einstellung mithilfe der API finden Sie UpdateMaintenanceStartTimein der Storage Gateway API-Referenz.

So ändern Sie den Zeitplan für das Wartungsfenster mit der Storage Gateway Gateway-Konsole:

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, für das Sie Wartungsupdates konfigurieren möchten.
3. Wählen Sie Aktionen und dann Wartungseinstellungen bearbeiten aus.
4. Gehen Sie unter Startzeit des Wartungsfensters wie folgt vor:

   a. Wählen Sie unter Zeitplan die Option Wöchentlich oder Monatlich aus, um die Häufigkeit des Wartungsfensters festzulegen.

   b. Wenn Sie Wöchentlich wählen, ändern Sie die Werte für Wochentag und Uhrzeit, um den bestimmten Zeitpunkt innerhalb jeder Woche festzulegen, an dem das Wartungsfenster beginnt.

      Wenn Sie Monatlich wählen, ändern Sie die Werte für Tag des Monats und Uhrzeit, um den bestimmten Zeitpunkt in jedem Monat festzulegen, an dem das Wartungsfenster beginnt.

      > **Note**
      >
      > Der Höchstwert, der für den Tag des Monats festgelegt werden kann, ist 28. Es ist nicht möglich, den Wartungsplan so festzulegen, dass er an den Tagen 29 bis 31 beginnt.
      > Wenn Sie bei der Konfiguration dieser Einstellung eine Fehlermeldung erhalten, kann dies bedeuten, dass Ihre Gateway-Software veraltet ist. Erwägen Sie, Ihr Gateway zunächst manuell zu aktualisieren und dann erneut zu versuchen, den Zeitplan für das Wartungsfenster zu konfigurieren.

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

Sie können die aktualisierten Einstellungen auf der Registerkarte Details für das ausgewählte Gateway in der Storage Gateway Gateway-Konsole überprüfen.

Manuelles Anwenden eines Updates

Wenn ein Softwareupdate für Ihr Gateway verfügbar ist, können Sie es manuell installieren, indem Sie wie folgt vorgehen. Bei diesem manuellen Aktualisierungsvorgang wird der Zeitplan für das Wartungsfenster ignoriert und das Update wird sofort angewendet, auch wenn die Wartungsupdates ausgeschaltet sind.

> **Note**
>
> Das folgende Verfahren beschreibt, wie Sie ein Update mithilfe der Storage Gateway Gateway-Konsole manuell anwenden. Informationen zum programmgesteuerten Ausführen dieser Aktion mithilfe der API finden Sie UpdateGatewaySoftwareNowin der Storage Gateway API-Referenz.

Um ein Gateway-Softwareupdate manuell mit der Storage Gateway Gateway-Konsole anzuwenden:

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, das Sie aktualisieren möchten.

   Wenn ein Update verfügbar ist, zeigt die Konsole auf der Registerkarte Gateway-Details ein blaues Benachrichtigungsbanner an, das eine Option zum Anwenden des Updates enthält.
3. Wählen Sie Update jetzt anwenden, um das Gateway sofort zu aktualisieren.

   > **Note**
   >
   > Dieser Vorgang führt zu einer vorübergehenden Unterbrechung der Gateway-Funktionalität während der Installation des Updates. Während dieser Zeit wird der Gateway-Status in der Storage Gateway Gateway-Konsole als OFFLINE angezeigt. Nach Abschluss der Installation des Updates nimmt das Gateway den normalen Betrieb wieder auf und sein Status ändert sich zu RUNNING.

Sie können überprüfen, ob die Gateway-Software auf die neueste Version aktualisiert wurde, indem Sie die Registerkarte Details für das ausgewählte Gateway in der Storage Gateway Gateway-Konsole überprüfen.

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. 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 EC2 Amazon-Gateway, das kurzlebigen Speicher verwendet, beenden und starten, ist das Gateway dauerhaft offline. Dies geschieht, weil der physische Speicherdatenträger ersetzt wird. Für dieses Problem gibt es keine Lösung. Die einzige Lösung besteht darin, das Gateway zu löschen und ein neues auf einer neuen EC2 Instance zu aktivieren.

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.

- Gateway VM local consolesee – siehe An der lokalen Konsole von Tape Gateway anmelden.
- Storage Gateway Gateway-API — siehe ShutdownGateway

Starten und Anhalten eines Tape Gateways

So beenden Sie ein Tape Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und wählen Sie dann das anzuhaltende Gateway. Der Status des Gateways lautet In Ausführung.
3. Wählen Sie für Actions (Aktionen) die Option Stop gateway (Gateway anhalten) aus und überprüfen Sie die ID des Gateways im Dialogfeld. Wählen Sie dann Stop gateway (Gateway anhalten) aus.

   Während das Gateway angehalten wird, sehen Sie möglicherweise eine Meldung mit dem Status des Gateways. Wenn das Gateway ausgeschaltet wird, werden eine Meldung und die Schaltfläche Start gateway (Gateway starten) auf der Registerkarte Details angezeigt.

Wenn Sie Ihr Gateway anhalten, kann nicht auf die Speicherressourcen zugegriffen werden, bis Sie den Speicher starten. Wenn das Gateway zum Zeitpunkt des Anhaltens Daten hochlud, wird der Upload fortgesetzt, nachdem Sie das Gateway gestartet haben.

So starten Sie ein Tape Gateway

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

Löschen Ihres Gateways und Entfernen der zugehörigen Ressourcen

Wenn Sie ein Gateway nicht weiter verwenden möchten, können Sie dieses zusammen mit den zugehörigen Ressourcen löschen. Durch das Entfernen von Ressourcen wird verhindert, dass Gebühren für Ressourcen entstehen, die Sie voraussichtlich nicht weiter verwenden werden, und Ihre monatliche Rechnung wird gesenkt.

Wenn Sie ein Gateway löschen, wird es nicht mehr in der AWS Storage Gateway 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 wird, führen Sie jedoch spezifische Anweisungen zum Entfernen zugehöriger Ressourcen aus.

> **Note**
>
> Wenn Sie ein Tape Gateway löschen, werden alle Bänder, die sich derzeit im `AVAILABLE` Status befinden, ebenfalls gelöscht, und alle Daten auf diesen Bändern gehen verloren. Wenn Sie Daten von Bändern behalten möchten, die von einem Gateway verwendet werden und das Sie löschen möchten, müssen Sie die Bänder archivieren, bevor Sie das Gateway löschen. Weitere Informationen finden Sie unter Archivierung virtueller Bänder.

Sie können ein Gateway mithilfe der Storage-Gateway-Konsole oder programmgesteuert löschen. Im Folgenden finden Sie Informationen zum Löschen eines Gateways mit der Storage-Gateway-Konsole. Informationen zum programmgesteuerten Löschen eines Gateways finden Sie unter AWS Storage Gateway API-Referenz..

Themen

- Löschen eines Gateways mithilfe der Storage-Gateway-Konsole
- Entfernen von Ressourcen von einem lokal bereitgestellten Gateway
- Ressourcen aus einem Gateway entfernen, das auf einer EC2 Amazon-Instance bereitgestellt wird

Löschen eines Gateways mithilfe der Storage-Gateway-Konsole

Die Schritte zum Löschen eines Gateways sind für alle Gateway-Typen gleich. Abhängig von dem Typ des Gateways, das Sie löschen möchten, und dem Host, auf dem es bereitgestellt wird, müssen Sie jedoch möglicherweise zusätzliche Aufgaben zum Entfernen von dem Gateway zugeordneten Ressourcen ausführen. Durch das Entfernen dieser Ressourcen wird verhindert, dass Sie für Ressourcen zahlen, die Sie voraussichtlich nicht mehr verwenden werden.

> **Note**
>
> Bei Gateways, die auf einer EC2 Amazon-Instance bereitgestellt werden, bleibt die Instance bestehen, bis Sie sie löschen.

Bei Gateways, die auf einer virtuellen Maschine (VM) bereitgestellt sind, ist die Gateway-VM nach dem Löschen des Gateways weiterhin in der Virtualisierungsumgebung vorhanden. Um die VM zu entfernen, verwenden Sie den VMware vSphere-Client, Microsoft Hyper-V Manager oder den Linux Kernel-based Virtual Machine (KVM) -Client, um eine Verbindung zum Host herzustellen und die VM zu entfernen. Beachten Sie, dass Sie die gelöschte Gateway-VM nicht erneut verwenden können, um ein neues Gateway zu aktivieren.

So löschen Sie ein Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend ein oder mehrere Gateways zum Löschen aus.
3. Wählen Sie für Aktionen die Option Gateway löschen aus. Das Bestätigungsdialogfeld wird angezeigt.

   Warning

   Bevor Sie diesen Schritt ausführen, stellen Sie sicher, dass derzeit keine Anwendungen in die Gateway-Volumes schreiben. Wenn Sie das Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten. Wenn ein Gateway gelöscht wird, gibt es keine Möglichkeit, es wiederherzustellen.

4. Vergewissern Sie sich, dass Sie die angegebenen Gateways löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen aus.
5. (Optional) Wenn Sie Feedback zu Ihrem gelöschten Gateway geben möchten, füllen Sie das Feedback-Dialogfeld aus und wählen Sie dann Absenden. Wählen Sie andernfalls Überspringen aus.

Important

Nach dem Löschen eines Gateways zahlen Sie keine Softwaregebühren mehr, aber Ressourcen wie virtuelle Bänder, Amazon Elastic Block Store (Amazon EBS) -Snapshots und EC2 Amazon-Instances bleiben bestehen. Diese Ressourcen werden Ihnen weiterhin berechnet. Sie können wählen, ob Sie EC2 Amazon-Instances und Amazon EBS-Snapshots entfernen möchten, indem Sie Ihr Amazon-Abonnement kündigen. EC2 Wenn Sie Ihr EC2

Amazon-Abonnement behalten möchten, können Sie Ihre Amazon EBS-Snapshots über die EC2 Amazon-Konsole löschen.

Entfernen von Ressourcen von einem lokal bereitgestellten Gateway

Anhand der folgenden Anweisungen können Sie Ressourcen von einem Gateway entfernen, das lokal bereitgestellt wird.

Entfernen von Ressourcen von einem auf einer VM bereitgestellten Tape Gateway

Beim Löschen einer Gateway-Virtual Tape Library (Gateway-VTL) führen Sie vor und nach dem Löschen des Gateways zusätzliche Schritte zur Bereinigung aus. Diese zusätzlichen Schritte helfen Ihnen beim Entfernen von Ressourcen, die Sie nicht benötigen, damit Sie nicht weiter für diese bezahlen.

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

> **Important**
>
> Vor dem Löschen eines Tape Gateways müssen Sie alle Bandabrufvorgänge abbrechen und alle abgerufenen Bänder auswerfen.
> Nachdem Sie das Tape Gateway gelöscht haben, müssen Sie alle zu diesem Tape Gateway gehörigen Ressourcen entfernen, die Sie nicht benötigen, um unnötige Kosten zu vermeiden.

Beim Löschen eines Tape Gateways kann eines von zwei Szenarien auftreten.

- Das Tape Gateway ist verbunden mit AWS — Wenn das Tape Gateway mit verbunden ist AWS und Sie das Gateway löschen, sind die mit dem Gateway verknüpften iSCSI-Ziele (d. h. die virtuellen Bandlaufwerke und der Media Changer) nicht mehr verfügbar.
- Das Tape Gateway ist nicht verbunden mit AWS — Wenn das Tape Gateway nicht verbunden ist AWS, z. B. wenn die zugrunde liegende VM ausgeschaltet ist oder Ihr Netzwerk ausgefallen ist, können Sie das Gateway nicht löschen. Wenn Sie versuchen, es zu löschen, haben Sie nach der erneuten Inbetriebnahme der Umgebung möglicherweise ein On-Premises ausgeführtes Tape Gateway mit verfügbaren iSCSI-Zielen. Es werden jedoch keine Tape Gateway-Daten auf, hoch- oder heruntergeladen AWS.

Wenn das zu löschende Tape nicht funktioniert, müssen Sie es zuerst deaktivieren, bevor Sie es löschen. Gehen Sie dazu wie folgt vor:

- Um Bänder mit dem Status "RETRIEVED" aus der Bibliothek zu löschen, werfen Sie das Band mithilfe Ihrer Sicherungssoftware aus. Anweisungen finden Sie unter Archivieren des Bandes.

Nach der Deaktivierung des Tape Gateways und dem Löschen der Bänder können Sie das Tape Gateway löschen. Anweisungen zum Löschen eines Gateways finden Sie unter Löschen eines Gateways mithilfe der Storage-Gateway-Konsole.

Wenn Sie Bänder archiviert haben, bleiben diese Bänder erhalten und Sie zahlen weiterhin für Speicher, bis Sie sie löschen. Informationen zum Löschen von Bändern aus einem Archiv finden Sie unter Virtuelle Bänder von Ihrem Tape Gateway löschen.

> **Important**
>
> Sie zahlen für virtuelle Bänder in einem Archiv für mindestens 90 Tage Speicher. Wenn Sie ein virtuelles Band abrufen, das weniger als 90 Tage im Archiv gespeichert war, werden Ihnen trotzdem 90 Tage Speicher berechnet.

Ressourcen aus einem Gateway entfernen, das auf einer EC2 Amazon-Instance bereitgestellt wird

Wenn Sie ein Gateway löschen möchten, das Sie auf einer EC2 Amazon-Instance bereitgestellt haben, empfehlen wir Ihnen, die AWS Ressourcen zu bereinigen, die mit dem Gateway verwendet wurden, insbesondere die EC2 Amazon-Instance, alle Amazon EBS-Volumes und auch Bänder, falls Sie ein Tape Gateway bereitgestellt haben. Auf diese Weise können Sie unerwartete nutzungsabhängige Gebühren vermeiden.

Entfernen von Ressourcen aus Ihrem auf Amazon bereitgestellten Tape Gateway EC2

Wenn Sie ein Tape bereitgestellt haben, schlagen wir vor, dass Sie die folgenden Schritte ausführen, um das Gateway zu löschen und seine Ressourcen zu bereinigen:

1. Löschen Sie alle virtuellen Bänder, die Sie auf das Tape Gateway abgerufen haben. Weitere Informationen finden Sie unter Virtuelle Bänder von Ihrem Tape Gateway löschen.

2. Löschen Sie alle virtuellen Bänder aus der Bandbibliothek. Weitere Informationen finden Sie unter Virtuelle Bänder von Ihrem Tape Gateway löschen.
3. Löschen Sie das Tape Gateway. Weitere Informationen finden Sie unter Löschen eines Gateways mithilfe der Storage-Gateway-Konsole.
4. Beenden Sie alle EC2 Amazon-Instances und löschen Sie alle Amazon EBS-Volumes. Weitere Informationen finden Sie unter Clean Up Your Instance and Volume im EC2 Amazon-Benutzerhandbuch.
5. Löschen Sie alle archivierten virtuellen Bänder. Weitere Informationen finden Sie unter Virtuelle Bänder von Ihrem Tape Gateway löschen.

> **Important**
>
> Sie zahlen für virtuelle Bänder im Archiv für mindestens 90 Tage Speicher. Wenn Sie ein virtuelles Band abrufen, das weniger als 90 Tage im Archiv gespeichert war, werden Ihnen trotzdem 90 Tage Speicher berechnet.

Durchführung von Wartungsaufgaben über die lokale Konsole

Dieser Abschnitt enthält die folgenden Themen, die Informationen zur Durchführung von Wartungsaufgaben mithilfe der lokalen Konsole der Gateway-Appliance enthalten. Die lokale Konsole wird direkt auf der Virtualisierungshostplattform ausgeführt, auf der Ihre Gateway-Appliance gehostet wird. Bei lokalen Gateways greifen Sie über Ihren Hyper-V- oder VMware Linux-KVM-Virtualisierungshost auf die lokale Konsole zu. Bei EC2 Amazon-Gateways greifen Sie auf die Konsole zu, indem Sie sich über SSH mit der EC2 Amazon-Instance verbinden. Die meisten Aufgaben sind auf den verschiedenen Host-Plattformen gleich, es gibt jedoch auch einige Unterschiede.

Topics

- Zugreifen auf die lokale Konsole des Gateways- Erfahren Sie, wie Sie sich bei der lokalen Konsole für ein lokales Gateway anmelden, das auf einer Linux-Kernel-basierten virtuellen Maschine (KVM) oder einer Microsoft Hyper-V VMware ESXi Manager-Plattform gehostet wird.
- Ausführen von Aufgaben in der lokalen VM-Konsole von - Erfahren Sie, wie Sie mit der lokalen Konsole grundlegende Einrichtungsaufgaben und erweiterte Konfigurationsaufgaben für ein lokales Gateway ausführen, z. B. einen HTTP-Proxy konfigurieren, den Status der Systemressourcen anzeigen oder Terminalbefehle ausführen.
- Aufgaben auf der Amazon EC2 Local Console ausführen- Erfahren Sie, wie Sie sich bei der lokalen Konsole anmelden, um grundlegende Einrichtungsaufgaben und erweiterte Konfigurationsaufgaben für ein EC2 Amazon-Gateway durchzuführen, z. B. einen HTTP-Proxy zu konfigurieren, den Status der Systemressourcen anzuzeigen oder Terminalbefehle auszuführen.

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

Themen

- Zugreifen auf die lokale Konsole des Gateways mit Linux KVM

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

Zugreifen auf die lokale Konsole des Gateways mit Linux KVM

Je nach verwendeter Linux-Verteilung gibt es verschiedene Möglichkeiten, virtuelle Maschinen auf KVM zu konfigurieren. Anweisungen für den Zugriff auf die KVM-Konfigurationsoptionen über die Befehlszeile folgen. Die Anweisungen können je nach KVM-Implementierung unterschiedlich sein.

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

1. Verwenden Sie den folgenden Befehl, um die derzeit in KVM verfügbaren Optionen VMs aufzulisten.

   ```
   # virsh list
   ```

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

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

   ```
   # virsh console Id
   ```

   *`Id`*Ersetzen Sie es durch die ID der VM, die Sie im vorherigen Schritt notiert haben.

   Die lokale Konsole des AWS Appliance-Gateways fordert Sie auf, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich bei der lokalen Gateway-Konsole anzumelden. Weitere Informationen finden Sie unter Bei der lokalen Tape Gateway-Konsole anmelden Bei der lokalen anmelden.

   Nach der Anmeldung wird das Menü AWS Geräteaktivierung — Konfiguration angezeigt. Sie können aus den Menüoptionen auswählen, um Gateway-Konfigurationsaufgaben auszuführen. Weitere Informationen finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine .

Zugreifen auf die lokale Gateway-Konsole mit VMware ESXi

Um auf die lokale Konsole Ihres Gateways zuzugreifen mit VMware ESXi

1. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM aus.
2. Stellen Sie sicher, dass die Gateway-VM eingeschaltet ist.

   > **Note**
   >
   > Wenn Ihre Gateway-VM eingeschaltet ist, erscheint ein grünes Pfeilsymbol zusammen mit dem VM-Symbol im VM-Browserfenster auf der linken Seite des Anwendungsfensters. Wenn Ihre Gateway-VM nicht eingeschaltet ist, können Sie sie einschalten, indem Sie in der Werkzeugleiste oben im Anwendungsfenster auf das grüne Einschaltsymbol klicken.

3. Wählen Sie im Hauptinformationsbereich auf der rechten Seite des Anwendungsfensters die Registerkarte Konsole.

   Nach einigen Augenblicken werden Sie von der lokalen Konsole des AWS Appliance-Gateways aufgefordert, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

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

4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich an der lokalen Gateway-Konsole anzumelden. Weitere Informationen finden Sie unter Bei der lokalen Tape Gateway-Konsole anmelden Bei der lokalen anmelden.

   Nach der Anmeldung wird das Menü AWS Geräteaktivierung — Konfiguration angezeigt. Sie können aus den Menüoptionen auswählen, um Gateway-Konfigurationsaufgaben auszuführen. Weitere Informationen finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine .

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

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

1. Wählen Sie Ihre Gateway-Appliance-VM im Bereich Virtuelle Maschinen auf der linken Seite des Microsoft Hyper-V Manager-Anwendungsfensters aus.
2. Stellen Sie sicher, dass das Gateway aktiviert ist.

   > **Note**
   >
   > Wenn Ihre Gateway-VM eingeschaltet `Running` ist, wird dies in der Statusspalte für die VM im Bereich Virtuelle Maschinen auf der linken Seite des Anwendungsfensters angezeigt. Wenn Ihre Gateway-VM nicht eingeschaltet ist, können Sie sie einschalten, indem Sie im Bereich Aktionen auf der rechten Seite des Anwendungsfensters auf Start klicken.

3. Wählen Sie im Bedienfeld „Aktionen“ die Option „Connect“.

   Das Fenster Virtual Machine Connection (Verbindung der virtuellen Maschine) wird angezeigt. Wenn ein Authentifizierungsfenster angezeigt wird, geben Sie die Anmeldeinformationen ein, die Sie vom Hypervisor-Administrator erhalten haben.

   Nach einigen Augenblicken werden Sie von der lokalen Konsole des AWS Appliance-Gateways aufgefordert, sich anzumelden, um Ihre Netzwerkkonfiguration und andere Einstellungen zu ändern.

4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich an der lokalen Gateway-Konsole anzumelden. Weitere Informationen finden Sie unter Bei der lokalen Tape Gateway-Konsole anmelden Bei der lokalen anmelden.

   Nach der Anmeldung wird das Menü AWS Geräteaktivierung — Konfiguration angezeigt. Sie können aus den Menüoptionen auswählen, um Gateway-Konfigurationsaufgaben auszuführen. Weitere Informationen finden Sie unter Ausführen von Aufgaben auf der lokalen Konsole der virtuellen Maschine .

Ausführen von Aufgaben in der lokalen VM-Konsole von

Für ein Tape Gateway , das Sie lokal bereitstellen, können Sie die folgenden Wartungsaufgaben mit der lokalen Gateway-Konsole ausführen, auf die Sie von Ihrer VM-Hostplattform aus zugreifen. Diese Aufgaben sind bei Hyper-V- und Linux-Kernel-basierten virtuellen Maschinen (KVM) Hypervisoren üblich. VMware

Topics

- An der lokalen Konsole von Tape Gateway anmelden- Erfahren Sie, wie Sie sich bei der lokalen Gateway-Konsole anmelden, wo Sie die Gateway-Netzwerkeinstellungen konfigurieren und das Standardkennwort ändern können.
- Konfiguration eines SOCKS5 Proxys für Ihr lokales Gateway- Erfahren Sie, wie Sie Storage Gateway so konfigurieren können, dass der gesamte AWS Endpunktdatenverkehr über einen Socket Secure Version 5 (SOCKS5) -Proxyserver geleitet wird.
- Konfigurieren Ihres Gateway-Netzwerks- Erfahren Sie, wie Sie Ihr Gateway so konfigurieren können, dass es DHCP verwendet oder eine statische IP-Adresse zuweist.
- Testen Sie Ihre Gateway-Verbindung zum Internet- Erfahren Sie, wie Sie die lokale Gateway-Konsole verwenden können, um die Verbindung zwischen dem Gateway und dem Internet zu testen.
- Storage-Gateway-Befehle in der lokalen Konsole für ein lokales Gateway ausführen- Erfahren Sie, wie Sie lokale Konsolenbefehle ausführen, mit denen Sie zusätzliche Aufgaben ausführen können, z. B. das Speichern von Routingtabellen, das Herstellen einer Verbindung zu Support usw.
- Anzeigen des Gateway-Systemressourcen-Status- Erfahren Sie, wie Sie die virtuellen CPU-Kerne, die Größe des Root-Volumes und den Arbeitsspeicher überprüfen, die für Ihre Gateway-Appliance verfügbar sind.

An der lokalen Konsole von Tape Gateway anmelden

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 von der AWS Storage Gateway Konsole aus festlegen, anstatt das Passwort von der lokalen Konsole aus 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

- 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 Storage-Gateway-Befehle in der lokalen Konsole für ein lokales Gateway ausführen. Sie können Ihr eigenes Passwort auch von der AWS Storage Gateway Konsole aus 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.

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 Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
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.

Konfiguration eines SOCKS5 Proxys für Ihr lokales Gateway

Volume Gateways und Tape Gateways unterstützen die Konfiguration eines Socket Secure Version 5 (SOCKS5) -Proxys zwischen Ihrem lokalen Gateway und. AWS

> **Note**
>
> Die einzige unterstützte Proxykonfiguration 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.

Um einen SOCKS5 Proxy für Volume- und Tape-Gateways zu konfigurieren

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

   - VMware ESXi — Weitere Informationen finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - KVM: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.

2. Geben Sie im Hauptmenü AWS Storage Gateway – Konfiguration die entsprechende Zahl ein, um SOCKS-Proxy-Konfiguration auszuwählen.
3. Geben Sie im Menü AWS Storage Gateway – SOCKS-Proxy-Konfiguration die entsprechende Zahl ein, um eine der folgenden Aufgaben auszuführen:

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren eines SOCKS-Proxys	Geben Sie die entsprechende Zahl ein, um SOCKS-Proxy konfigurieren auszuwählen. Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
Anzeigen der aktuellen SOCKS-Proxy-Konfiguration	Geben Sie die entsprechende Zahl ein, um Aktuelle SOCKS-Proxykonfiguration anzeigen auszuwählen. Wenn kein SOCKS-Proxy konfiguriert ist, wird die Meldung `SOCKS Proxy not configured` angezeigt. Ist ein SOCKS-Proxy konfiguriert, werden der Hostname und Port des Proxys angezeigt.
Entfernen einer SOCKS-Proxy-Konfiguration	

Zur Ausführung dieser Aufgabe	Vorgehensweise
	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 unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - KVM: Weitere Informationen finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Geben Sie im Hauptmenü AWS Storage Gateway – Konfiguration die entsprechende Zahl ein, um Netzwerkkonfiguration auszuwählen.
3. Führen Sie im Menü Netzwerkkonfiguration AWS von Storage Gateway eine der folgenden Aufgaben aus:

Zur Ausführung dieser Aufgabe	Vorgehensweise
Beschreiben des Netzwerkadapters	Geben Sie die entsprechende Zahl ein, um Adapter beschreiben auszuwählen.

Zur Ausführung dieser Aufgabe	Vorgehensweise
	Eine Liste der Adapternamen wird angezeigt, und Sie werden aufgefordert, einen Adaptername einzugeben, z. B. **`eth0`**. Wenn der von Ihnen angegebene Adapter verwendet wird, werden die folgenden Informationen zum Adapter angezeigt: • Media Access Control-Adresse (MAC) • IP-Adresse • Netzmaske • Gateway-IP-Adresse • DHCP-aktivierter Status Sie verwenden die hier aufgeführten Adapternamen, wenn Sie eine statische IP-Adresse konfigurieren oder den Standardadapter Ihres Gateways festlegen.
Konfigurieren von DHCP	Geben Sie die entsprechende Zahl ein, um DHCP konfigurieren auszuwählen. Sie werden aufgefordert, die Netzwerkschnittstelle für die Verwendung von DHCP zu konfigurieren.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren einer statischen IP-Adresse für Ihr Gateway	Geben Sie die entsprechende Zahl ein, um Statische IP-Adresse konfigurieren auszuwählen. Sie werden aufgefordert, die folgenden Informationen zur Konfiguration einer statischen IP-Adresse einzugeben: • Netzwerkadaptername • IP-Adresse • Netzmaske • Standard-Gateway-Adresse • Primary Domain Name Service-Adresse (DNS) • Sekundäre DNS-Adresse **Important** Wenn Ihr Gateway bereits aktiviert wurde, müssen Sie es in der Storage-Gateway-Konsole beenden und neu starten, damit die Einstellungen wirksam werden. Weitere Informationen finden Sie unter Herunterfahren der Gateway-VM.

Zur Ausführung dieser Aufgabe	Vorgehensweise
	Wenn Ihr Gateway mehrere Netzwerkschnittstellen verwendet, müssen Sie alle aktivierten Schnittstellen für die Verwendung von DHCP- oder statischen IP-Adressen einrichten. Angenommen, Ihre Gateway-VM verwendet als DHCP konfigurierte Schnittstellen. Wenn Sie später eine Schnittstelle für eine statische IP einrichten, wird die andere Schnittstelle deaktiviert. Um die Schnittstelle in diesem Fall zu aktivieren, müssen Sie sie für eine statische IP einrichten. Wenn beide Schnittstellen anfänglich für die Verwendung von statischen IP-Adressen eingerichtet sind und Sie das Gateway für die Verwendung von DHCP einrichten, verwenden beide Schnittstellen DHCP.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Konfigurieren eines Hostnamens für Ihr Gateway	Geben Sie die entsprechende Zahl ein, um Hostname konfigurieren auszuwählen. Sie werden aufgefordert, auszuwählen, ob das Gateway einen von Ihnen angegebenen statischen Hostnamen verwenden oder einen Namen automatisch über DCHP oder rDNS beziehen soll. Wenn Sie Statisch wählen, werden Sie aufgefordert, einen statischen Hostnamen anzugeben, z. B. `testgateway.example.com` Geben Sie einy, um die Konfiguration anzuwenden. **Note** Wenn Sie einen statischen Hostnamen für Ihr Gateway konfigurieren, stellen Sie sicher, dass sich der angegebene Hostname in der Domäne befindet, zu der das Gateway gehört. Sie müssen außerdem einen A-Eintrag in Ihrem DNS-System erstellen, der die IP-Adresse des Gateways auf seinen statischen Hostnamen verweist.

Zur Ausführung dieser Aufgabe	Vorgehensweise
Zurücksetzen der Netzwerkkonfiguration Ihres Gateways auf DHCP	Geben Sie die entsprechende Zahl ein, um Alles auf DHCP zurücksetzen auszuwählen. Alle Netzwerkschnittstellen sind für die Verwendung von DHCP eingerichtet. **Important** Wenn Ihr Gateway bereits aktiviert wurde, müssen Sie es in der Storage-Gateway-Konsole beenden und neu starten, damit die Einstellungen wirksam werden. Weitere Informationen finden Sie unter Herunterfahren der Gateway-VM.
Einrichten des Standard-Routing-Adapters Ihres Gateways	Geben Sie die entsprechende Zahl ein, um Standardadapter festlegen auszuwählen. Die Adapter, die für Ihr Gateway verfügbar sind, werden angezeigt, und Sie werden aufgefordert, einen der Adapter auszuwählen, z. B. **`eth0`**.
Anzeigen der DNS-Konfiguration Ihres Gateways	Geben Sie die entsprechende Zahl ein, um DNS-Konfiguration anzeigen auszuwählen. Die IP-Adressen des primären und sekundären DNS-Namenservers werden angezeigt.

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

Testen Sie Ihre Gateway-Verbindung zum Internet

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 unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - 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 AWS-Region wie in den folgenden Schritten beschrieben angeben.
3. Wenn Ihr Gateway noch nicht aktiviert ist, geben Sie die entsprechende Zahl ein, um den Endpunkttyp für Ihr Gateway auszuwählen.
4. Wenn Sie den öffentlichen Endpunkttyp ausgewählt haben, geben Sie die entsprechende Zahl ein, um den Endpunkttyp auszuwählen AWS-Region , den Sie testen möchten. Unterstützte Endpunkte AWS-Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Im Verlauf des Tests zeigt jeder Endpunkt entweder [PASSED] oder [FAILED] an, womit der Status der Verbindung wie folgt angegeben wird:

Fehlermeldung	Beschreibung
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über Netzwerkkonnektivität.
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway hat keine Netzwerkkonnektivität.

Storage-Gateway-Befehle in der lokalen Konsole für ein lokales Gateway ausführen

Die lokale Konsole der VM in Storage Gateway stellt eine sichere Umgebung für die Konfiguration und Diagnose von Problemen mit dem Gateway bereit. Mithilfe der lokalen Konsolenbefehle können Sie Wartungsaufgaben wie das Speichern von Routingtabellen, das Herstellen einer Verbindung zu Support usw. ausführen.

So führen Sie eine Konfiguration oder einen Diagnosebefehl aus

1. Melden Sie sich bei der lokalen Konsole des Gateways an:
   - Weitere Informationen zur Anmeldung an der VMware ESXi lokalen Konsole finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Geben Sie im Hauptmenü AWS -Geräteaktivierung – Konfiguration die entsprechende Zahl ein, um Gateway-Konsole auszuwählen.
3. Geben Sie in der Eingabeaufforderung der Gateway-Konsole **h** ein.

   Die Konsole zeigt das Menü VERFÜGBARE BEFEHLE mit den verfügbaren Befehlen an:

Befehl	Funktion
dig	Sammeln Sie die Ausgaben von dig für die DNS-Fehlerbehebung.
exit	Kehren Sie zum Konfigurationsmenü zurück.
h	Zeigen Sie die Liste der verfügbaren Befehle an.
ifconfig	Netzwerkschnittstellen anzeigen oder konfigurieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren. Anweisungen finden Sie unter Konfigurieren Ihres Gateway-Netzwerks.
ip	Routing, Geräte und Tunnel anzeigen/manipulieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren. Anweisungen finden Sie unter Konfigurieren Ihres Gateway-Netzwerks.

Befehl	Funktion
iptables	Administrationstool für IPv4 Paketfilterung und NAT.
ncport	Testen Sie die Konnektivität zu einem bestimmten TCP-Port in einem Netzwerk.
nping	Sammeln Sie die Ausgaben von nping zur Netzwerkfehlerbehebung.
open-support-channel	Connect zum AWS Support her.
passwd	Aktualisieren Sie die Authentifizierungstoken.
save-iptables	IP-Tabellen speichern.
save-routing-table	Speichern Sie den neu hinzugefügten Eintrag in der Routingtabelle.
sslcheck	Gibt die Ausgabe mit dem Zertifikatsaussteller zurück **Note** Storage Gateway verwendet die Überprüfung durch den Zertifikatsaussteller und unterstützt keine SSL-Inspektion. Wenn dieser Befehl einen anderen Aussteller als aws-appliance@amazon.com zurückgibt, ist es wahrscheinlich, dass eine Anwendung eine SSL-Inspektion durchführt. In diesem Fall empfehlen wir, die SSL-Inspektion für die Storage Gateway Gateway-Appliance zu umgehen.

Befehl	Funktion
tcptraceroute	Erfassen Sie die Traceroute-Ausgabe des TCP-Datenverkehrs zu einem Ziel.

4. Geben Sie an der Eingabeaufforderung der Gateway-Konsole den entsprechenden Befehl für die Funktion ein, die Sie verwenden möchten, und folgen Sie den Anweisungen.

Um mehr über einen Befehl zu erfahren, geben Sie *command name* in der Befehlszeile **man** + ein.

Anzeigen des Gateway-Systemressourcen-Status

Beim Starten überprüft Ihr Gateway seine virtuellen CPU-Kerne, Stamm-Volume-Größe und RAM. Er kann dann bestimmen, ob ausreichend Systemressourcen für die ordnungsgemäße Funktionsweise Ihres Gateways verfügbar sind. Sie können die Ergebnisse dieser Prüfung auf der lokalen Gateway-Konsole anzeigen.

So zeigen Sie den Status einer Systemressourcenprüfung an

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

   - Weitere Informationen zur Anmeldung an der VMware ESXi Konsole finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zum Anmelden bei der lokalen KVM-Konsole finden Sie unter Zugreifen auf die lokale Konsole des Gateways mit Linux KVM.
2. Geben Sie im Hauptmenü AWS -Appliance-Aktivierung – Konfiguration) die entsprechende Zahl ein, um Systemressourcenprüfung anzeigen auszuwählen.

   Für jede Ressource wird [OK], [WARNING] oder [FAIL] angezeigt, was den Status der Ressource wie folgt angibt:

Fehlermeldung	Beschreibung
[OK]	Die Ressource hat die Systemressourcenprüfung bestanden.

Fehlermeldung	Beschreibung
[WARNING] ([WARNUNG])	Die Ressource erfüllt nicht die empfohlenen Anforderungen, aber das Gateway ist weiterhin funktionsfähig. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.
[FAIL] ([FEHLGESCHLAGEN])	Die Ressource erfüllt nicht die Mindestanforderungen. Das Gateways funktioniert möglicherweise nicht ordnungsgemäß. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.

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

Aufgaben auf der Amazon EC2 Local Console ausführen

Einige Storage Gateway Gateway-Wartungsaufgaben erfordern, dass Sie sich bei der lokalen Gateway-Konsole für ein Gateway anmelden, das Sie auf einer EC2 Amazon-Instance bereitgestellt haben. Sie können mit einem Secure Shell (SSH) -Client auf die lokale Gateway-Konsole auf Ihrer EC2 Amazon-Instance zugreifen. In den Themen in diesem Abschnitt wird beschrieben, wie Sie sich bei der lokalen Gateway-Konsole anmelden und Wartungsaufgaben ausführen.

Topics

- Melden Sie sich bei Ihrer lokalen Amazon EC2 Gateway-Konsole an— Erfahren Sie, wie Sie Ihre EC2 Amazon-Instance mithilfe eines Secure Shell (SSH) -Clients mit der lokalen Gateway-Konsole verbinden und sich dort anmelden können.
- Routing Ihres bereitgestellten Gateways EC2 über einen HTTP-Proxy- Erfahren Sie, wie Sie Storage Gateway so konfigurieren können, dass der gesamte AWS Endpunktverkehr über einen Socket Secure Version 5 (SOCKS5) -Proxyserver an Ihre Amazon EC2 Gateway-Instance weitergeleitet wird.

- Testen der Gateway-Netzwerkkonnektivität- Erfahren Sie, wie Sie die lokale Gateway-Konsole verwenden können, um die Netzwerkkonnektivität zwischen Ihrem Gateway und verschiedenen Netzwerkressourcen zu testen.
- Anzeigen des Gateway-Systemressourcen-Status- Erfahren Sie, wie Sie mit der lokalen Gateway-Konsole die virtuellen CPU-Kerne, die Größe des Root-Volumes und den Arbeitsspeicher überprüfen können, die für Ihre Gateway-Appliance verfügbar sind.
- Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole- Erfahren Sie, wie Sie lokale Konsolenbefehle ausführen können, mit denen Sie zusätzliche Aufgaben ausführen können, z. B. das Speichern von Routingtabellen, das Herstellen einer Verbindung zu Support usw.

Melden Sie sich bei Ihrer lokalen Amazon EC2 Gateway-Konsole an

Sie können mithilfe eines Secure Shell (SSH) -Clients eine Verbindung zu Ihrer EC2 Amazon-Instance herstellen. Ausführliche Informationen finden Sie unter Connect to Your Instance im EC2 Amazon-Benutzerhandbuch. Für diese Art des Verbindungsaufbaus benötigen Sie das SSH-Schlüsselpaar, das Sie beim Starten der Instance angegeben haben. Informationen zu EC2 Amazon-Schlüsselpaaren finden Sie unter EC2 Amazon-Schlüsselpaare im EC2 Amazon-Benutzerhandbuch.

So melden Sie sich bei der lokalen Konsole des Gateways an

1. Melden Sie sich bei der lokalen Konsole an. Wenn Sie von einem Windows-Computer aus eine Verbindung zu Ihrer EC2 Instance herstellen, melden Sie sich als Administrator 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	Routing Ihres bereitgestellten Gateways EC2 über einen HTTP-Proxy
Testen der Netzwerkverbindung	Testen der Gateway-Netzwerkkonnektivität
Ausführen von Storage-Gateway-Konsolenbefehlen	Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole

Für weitere Informationen zu dieser Aufgabe	Siehe folgendes Thema
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.

Routing Ihres bereitgestellten Gateways EC2 über einen HTTP-Proxy

Storage Gateway unterstützt die Konfiguration eines Socket Secure Version 5 (SOCKS5) -Proxys zwischen Ihrem auf Amazon bereitgestellten Gateway EC2 und AWS.

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. Nachdem Sie dies getan haben, leitet Storage Gateway den gesamten AWS Endpunktdatenverkehr über Ihren Proxyserver weiter. Die Kommunikation zwischen dem Gateway und den Endpunkten ist verschlüsselt, auch wenn der HTTP-Proxy verwendet wird.

So leiten Sie Ihren Gateway-Internet-Datenverkehr über einen lokalen Proxy-Server weiter

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2 Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS -Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um HTTP-Proxy aktivieren auszuwählen.
3. Geben Sie im Menü AWS Appliance-Aktivierung HTTP-Proxy-Konfiguration die entsprechende Zahl für die Aufgabe ein, die Sie ausführen möchten:

   - Konfigurieren eines HTTP-Proxy konfigurieren – Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
   - Anzeigen der aktuellen HTTP-Proxy-Konfiguration – Wenn kein HTTP-Proxy konfiguriert ist, wird die Nachricht `HTTP Proxy not configured` angezeigt. Ist ein HTTP-Proxy konfiguriert, werden der Hostname und Port des Proxys angezeigt.

- Entfernen einer HTTP-Proxy-Konfiguration – Die Nachricht `HTTP Proxy Configuration Removed` wird angezeigt.

Testen der Gateway-Netzwerkkonnektivität

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

So testen Sie die Konnektivität Ihres Gateways

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2 Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS -Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um Netzwerkkonnektivität testen auszuwählen.

   Wenn Ihr Gateway bereits aktiviert wurde, beginnt der Konnektivitätstest sofort. Für Gateways, die noch nicht aktiviert wurden, müssen Sie den Endpunkttyp AWS-Region wie in den folgenden Schritten beschrieben angeben.
3. Wenn Ihr Gateway noch nicht aktiviert ist, geben Sie die entsprechende Zahl ein, um den Endpunkttyp für Ihr Gateway auszuwählen.
4. Wenn Sie den öffentlichen Endpunkttyp ausgewählt haben, geben Sie die entsprechende Zahl ein, um den Endpunkttyp auszuwählen AWS-Region , den Sie testen möchten. Unterstützte Endpunkte AWS-Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Im Verlauf des Tests zeigt jeder Endpunkt entweder [PASSED] oder [FAILED] an, womit der Status der Verbindung wie folgt angegeben wird:

Fehlermeldung	Beschreibung
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über Netzwerkkonnektivität.
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway hat keine Netzwerkkonnektivität.

Anzeigen des Gateway-Systemressourcen-Status

Beim Starten überprüft Ihr Gateway seine virtuellen CPU-Kerne, Stamm-Volume-Größe und RAM. Er kann dann bestimmen, ob ausreichend Systemressourcen für die ordnungsgemäße Funktionsweise Ihres Gateways verfügbar sind. Sie können die Ergebnisse dieser Prüfung auf der lokalen Gateway-Konsole anzeigen.

So zeigen Sie den Status einer Systemressourcenprüfung an

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2 Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS -Geräteaktivierung – Konfiguration) die entsprechende Zahl ein, um Systemressourcenprüfung anzeigen auszuwählen.

   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 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. Mithilfe der Konsolenbefehle können Sie Wartungsaufgaben wie das Speichern von Routingtabellen oder das Herstellen einer Verbindung zu Support ausführen.

So führen Sie eine Konfiguration oder einen Diagnosebefehl aus

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2 Gateway-Konsole an.
2. Geben Sie im Hauptmenü AWS -Geräteaktivierung – Konfiguration die entsprechende Zahl ein, um Gateway-Konsole auszuwählen.
3. Geben Sie in der Eingabeaufforderung der Gateway-Konsole h ein.

   Die Konsole zeigt das Menü VERFÜGBARE BEFEHLE mit den verfügbaren Befehlen an:

Befehl	Funktion
dig	Sammeln Sie die Ausgaben von dig für die DNS-Fehlerbehebung.
exit	Kehren Sie zum Konfigurationsmenü zurück.
h	Zeigen Sie die Liste der verfügbaren Befehle an.
ifconfig	Netzwerkschnittstellen anzeigen oder konfigurieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren.

Befehl	Funktion
ip	Routing, Geräte und Tunnel anzeigen/manipulieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren.
iptables	Administrationstool für IPv4 Paketfilterung und NAT.
ncport	Testen Sie die Konnektivität zu einem bestimmten TCP-Port in einem Netzwerk.
nping	Sammeln Sie die Ausgaben von nping zur Netzwerkfehlerbehebung.
open-support-channel	Connect zum AWS Support her.
save-iptables	IP-Tabellen speichern.
save-routing-table	Speichern Sie den neu hinzugefügten Eintrag in der Routingtabelle.
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`.

Leistung und Optimierung für Tape Gateway

In diesem Abschnitt wird die Leistung von Storage Gateway beschrieben.

Themen

- Leistungsleitfaden für Tape Gateway
- Optimierung der Gateway-Leistung

Leistungsleitfaden für Tape Gateway

In diesem Abschnitt finden Sie eine Konfigurationsanleitung für die Bereitstellung von Hardware für Ihre Tape-Gateway-VM. Die in der Tabelle aufgeführten EC2 Amazon-Instance-Größen und -Typen sind Beispiele und dienen als Referenz.

Konfiguration	Schreibdurchsatz in Gbit/s	Lesedurchsatz aus Cache in Gbit/s	Lesen Sie „Amazon Web Services Cloud-Durchsatz in Gbit/s“
Host-Plattform: EC2 Amazon-Instance — c5.4xlarge CPU: 16 vCPU | RAM: 32 GB Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPS Cache-Festplatte: gestreiftes RAID (2 x 500 GB, io1 EBS SSD, 25000) IOPs Pufferfestplatte hochladen: 450 GB, io1 SSD, 2000 IOPs Netzwerkbandbreite zur Cloud: 10 Gbit/s	2.3	4,0	2.2

Konfiguration	Schreibdurchsatz in Gbit/s	Lesedurchsatz aus Cache in Gbit/s	Lesen Sie „Amazon Web Services Cloud-Durchsatz in Gbit/s“
Host-Plattform: Storage Gateway-Hardware Appliance Cache-Datenträger: 2,5 TB Upload-Pufferdatenträger: 2 TB Netzwerkbandbreite zur Cloud: 10 Gbit/s	2.3	8.8	3.8
Host-Plattform: Amazon EC2instance — c5d.9xlarge CPU: 36 vCPU | RAM: 72 GB Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPS Cache-Festplatte: 900-GB-Festplatte NVMe Upload-Pufferfestplatte: NVMe 900-GB-Festplatte Netzwerkbandbreite zur Cloud: 10 Gbit/s	5.2	11.6	5.2

Konfiguration	Schreibdurchsatz in Gbit/s	Lesedurchsatz aus Cache in Gbit/s	Lesen Sie „Amazon Web Services Cloud-Durchsatz in Gbit/s“
Host-Plattform: Amazon EC2instance — c5d.metal CPU: 96 vCPU | RAM: 192 GB Stammfestplatte: 80 GB, io1 SSD, 4.000 IOPS Cache-Festplatte: gestreiftes RAID (2 x 900 GB-Festplatte) NVMe Pufferfestplatte hochladen: NVMe 900-GB-Festplatte Netzwerkbandbreite zur Cloud: 10 Gbit/s	5.2	11.6	7.2

Note

Diese Leistung wurde unter der Verwendung einer Blockgröße von 1 MB und zehn Bandlaufwerken gleichzeitig erzielt.
Die EC2 Konfigurationen in der obigen Tabelle sollen nur repräsentativ für die Leistung sein, die Sie auf Ihren eigenen physischen Servern mit ähnlichen Ressourcen erzielen könnten. Die EC2 Konfigurationen, bei denen ein Striped-RAID verwendet wurde, wurden beispielsweise über einen speziellen Mechanismus vorgenommen, der von unserem Gateway in der Regel nicht unterstützt wird. EC2 Um eine ähnliche Leistung zu erzielen, sollten Sie stattdessen einen Hardware-RAID-Controller verwenden, der an den On-Premises-Server angeschlossen ist, auf dem Ihr Gateway läuft.
Die Leistung hängt von der Konfiguration Ihrer Hostplattform und der Netzwerkbandbreite ab.

Informationen zur Verbesserung der Schreib- und Lese-Durchsatzleistung Ihres Tape Gateways finden Sie unter Optimieren von iSCSI-Einstellungen, Verwenden Sie eine größere Blockgröße für Bandlaufwerke und Optimieren der Leistung von virtuellen Bandlaufwerken in der Sicherungssoftware.

Optimierung der Gateway-Leistung

Empfohlene Gateway-Serverkonfiguration

Um die beste Leistung aus Ihrem Gateway herauszuholen, wird von Storage Gateway die folgende Gateway-Konfiguration für den Host-Server Ihres Gateways empfohlen:

- Mindestens 64 dedizierte physische CPU-Kerne
- Für ein Tape Gateway sollte Ihre Hardware die folgenden Mengen an RAM reservieren:
  - Mindestens 16 GiB reservierter RAM für Gateways mit einer Cache-Größe von bis zu 16 TiB
  - Mindestens 32 GiB reservierter RAM für Gateways mit einer Cache-Größe von 16 TiB bis 32 TiB
  - Mindestens 48 GiB reservierter RAM für Gateways mit einer Cache-Größe von 32 TiB bis 64 TiB

> **Note**
>
> Für eine optimale Gateway-Leistung müssen Sie mindestens 32 GiB RAM bereitstellen.

- Festplatte 1, die wie folgt als Gateway-Cache verwendet werden soll:
  - Gestreiftes RAID (redundantes Array unabhängiger Festplatten), bestehend aus NVMe SSDs.
- Festplatte 2, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
  - Gestreiftes RAID bestehend aus NVMe SSDs.
- Festplatte 3, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
  - Gestreiftes RAID bestehend aus NVMe SSDs.
- Netzwerkadapter 1 auf VM Netzwerk 1 konfiguriert:
  - Verwenden Sie das VM-Netzwerk 1 und fügen Sie VMXnet3 (10 Gbit/s) hinzu, das für die Aufnahme verwendet werden soll.
- Netzwerkadapter 2 auf VM Netzwerk 2 konfiguriert:
  - Verwenden Sie das VM-Netzwerk 2 und fügen Sie ein VMXnet3 (10 Gbit/s) hinzu, mit dem eine Verbindung hergestellt werden soll. AWS

Hinzufügen von Ressourcen zu Ihrem Gateway

Die folgenden Engpässe können die Leistung Ihres Tape Gateway unter den theoretischen maximalen Dauerdurchsatz (Ihre Bandbreite zur AWS Cloud) reduzieren:

- Anzahl CPU-Kerne
- Durchsatz der Cache-/Upload-Puffer-Festplatte
- RAM-Gesamtgröße
- Netzwerkbandbreite bis 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

  Um die Gateway-Leistung zu optimieren, können Sie Hochleistungsfestplatten wie Solid-State-Laufwerke (SSDs) und einen NVMe Controller hinzufügen. Sie können auch virtuelle Festplatten direkt von einem Storage Area Network (SAN) anstelle des Microsoft Hyper-V NTFS, zu Ihrer VM hinzufügen. Verbesserte Festplattenleistung führt in der Regel zu höherem Durchsatz und zu mehr Eingabe-/Ausgabevorgängen pro Sekunde (IOPS).

  Verwenden Sie zur Messung des Durchsatzes die `WriteBytes` Metriken `ReadBytes` und zusammen mit der `Samples` CloudWatch Amazon-Statistik. Beispiel: Mit dem `Samples` Statistik der `ReadBytes` Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie die IOPS. Allgemein gilt, wenn Sie diese Metriken für ein Gateway überprüfen, suchen Sie nach niedrigem Durchsatz und niedrigen IOPS.-Trends um Engpässe im Zusammenhang mit Datenträgern angeben zu können. Weitere Informationen zu Gateway-Metriken, finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

  > **Note**
  >
  > CloudWatch Metriken sind nicht für alle Gateways verfügbar. Weitere Informationen, zu Gateway Metriken, finden Sie unter Überwachen von Storage Gateway.

Hinzufügen von weiteren Upload-Puffer-Festplatten

Um einen höheren Schreibdurchsatz zu erreichen, fügen Sie mindestens zwei Upload-Puffer-Festplatten hinzu. Werden Daten auf das Gateway geschrieben, werden sie lokal auf die Upload-Puffer-Festplatten geschrieben und dort gespeichert. Danach werden die gespeicherten lokalen Daten asynchron von den Festplatten gelesen, um sie zu verarbeiten und in AWS hochzuladen. Wenn weitere Upload-Puffer-Festplatten hinzugefügt werden, kann dies die Anzahl der gleichzeitigen I/O-Vorgänge auf den einzelnen Festplatten verringern. Dies kann zu einem erhöhten Schreibdurchsatz für das Gateway führen.

Sichern von virtuellen Gateway-Festplatten mit getrennten physischen Datenträgern

Bei der Bereitstellung von Gateway-Datenträgern wird dringend empfohlen, keine lokalen Festplatten für den Upload-Puffer und Cache-Speicher bereitzustellen, die die gleiche zugrunde liegende physische Speicherressource verwenden. Beispielsweise VMware ESXi werden die zugrunde liegenden physischen Speicherressourcen als Datenspeicher dargestellt. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-Dateien.

Wenn Sie eine virtuelle Festplatte bereitstellen (z. B. als Upload-Puffer), können Sie die virtuelle Festplatte im gleichen Datenspeicher wie die VM oder in einem anderen Datenspeicher speichern.

Wenn Sie über mehr als einen Datenspeicher verfügen, sollten Sie unbedingt einen Datenspeicher für jeden Typ von lokalem Speicher wählen, den sie erstellen. Ein Datenspeicher, der nur durch einen einzigen zugrunde liegenden physischen Datenträger gestützt wird, kann zu einer schlechten Leistung führen. Beispielsweise wenn Sie solch einen Datenträger sowohl zum Stützen des Cache-Speichers als auch des Upload-Puffers in einer Gateway-Konfiguration verwenden. Dementsprechend kann auch ein Datenspeicher, der durch eine leistungsschwächere RAID-Konfiguration gestützt wird, wie z. B. RAID 1 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 außerdem sicher, dass Sie den Host-Server nicht CPUs überlastet haben.

Wenn Sie Ihrem Gateway-Hostserver 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. Stellen Sie CPUs außerdem sicher, dass Ihr Gateway genügend CPU-Ressourcen erhält, wenn der Host mit anderen geteilt wird VMs. Über genügend CPU-Ressourcen zu verfügen hat den allgemeinen Effekt der Verbesserung des Durchsatzes.

Erhöhen der Bandbreite zwischen Ihrem Gateway und der AWS Cloud

Wenn Sie Ihre Bandbreite zu und von dort erhöhen, AWS wird die maximale Geschwindigkeit des Dateneingangs zu Ihrem Gateway und des Datenausgangs in die Cloud erhöht. AWS Dies kann die Leistung Ihres Gateways verbessern, wenn die Netzwerkgeschwindigkeit der begrenzende Faktor in Ihrer Gateway-Konfiguration ist und nicht andere Faktoren wie langsame Festplatten oder eine mangelhafte Bandbreite der Verbindung zwischen Gateway und Initiator.

Die Netzwerkbandbreite von und zu AWS definiert die theoretische maximale Durchschnittsleistung Ihres Tape Gateways bei anhaltenden Workloads.

- Die durchschnittliche Geschwindigkeit, mit der Sie über lange Zeiträume Daten auf Ihr Tape Gateway schreiben können, wird Ihre Upload-Bandbreite zu AWS nicht überschreiten.
- Die durchschnittliche Geschwindigkeit, mit der Sie über lange Zeiträume Daten von Ihrem Tape Gateway lesen können, wird Ihre Download-Bandbreite nicht überschreiten. AWS

> **Note**
>
> Die beobachtete Gateway-Leistung wird wahrscheinlich geringer sein als die Netzwerkbandbreite. Dies ist auf andere hier aufgeführte einschränkende Faktoren zurückzuführen, wie z. B. den Durchsatz der Cache/Upload-Puffer-Festplatte, die Anzahl der CPU-Kerne, die RAM-Gesamtgröße oder die Bandbreite zwischen Ihrem Initiator und dem Gateway. Darüber hinaus umfasst der normale Betrieb Ihres Gateways viele Maßnahmen zum Schutz Ihrer Daten, was dazu führen kann, dass die beobachtete Leistung geringer als die Netzwerkbandbreite ist.

Optimieren von iSCSI-Einstellungen

Sie können die iSCSI-Einstellungen auf Ihrem iSCSI-Initiator optimieren, um eine höhere E/A-Leistung zu erzielen. Wir empfehlen die Auswahl von 256 KiB für `MaxReceiveDataSegmentLength` und `FirstBurstLength` sowie von 1 MiB für `MaxBurstLength`. Weitere Hinweise zum Konfigurieren von iSCSI-Einstellungen finden Sie unter Anpassen von iSCSI-Einstellungen.

> **Note**
>
> Diese empfohlenen Einstellungen können eine insgesamt bessere Leistung ermöglichen. Die spezifischen iSCSI-Einstellungen, die zur Leistungsoptimierung erforderlich sind, variieren jedoch je nach verwendeter Backup-Software. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Backup-Software.

Verwenden Sie eine größere Blockgröße für Bandlaufwerke

Bei einem Tape Gateway beträgt die Standardblockgröße für ein Bandlaufwerk 64 KB. Sie können jedoch die Blockgröße auf bis zu 1 MB erhöhen, um die E/A-Leistung zu verbessern.

Die von Ihnen gewählte Blockgröße hängt von der maximalen Blockgröße ab, die Ihre Sicherungssoftware unterstützt. Es wird empfohlen, in Ihrer Sicherungssoftware die größtmögliche Blockgröße für Bandlaufwerke festzulegen. Allerdings darf diese Blockgröße nicht größer sein der Höchstwert von 1 MB, den das Gateway unterstützt.

Tape Gateways handeln die Blockgröße für virtuelle Bandlaufwerke so aus, dass sie automatisch mit der Einstellung in der Sicherungssoftware übereinstimmen. Wenn Sie die Blockgröße in der Sicherungssoftware erhöhen, wird empfohlen, bei den Einstellungen zu überprüfen, ob der Host-Initiator die neue Blockgröße unterstützt. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Sicherungssoftware. Weitere Informationen zu spezifischen Anleitungen für die Gateway-Leistung finden Sie unter Leistung und Optimierung für Tape Gateway.

Optimieren der Leistung von virtuellen Bandlaufwerken in der Sicherungssoftware

Ihre Sicherungssoftware kann auf bis zu 10 virtuellen Bandlaufwerken in einem Tape Gateway gleichzeitig Daten sichern. Wir empfehlen, dass Sie Sicherungsaufträge in Ihrer Sicherungssoftware konfigurieren, bei denen mindestens vier (4) virtuelle Bandlaufwerke gleichzeitig im Tape Gateway verwendet werden. Es lässt sich ein besserer Schreibdurchsatz erreichen, wenn die Sicherungssoftware die Daten auf mehreren virtuellen Bändern gleichzeitig sichert.

In der Regel können Sie einen höheren maximalen Durchsatz erreichen, wenn Sie mit mehr virtuellen Bändern gleichzeitig arbeiten (lesen oder schreiben). Wenn Sie mehr Bandlaufwerke verwenden, kann Ihr Gateway mehr Anforderungen gleichzeitig bearbeiten, wodurch möglicherweise die Leistung verbessert wird.

Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung

Erhöhen der Bandbreite zwischen Ihrem Anwendungsserver und Ihrem Gateway

Die Verbindung zwischen Ihrem iSCSI-Initiator und dem Gateway kann die Upload- und Download-Leistung einschränken. Wenn Ihr Gateway eine deutlich schlechtere Leistung als erwartet aufweist und Sie die Anzahl der CPU-Kerne und den Festplattendurchsatz bereits verbessert haben, sollten Sie Folgendes in Betracht ziehen:

- Rüsten Sie Ihre Netzwerkkabel auf, um eine höhere Bandbreite zwischen Ihrem Initiator und dem Gateway zu erreichen.
- Verwenden Sie so viele Bandlaufwerke wie möglich gleichzeitig. iSCSI unterstützt keine Warteschlangenbildung für mehrere Anforderungen für dasselbe Ziel. Daher gilt, je mehr Bandlaufwerke Sie verwenden, desto mehr Anforderungen kann Ihr Gateway gleichzeitig bedienen. Auf diese Weise können Sie die Bandbreite zwischen Ihrem Gateway und dem Initiator besser nutzen und den scheinbaren Durchsatz Ihres Gateways erhöhen.

Zum Optimieren der Gateway-Leistung, stellen Sie sicher, dass die Netzwerkbandbreite zwischen Ihrer Anwendung und dem Gateway, Ihre Anwendungsansprüche unterstützen kann. Sie können die Metriken `ReadBytes` und `WriteBytes` des Gateways verwenden, um den gesamten Datendurchsatz zu messen. Weitere Informationen zu diesen Metriken finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

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

Hinzufügen von CPU-Ressourcen zu Ihrer Anwendungsumgebung

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

Sicherheit im AWS Storage Gateway

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der Amazon Web Services Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AWS Storage Gateway gelten, finden Sie unter AWS Services in Scope by Compliance Program AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Storage Gateway angewendet werden kann. Die folgenden Themen veranschaulichen, wie Sie Storage Gateway konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Storage Gateway Gateway-Ressourcen zu überwachen und zu sichern.

Themen

- Datenschutz in AWS Storage Gateway
- Identity and Access Management für AWS Storage Gateway
- Compliance-Validierung für AWS Storage Gateway
- Resilienz im AWS Storage Gateway
- Infrastructure Security in AWS Storage Gateway
- AWS Bewährte Methoden im Bereich Sicherheit
- Einloggen und Überwachen AWS Storage Gateway

Datenschutz in AWS Storage Gateway

Das AWS Modell der mit gilt für den Datenschutz in AWS Storage Gateway. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Storage Gateway oder anderen Geräten arbeiten und die Konsole, die API oder AWS-Services verwenden AWS SDKs. AWS CLI Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung mit AWS KMS

Storage Gateway verwendet SSL/TLS (Secure Socket Layers/Transport Layer Security (), um Daten zu verschlüsseln, die zwischen Ihrer Gateway-Appliance und dem AWS Speicher übertragen werden. 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 Gateway-API zu verwenden, um Ihr Gateway so zu konfigurieren, dass in der Cloud gespeicherte Daten mithilfe 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 wählen. Storage Gateway unterstützt keine asymmetrischen Schlüssel. Weitere Informationen finden Sie unter Using Symmetric and Asymmetric Keys (Verwenden von symmetrischen und asymmetrischen Schlüsseln) im AWS Key Management Service -Benutzerhandbuch.

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 Gateway-API zum Verschlüsseln von Daten, die in eine Dateifreigabe geschrieben wurden, finden Sie unter Create NFSFile Share in der AWS Storage Gateway API-Referenz.

Verschlüsseln eines Volumes

Für zwischengespeicherte und gespeicherte Volumes können Sie Ihr Gateway so konfigurieren, dass in der Cloud gespeicherte Volumendaten mithilfe der Storage Gateway AWS KMS Gateway-API mit verwalteten Schlüsseln verschlüsselt werden. 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 Gateway-API zur Verschlüsselung von Daten, die auf ein zwischengespeichertes oder gespeichertes Volume geschrieben wurden, finden Sie unter CreateCachediSCSIVolumeoder CreateStorediSCSIVolumein der AWS Storage Gateway API-Referenz.

Verschlüsseln eines Bands

Für ein virtuelles Band können Sie Ihr Gateway so konfigurieren, dass in der Cloud gespeicherte Banddaten mithilfe der Storage Gateway AWS KMS Gateway-API mit verwalteten Schlüsseln verschlüsselt werden. 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 Gateway-API zur Verschlüsselung von Daten, die auf ein virtuelles Band geschrieben wurden, finden Sie CreateTapesin der AWS Storage Gateway API-Referenz.

Beachten AWS KMS Sie bei der Verschlüsselung Ihrer Daten Folgendes:

- Ihre Daten werden im Ruhezustand in der Cloud verschlüsselt. Das bedeutet, dass die Daten in Amazon S3 verschlüsselt werden.
- IAM-Benutzer müssen über die erforderlichen Berechtigungen verfügen, um die AWS KMS API-Operationen aufrufen zu können. Weitere Informationen finden Sie unter Verwenden von IAM-Richtlinien mit AWS KMS im Entwicklerhandbuch zu AWS Key Management Service .
- Wenn Sie Ihren AWS AWS KMS Schlüssel löschen oder deaktivieren oder das Grant-Token widerrufen, können Sie nicht auf die Daten auf dem Volume oder Band zugreifen. Weitere Informationen finden Sie unter Löschen von KMS-Schlüsseln im Entwicklerhandbuch zu AWS Key Management Service .
- Wenn Sie einen Snapshot von einem Volume erstellen, das KMS-verschlüsselt ist, wird der Snapshot verschlüsselt. Der Snapshot erbt den KMS-Schlüssel des Volumes.
- Wenn Sie ein neues Volume aus einem KMS-verschlüsselten Snapshot erstellen, wird der Snapshot verschlüsselt. Sie können einen anderen KMS-Schlüssel für das neue Volume angeben.

> **Note**
>
> Storage Gateway unterstützt derzeit nicht das Erstellen eines unverschlüsselten Volumes von einem Wiederherstellungspunkt eines KMS-verschlüsselten Volumes oder eines KMS-verschlüsselten Snapshots.

Weitere Informationen zu AWS KMS finden Sie unter Was ist AWS Key Management Service?

Identity and Access Management für AWS Storage Gateway

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um SGW-Ressourcen zu verwenden AWS . IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert AWS Storage Gateway mit IAM
- Beispiele für identitätsbasierte Richtlinien für Storage Gateway
- Fehlerbehebung bei Identität und Zugriff auf AWS Storage Gateway

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in AWS SGW ausführen.

Dienstbenutzer — Wenn Sie den AWS SGW-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS SGW-Funktionen verwenden, 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 bei Identität und Zugriff auf AWS Storage Gateway finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS SGW haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS SGW-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff AWS auf SGW. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS SGW-Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die

Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit AWS SGW nutzen kann, finden Sie unter. So funktioniert AWS Storage Gateway mit IAM

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf SGW schreiben können. AWS Beispiele für identitätsbasierte AWS SGW-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Storage Gateway

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die 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 AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, 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. Verwenden Sie diese nur, 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

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf 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 Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten 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 innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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 Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. 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 auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst 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.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein

Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 von der AWS Management Console AWS CLI, der 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

Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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

Zugriffskontrolllisten () ACLs

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

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete 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.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) 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 darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert AWS Storage Gateway mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf AWS SGW verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen mit SGW verwendet werden können. AWS

IAM-Funktionen, die Sie mit AWS Storage Gateway verwenden können

IAM-Feature	AWS SGW-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja

IAM-Feature	AWS SGW-Unterstützung
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

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

Identitätsbasierte Richtlinien für SGW AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. 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 SGW AWS

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

Ressourcenbasierte Richtlinien innerhalb von SGW AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für SGW AWS

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. 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 Authorization Reference.

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

```
sgw
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

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

Politische Ressourcen für SGW AWS

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. 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 Eigenschaften finden Sie unter Von AWS Storage Gateway definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Storage Gateway definierte Aktionen.

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

Bedingungsschlüssel für Richtlinien für SGW AWS

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS SGW-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Storage Gateway in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Storage Gateway definierte Aktionen.

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

ACLs AWS in SGW

Unterstützt ACLs: Nein

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

ABAC mit SGW AWS

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit SGW AWS

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären

Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. 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 von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen für AWS SGW weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst 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.

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**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS SGW-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AWS SGW Sie dazu anleitet.

Servicebezogene Rollen für SGW AWS

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Storage Gateway

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS SGW-Ressourcen zu erstellen oder zu ändern. 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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS SGW definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Storage Gateway in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der SGW-Konsole AWS
- 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:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue

und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der SGW-Konsole AWS

Um auf die AWS Storage Gateway Gateway-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS SGW-Ressourcen in Ihrem AWS-Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS SGW-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS SGW `ConsoleAccess` - oder `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der OR-API. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Fehlerbehebung bei Identität und Zugriff auf AWS Storage Gateway

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS SGW und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in SGW durchzuführen AWS

- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS SGW-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in SGW durchzuführen AWS

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `sgw:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `sgw:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Durchführung der `iam:PassRole` Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AWS SGW übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS SGW auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

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

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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS SGW diese Funktionen unterstützt, finden Sie unter. So funktioniert AWS Storage Gateway mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Compliance-Validierung für AWS Storage Gateway

Externe Prüfer bewerten die Sicherheit und Konformität von AWS Storage Gateway im Rahmen mehrerer AWS Compliance-Programme. Dazu gehören SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR und HITRUST CSF.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS . Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Compliance-Verantwortung bei der Verwendung von Storage Gateway wird durch die Sensibilität Ihrer Daten, die Compliance-Ziele Ihres Unternehmens und die geltenden Gesetze und Vorschriften bestimmt. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Schnellstartanleitungen zu Sicherheit und Compliance Schnellstartanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Implementierung von sicherheits- und Compliance-orientierten Basisumgebungen beschrieben. AWS
- Whitepaper „Architecting for HIPAA Security and Compliance“ — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen entwickeln können. AWS
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen können AWS , ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Resilienz im AWS Storage Gateway

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones.

An AWS-Region ist ein physischer Standort auf der ganzen Welt, an dem Rechenzentren gebündelt sind. Jede Gruppe logischer Rechenzentren wird als Availability Zone (AZ) bezeichnet. Jedes AWS-Region besteht aus mindestens drei isolierten und physisch getrennten Einheiten AZs innerhalb eines geografischen Gebiets. Im Gegensatz zu anderen Cloud-Anbietern, die eine Region häufig als ein einzelnes Rechenzentrum definieren, AWS-Region bietet das Design mit mehreren AZ-Anschlüssen deutliche Vorteile. Jede AZ verfügt über unabhängige Stromversorgung, Kühlung und physische Sicherheit und ist über redundante ultra-low-latency Netzwerke verbunden. Wenn

Ihre Bereitstellung einen Schwerpunkt auf Hochverfügbarkeit erfordert, können Sie Dienste und Ressourcen so konfigurieren, dass mehrere Dienste und Ressourcen verfügbar sind, AZs um eine höhere Fehlertoleranz zu erreichen.

AWS-Regionen erfüllen die höchsten Standards in Bezug auf Infrastruktursicherheit, Compliance und Datenschutz. Der gesamte Verkehr zwischen beiden AZs ist verschlüsselt. Die Netzwerkleistung reicht aus, um eine synchrone Replikation zwischen AZs zu erreichen. AZs vereinfacht die Partitionierung von Diensten und Ressourcen für hohe Verfügbarkeit. Wenn Ihre Bereitstellung übergreifend partitioniert ist AZs, sind Ihre Ressourcen besser isoliert und vor Problemen wie Stromausfällen, Blitzeinschlägen, Tornados, Erdbeben und mehr geschützt. AZs sind physisch durch eine nennenswerte Entfernung von allen anderen AZ getrennt, obwohl sich alle innerhalb von 100 km (60 Meilen) voneinander befinden.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Storage Gateway mehrere Funktionen, mit denen Sie Ihre Anforderungen an Datenstabilität und Backup erfüllen können:

- Verwenden Sie VMware vSphere High Availability (VMware HA), um Speicher-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen zu schützen. Weitere Informationen finden Sie unter Verwenden von VMware vSphere High Availability mit Storage Gateway.
- Archivieren Sie virtuelle Bänder in S3 Glacier Flexible Retrieval. Weitere Informationen finden Sie unter Archivierung virtueller Bänder.

Infrastructure Security in AWS Storage Gateway

Als verwalteter Service ist AWS Storage Gateway durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Storage Gateway zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.2 unterstützen. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS

Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

> **Note**
>
> Sie sollten die AWS Storage Gateway Gateway-Appliance wie eine verwaltete virtuelle Maschine behandeln und nicht versuchen, auf ihre Installation zuzugreifen oder sie in irgendeiner Weise zu ändern. Der Versuch, Scansoftware zu installieren oder Softwarepakete mit anderen Methoden als dem normalen Gateway-Aktualisierungsmechanismus zu aktualisieren, kann zu Fehlfunktionen des Gateways führen und unsere Fähigkeit, das Gateway zu unterstützen oder zu reparieren, beeinträchtigen.
> AWS überprüft, analysiert und behebt CVEs regelmäßig Abhilfemaßnahmen. Im Rahmen unseres normalen Softwareveröffentlichungszyklus integrieren wir Korrekturen für diese Probleme in Storage Gateway. Diese Fixes werden in der Regel als Teil des normalen Gateway-Aktualisierungsprozesses während planmäßiger Wartungsfenster angewendet. Weitere Informationen zu Gateway-Updates finden Sie unter verwalten.

AWS Bewährte Methoden im Bereich 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.

Einloggen und Überwachen AWS Storage Gateway

Storage Gateway ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Storage Gateway ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Storage Gateway als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Storage-Gateway-Konsole und Code-Aufrufe der Storage-Gateway-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Storage Gateway. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von

gesammelten Informationen können Sie die Anfrage CloudTrail, die an Storage Gateway gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Storage Gateway Gateway-Informationen in CloudTrail

CloudTrail ist in Ihrem Amazon Web Services Services-Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität in Storage Gateway auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Dienstereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihrem Amazon Web Services-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

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 Übertragung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Storage-Gateway-Aktionen werden protokolliert und im Thema Aktionen dokumentiert. Beispielsweise generieren Aufrufe der `ShutdownGateway` Aktionen `ActivateGatewayListGateways`, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Informationen zu Storage-Gateway-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die Aktion demonstriert.

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
```

```
                                                    "responseElements": {
                                                                        "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                                    },
                                                    "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                                    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                                    "eventType": "AwsApiCall",
                                                    "apiVersion": "20130630",
                                                    "recipientAccountId": "444455556666"
            }]
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die ListGateways Aktion demonstriert.

```
{
 "Records": [{
              "eventVersion": "1.02",
              "userIdentity": {
                               "type": "IAMUser",
                               "principalId": "AIDAII5AUEPBH2M7JTNVC",
                               "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                               "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                               " userName ":" JohnDoe "
                               },

                               " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                               " eventSource ":" storagegateway.amazonaws.com ",
                               " eventName ":" ListGateways ",
                               " awsRegion ":" us-east-2 ",
                               " sourceIPAddress ":" 192.0.2.0 ",
                               " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                               " requestParameters ":null,
                               " responseElements ":null,
                               "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                               " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
```

```
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
            }]
}
```

Fehlerbehebung bei Ihrem Gateway

Im Folgenden finden Sie Informationen zu bewährten Methoden und zur Behebung von Problemen im Zusammenhang mit Gateways, Hostplattformen, virtuellen Bändern, Hochverfügbarkeit, Datenwiederherstellung und Sicherheit. Die Informationen zur Fehlerbehebung bei lokalen Gateways beziehen sich auf Gateways, die auf unterstützten Virtualisierungsplattformen eingesetzt werden. Die Informationen zur Fehlerbehebung bei Hochverfügbarkeitsproblemen beziehen sich auf Gateways, die auf der VMware vSphere High Availability (HA) -Plattform ausgeführt werden.

Topics

- Fehlerbehebung: Gateway-Offline-Probleme- Erfahren Sie, wie Sie Probleme diagnostizieren, die dazu führen können, dass Ihr Gateway in der Storage Gateway Gateway-Konsole als offline angezeigt wird.
- Problembehandlung: interner Fehler bei der Gateway-Aktivierung- Erfahren Sie, wie Sie vorgehen, wenn Sie beim Versuch, Ihr Storage Gateway zu aktivieren, eine interne Fehlermeldung erhalten.
- Fehlerbehebung bei lokalen Gateway-Problemen- Erfahren Sie mehr über typische Probleme, die bei der Arbeit mit Ihren lokalen Gateways auftreten können, und darüber, wie Sie eine Verbindung zu Ihrem Gateway herstellen können Support , um Sie bei der Fehlerbehebung zu unterstützen.
- Fehlerbehebung bei der Einrichtung von Microsoft Hyper-V- Erfahren Sie mehr über typische Probleme, die bei der Bereitstellung von Storage Gateway auf der Microsoft Hyper-V-Plattform auftreten können.
- Behebung von Problemen mit Amazon EC2 Gateway- Hier finden Sie Informationen zu typischen Problemen, die bei der Arbeit mit auf Amazon EC2 bereitgestellten Gateways auftreten können.
- Fehlerbehebung bei Hardware-Appliance-Problemen- Erfahren Sie, wie Sie Probleme lösen können, die möglicherweise mit der Storage Gateway Gateway-Hardware-Appliance auftreten.
- Beheben von Problemen mit virtuellen Bändern- Erfahren Sie, welche Maßnahmen Sie ergreifen können, wenn unerwartete Probleme mit Ihren virtuellen Bändern auftreten.
- Beheben von Problemen mit Hochverfügbarkeit- Erfahren Sie, wie Sie vorgehen können, wenn Probleme mit Gateways auftreten, die in einer VMware HA-Umgebung eingesetzt werden.

Fehlerbehebung: Gateway-Offline-Probleme

Ermitteln Sie anhand der folgenden Informationen zur Fehlerbehebung, was zu tun ist, wenn die AWS Storage Gateway Konsole anzeigt, dass Ihr Gateway offline ist.

Ihr Gateway wird möglicherweise aus einem oder mehreren der folgenden Gründe als offline angezeigt:

- Das Gateway kann die Storage Gateway-Dienstendpunkte nicht erreichen.
- Das Gateway wurde unerwartet heruntergefahren.
- Eine dem Gateway zugeordnete Cache-Festplatte wurde getrennt oder geändert oder ist ausgefallen.

Um Ihr Gateway wieder online zu schalten, identifizieren und beheben Sie das Problem, das dazu geführt hat, dass Ihr Gateway offline gegangen ist.

Überprüfen Sie die zugehörige Firewall oder den zugehörigen Proxy

Wenn Sie Ihr Gateway für die Verwendung eines Proxys konfiguriert haben oder Ihr Gateway hinter einer Firewall platziert haben, überprüfen Sie die Zugriffsregeln des Proxys oder der Firewall. Der Proxy oder die Firewall muss den Datenverkehr zu und von den Netzwerkports und Dienstendpunkten zulassen, die von Storage Gateway benötigt werden. Weitere Informationen finden Sie unter Netzwerk- und Firewallanforderungen .

Suchen Sie nach einer laufenden SSL- oder Deep-Packet-Inspektion des Datenverkehrs Ihres Gateways

Wenn derzeit eine SSL- oder Deep-Packet-Inspection für den Netzwerkverkehr zwischen Ihrem Gateway und durchgeführt wird AWS, kann Ihr Gateway möglicherweise nicht mit den erforderlichen Service-Endpunkten kommunizieren. Um Ihr Gateway wieder online zu schalten, müssen Sie die Inspektion deaktivieren.

Suchen Sie nach einem Strom- oder Hardwarefehler auf dem Hypervisor-Host

Ein Strom- oder Hardwarefehler auf dem Hypervisor-Host Ihres Gateways kann dazu führen, dass Ihr Gateway unerwartet heruntergefahren wird und nicht mehr erreichbar ist. Nachdem Sie die Stromversorgung und die Netzwerkkonnektivität wiederhergestellt haben, ist Ihr Gateway wieder erreichbar.

Nachdem Ihr Gateway wieder online ist, sollten Sie unbedingt Maßnahmen ergreifen, um Ihre Daten wiederherzustellen. Weitere Informationen finden Sie unter Bewährte Methoden für die Wiederherstellung Ihrer Daten .

Suchen Sie nach Problemen mit einer zugehörigen Cache-Festplatte

Ihr Gateway kann offline gehen, wenn mindestens eine der mit Ihrem Gateway verbundenen Cache-Festplatten entfernt, geändert oder in der Größe geändert wurde oder wenn sie beschädigt ist.

Wenn eine funktionierende Cache-Festplatte vom Hypervisor-Host entfernt wurde:

1. Fahren Sie das Gateway herunter.
2. Fügen Sie die Festplatte erneut hinzu.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie die Festplatte demselben Festplattenknoten hinzufügen.

3. Starten Sie Ihr Gateway neu.

Wenn ein Cache-Laufwerk beschädigt ist, ersetzt wurde oder dessen Größe geändert wurde:

1. Fahren Sie das Gateway herunter.
2. Setzen Sie die Cache-Festplatte zurück.
3. Konfigurieren Sie die Festplatte für den Cache-Speicher neu.
4. Starten Sie Ihr Gateway neu.

Weitere Informationen zur Behebung einer beschädigten Cache-Festplatte für ein Band-Gateway finden Sie unter Sie müssen ein virtuelles Band von einer defekten Cache-Festplatte wiederherstellen.

Problembehandlung: interner Fehler bei der Gateway-Aktivierung

Storage Gateway Gateway-Aktivierungsanforderungen durchlaufen zwei Netzwerkpfade. Eingehende Aktivierungsanfragen, die von einem Client gesendet werden, stellen über Port 80 eine Verbindung zur virtuellen Maschine (VM) oder Amazon Elastic Compute Cloud (Amazon EC2) -Instance des Gateways her. Wenn das Gateway die Aktivierungsanfrage erfolgreich empfängt, kommuniziert das Gateway mit den Storage Gateway Gateway-Endpunkten, um einen Aktivierungsschlüssel zu erhalten. Wenn das Gateway die Storage Gateway Gateway-Endpunkte nicht erreichen kann, antwortet das Gateway dem Client mit einer internen Fehlermeldung.

Verwenden Sie die folgenden Informationen zur Fehlerbehebung, um zu ermitteln, was zu tun ist, wenn Sie beim Versuch, Ihren AWS Storage Gateway zu aktivieren, eine interne Fehlermeldung erhalten.

> **Note**
>
> - Stellen Sie sicher, dass Sie neue Gateways mit der neuesten Image-Datei für virtuelle Maschinen oder der neuesten Version von Amazon Machine Image (AMI) bereitstellen. Sie erhalten einen internen Fehler, wenn Sie versuchen, ein Gateway zu aktivieren, das ein veraltetes AMI verwendet.
> - Stellen Sie sicher, dass Sie den richtigen Gateway-Typ auswählen, den Sie bereitstellen möchten, bevor Sie das AMI herunterladen. Die OVA-Dateien AMIs für jeden Gateway-Typ sind unterschiedlich und nicht austauschbar.

Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt

Um Aktivierungsfehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt zu beheben, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Überprüfen Sie die erforderlichen Ports

Vergewissern Sie sich bei Gateways, die vor Ort bereitgestellt werden, dass die Ports auf Ihrer lokalen Firewall geöffnet sind. Überprüfen Sie bei Gateways, die auf einer EC2 Amazon-Instance bereitgestellt werden, ob die Ports in der Sicherheitsgruppe der Instance geöffnet sind. Um zu überprüfen, ob die Ports geöffnet sind, führen Sie auf dem öffentlichen Endpunkt von einem Server aus einen Telnet-Befehl aus. Dieser Server muss sich im selben Subnetz wie das Gateway befinden. Mit den folgenden Telnet-Befehlen wird beispielsweise die Verbindung zu Port 443 getestet:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Um zu überprüfen, ob das Gateway selbst den Endpunkt erreichen kann, greifen Sie auf die lokale VM-Konsole des Gateways zu (für lokal bereitgestellte Gateways). Oder Sie können eine SSH-Verbindung zur Gateway-Instance herstellen (für Gateways, die auf Amazon EC2 bereitgestellt werden). Führen Sie dann einen Netzwerkverbindungstest durch. Vergewissern Sie sich, dass der Test zurückkehrt`[PASSED]`. Weitere Informationen finden Sie unter Testen Ihrer Gateway-Verbindung mit dem Internet .

> **Note**
>
> Der Standard-Anmeldename für die Gateway-Konsole lautet`admin`, und das Standardkennwort ist`password`.

Stellen Sie sicher, dass die Firewall-Sicherheit keine Pakete verändert, die vom Gateway an die öffentlichen Endpunkte gesendet werden

SSL-Inspektionen, Deep Packet Inspections oder andere Formen der Firewall-Sicherheit können die vom Gateway gesendeten Pakete beeinträchtigen. Der SSL-Handshake schlägt fehl, wenn das SSL-Zertifikat so geändert wird, wie es der Aktivierungsendpunkt erwartet. Um sicherzustellen, dass keine SSL-Inspektion im Gange ist, führen Sie einen OpenSSL-Befehl auf dem Hauptaktivierungsendpunkt (`anon-cp.storagegateway.region.amazonaws.com`) an Port 443 aus. Sie müssen diesen Befehl von einem Computer aus ausführen, der sich im selben Subnetz wie das Gateway befindet:

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Ersetze es *`region`* durch dein AWS-Region.

Wenn keine SSL-Überprüfung im Gange ist, gibt der Befehl eine Antwort zurück, die der folgenden ähnelt:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
```

```
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Wenn eine laufende SSL-Inspektion stattfindet, zeigt die Antwort eine veränderte Zertifikatskette, die der folgenden ähnelt:

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

Der Aktivierungsendpunkt akzeptiert SSL-Handshakes nur, wenn er das SSL-Zertifikat erkennt. Das bedeutet, dass der ausgehende Datenverkehr des Gateways zu den Endpunkten von Inspektionen ausgenommen werden muss, die von Firewalls in Ihrem Netzwerk durchgeführt werden. Bei diesen Inspektionen kann es sich um eine SSL-Inspektion oder eine Deep Packet Inspection handeln.

Überprüfen Sie die Gateway-Zeitsynchronisierung

Übermäßige Zeitverschiebungen können zu SSL-Handshake-Fehlern führen. Bei lokalen Gateways können Sie die lokale VM-Konsole des Gateways verwenden, um die Zeitsynchronisierung Ihres Gateways zu überprüfen. Der Zeitversatz sollte nicht größer als 60 Sekunden sein.

Die Option System Time Management ist auf Gateways, die auf EC2 Amazon-Instances gehostet werden, nicht verfügbar. Um sicherzustellen, dass EC2 Amazon-Gateways die Zeit ordnungsgemäß synchronisieren können, stellen Sie sicher, dass die EC2 Amazon-Instance über die Ports UDP und TCP 123 eine Verbindung zur folgenden NTP-Serverpool-Liste herstellen kann:

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

Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen Amazon VPC-Endpunkt

Um Aktivierungsfehler bei der Aktivierung Ihres Gateways über einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt zu beheben, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Überprüfen Sie die erforderlichen Ports

Stellen Sie sicher, dass die erforderlichen Ports innerhalb Ihrer lokalen Firewall (für lokal bereitgestellte Gateways) oder Sicherheitsgruppe (für in Amazon bereitgestellte Gateways EC2) geöffnet sind. Die Ports, die für die Verbindung eines Gateways mit einem Storage Gateway Gateway-VPC-Endpunkt erforderlich sind, unterscheiden sich von denen, die für die Verbindung eines Gateways mit öffentlichen Endpunkten erforderlich sind. Die folgenden Ports sind für die Verbindung mit einem Storage Gateway Gateway-VPC-Endpunkt erforderlich:

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

- TCP 2222

Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts für Storage Gateway für Storage Gateway.

Überprüfen Sie außerdem die Sicherheitsgruppe, die an Ihren Storage Gateway Gateway-VPC-Endpunkt angehängt ist. Die dem Endpunkt zugeordnete Standardsicherheitsgruppe lässt möglicherweise nicht die erforderlichen Ports zu. Erstellen Sie eine neue Sicherheitsgruppe, die Datenverkehr aus dem IP-Adressbereich Ihres Gateways über die erforderlichen Ports zulässt. Fügen Sie dann diese Sicherheitsgruppe dem VPC-Endpunkt hinzu.

> **Note**
>
> Verwenden Sie die Amazon VPC-Konsole, um die Sicherheitsgruppe zu überprüfen, die mit dem VPC-Endpunkt verbunden ist. Sehen Sie sich Ihren Storage Gateway Gateway-VPC-Endpunkt von der Konsole aus an und wählen Sie dann die Registerkarte Sicherheitsgruppen aus.

Um zu überprüfen, ob die erforderlichen Ports geöffnet sind, können Sie Telnet-Befehle auf dem Storage Gateway Gateway-VPC-Endpunkt ausführen. Sie müssen diese Befehle von einem Server aus ausführen, der sich im selben Subnetz wie das Gateway befindet. Sie können die Tests für den ersten DNS-Namen ausführen, der keine Availability Zone angibt. Mit den folgenden Telnet-Befehlen werden beispielsweise die erforderlichen Portverbindungen mithilfe des DNS-Namens vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com getestet:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Stellen Sie sicher, dass die Firewall-Sicherheit keine Pakete verändert, die vom Gateway an Ihren Storage Gateway Amazon VPC-Endpunkt gesendet werden.

SSL-Inspektionen, Deep Packet Inspections oder andere Formen der Firewall-Sicherheit können die vom Gateway gesendeten Pakete beeinträchtigen. Der SSL-Handshake schlägt fehl, wenn das

SSL-Zertifikat so geändert wird, wie es der Aktivierungsendpunkt erwartet. Um sicherzustellen, dass keine SSL-Inspektion im Gange ist, führen Sie einen OpenSSL-Befehl auf Ihrem Storage Gateway Gateway-VPC-Endpunkt aus. Sie müssen diesen Befehl von einem Computer aus ausführen, der sich im selben Subnetz wie das Gateway befindet. Führen Sie den Befehl für jeden erforderlichen Port aus:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Wenn keine SSL-Überprüfung durchgeführt wird, gibt der Befehl eine Antwort zurück, die der folgenden ähnelt:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
```

```
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Wenn eine laufende SSL-Inspektion stattfindet, zeigt die Antwort eine veränderte Zertifikatskette, die der folgenden ähnelt:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

Der Aktivierungsendpunkt akzeptiert SSL-Handshakes nur, wenn er das SSL-Zertifikat erkennt. Das bedeutet, dass der ausgehende Datenverkehr des Gateways zu Ihrem VPC-Endpunkt über die erforderlichen Ports von den Inspektionen Ihrer Netzwerk-Firewalls ausgenommen ist. Bei diesen Inspektionen kann es sich um SSL-Inspektionen oder Deep-Packet-Inspektionen handeln.

Überprüfen Sie die Gateway-Zeitsynchronisierung

Übermäßige Zeitverschiebungen können zu SSL-Handshake-Fehlern führen. Bei lokalen Gateways können Sie die lokale VM-Konsole des Gateways verwenden, um die Zeitsynchronisierung Ihres Gateways zu überprüfen. Der Zeitversatz sollte nicht größer als 60 Sekunden sein.

Die Option System Time Management ist auf Gateways, die auf EC2 Amazon-Instances gehostet werden, nicht verfügbar. Um sicherzustellen, dass EC2 Amazon-Gateways die Zeit ordnungsgemäß synchronisieren können, stellen Sie sicher, dass die EC2 Amazon-Instance über die Ports UDP und TCP 123 eine Verbindung zur folgenden NTP-Serverpool-Liste herstellen kann:

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

Suchen Sie nach einem HTTP-Proxy und bestätigen Sie die zugehörigen Sicherheitsgruppeneinstellungen

Prüfen Sie vor der Aktivierung, ob Sie einen HTTP-Proxy bei Amazon auf der lokalen Gateway-VM als Squid-Proxy auf Port 3128 EC2 konfiguriert haben. Bestätigen Sie in diesem Fall Folgendes:

- Die Sicherheitsgruppe, die an den HTTP-Proxy auf Amazon angehängt ist, EC2 muss über eine Regel für eingehenden Datenverkehr verfügen. Diese Regel für eingehenden Datenverkehr muss Squid-Proxyverkehr auf Port 3128 von der IP-Adresse der Gateway-VM aus zulassen.
- Die Sicherheitsgruppe, die dem Amazon EC2 VPC-Endpunkt zugeordnet ist, muss Regeln für eingehenden Datenverkehr haben. Diese Regeln für eingehenden Datenverkehr müssen Traffic auf den Ports 1026-1028, 1031, 2222 und 443 von der IP-Adresse des HTTP-Proxys auf Amazon zulassen. EC2

Beheben Sie Fehler, wenn Sie Ihr Gateway über einen öffentlichen Endpunkt aktivieren und es in derselben VPC einen Storage Gateway Gateway-VPC-Endpunkt gibt

Um Fehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt zu beheben, wenn sich in derselben VPC ein Amazon Virtual Private Cloud (Amazon VPC) -Endpoint befindet, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Vergewissern Sie sich, dass die Einstellung Privaten DNS-Namen aktivieren auf Ihrem Storage Gateway Gateway-VPC-Endpunkt nicht aktiviert ist

Wenn Enable Private DNS Name aktiviert ist, können Sie keine Gateways von dieser VPC zum öffentlichen Endpunkt aktivieren.

Gehen Sie wie folgt vor, um die Option für private DNS-Namen zu deaktivieren:

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Ihren Storage Gateway VPC-Endpunkt.
4. Wählen Sie Aktionen.
5. Wählen Sie Private DNS-Namen verwalten aus.
6. Deaktivieren Sie für „Privaten DNS-Namen aktivieren“ die Option „Für diesen Endpunkt aktivieren“.
7. Wählen Sie Private DNS-Namen ändern, um die Einstellung zu speichern.

Fehlerbehebung bei lokalen Gateway-Problemen

Im Folgenden finden Sie Informationen zu typischen Problemen, die bei der Arbeit mit Ihren lokalen Gateways auftreten können, sowie Informationen zur Aktivierung Support zur Behebung von Problemen mit Ihrem Gateway.

Die folgende Tabelle listet typische Probleme auf, die möglicherweise im Umgang mit Ihren lokalen Gateways auftreten.

Problem	Maßnahme
Sie können die IP-Adresse Ihrer Gateway nicht ermitteln.	Verwenden Sie den Hypervisor-Client zum Herstellen einer Verbindung mit Ihrem Host, um die Gateway-IP-Adresse zu ermitteln. • Denn VMware ESXi die IP-Adresse der VM finden Sie im vSphere-Client auf der Registerkarte Zusammenfassung. • Für Microsoft Hyper-V, kann die IP-Adresse der VM's gefunden werden, indem man sich auf der lokalen Konsole anmeldet. Wenn Sie immer noch Probleme haben die Gateway-IP-Adresse zu ermitteln: • Stellen Sie sicher, dass der VM aktiviert ist. Nur wenn die VM aktiviert ist, wird dem Gateway eine IP-Adresse zugewiesen. • Warten Sie bis die VM den Startup abgeschlossen hat. Wenn Sie Ihre VM gerade erst aktiviert haben, kann es einige Minuten dauern, bis die Gateways mit der Boot-Sequenz abschließen.
Sie haben Netzwerk- oder Firewall-Probleme.	• Erteilen Sie dem Gateway die Zugriffserlaubnis für die entsprechenden Ports. • SSL-Zertifikat für jedes Zertifikatvalidation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign. • Falls Sie den Netzwerkdatenverkehr mithilfe einer Firewall oder eines Routers filtern oder einschränken, müssen Sie die Firewall und den Router so konfigurieren, dass diese Service-Endpunkte für die ausgehende Kommunikation mit AWS verwendet werden dürfen. Weitere Informationen zum Netzwerk und Firewall-Anforderungen finden Sie unter Netzwerk- und Firewall-Anforderungen.
Die Aktivierung des Gateways schlägt fehl, wenn Sie in der Storage-	• Überprüfen Sie, dass auf die Gateway-VM zugegriffen werden kann, indem Sie die VM Ihres Clients anpingen.

Problem	Maßnahme
Gateway-Managementkonsole auf die Schaltfläche Weiter zur Aktivierung klicken.	• Stellen Sie sicher, dass Ihre VM eine Netzwerkverbindung zum Internet hat. Andernfalls müssen Sie die Konfiguration eines SOCKS-Proxy vornehmen. Weitere Informationen zur Verfahrensweise finden Sie unter Konfiguration eines SOCKS5 Proxys für Ihr lokales Gateway. • 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. Hinweise zum Synchronisieren der Uhrzeit von Hypervisor-Hosts und VMs finden Sie unter. Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Hostzeit • 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. • SSL-Zertifikat für jedes Zertifikatvalidation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign. • 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 für die Einrichtung von Tape Gateway.

Problem	Maßnahme
Entfernen Sie eine als Upload-Pufferspeicher zugewiesene Festplatte. Beispielsweise möchten Sie die Anzahl der Upload-Pufferspeicher für ein Gateway reduzieren oder eine Festplatte ersetzen, die als fehlgeschlagener Puffer verwendet wurde.	Anweisungen zum Entfernen eines Datenträgers, der als Upload-Pufferspeicherplatz zugewiesen ist, finden Sie unter Entfernen von Datenträgern aus dem Gateway.
Sie müssen die Bandbreite zwischen Ihrem Gateway und AWS verbessern.	Sie können die Bandbreite von Ihrem Gateway zu verbessern, AWS indem Sie Ihre Internetverbindung AWS auf einem Netzwerkadapter (NIC) einrichten, der von dem Netzwerkadapter (NIC) getrennt ist, der Ihre Anwendungen und die Gateway-VM verbindet. Dieser Ansatz ist nützlich, wenn Sie eine Verbindung mit hoher Bandbreite haben AWS und Bandbreitenkonflikte vermeiden möchten, insbesondere bei einer Snapshot-Wiederherstellung. Für Workloads mit hohem Durchsatz können Sie AWS Direct Connect verwenden, um eine dedizierte Netzwerkverbindung zwischen dem lokalen Gateway und AWS herzustellen. Verwenden Sie die `CloudBytesUploaded` Metriken `CloudBytesDownloaded` und des Gateways AWS, um die Bandbreite der Verbindung von Ihrem Gateway zu zu messen. Weitere Informationen zu diesem Thema finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS. Indem Sie Ihre Internetverbindung verbessern, stellen Sie sicher, dass Ihr Upload-Puffer nicht aufgefüllt wird.

Problem	Maßnahme

Durchsatz zu oder von Ihrem Gateway sinkt auf Null.	• Stellen Sie auf der Registerkarte Gateway der Storage Gateway Gateway-Konsole sicher, dass die IP-Adressen für Ihre Gateway-VM denen entsprechen, die Sie mit Ihrer Hypervisor-Client-Software (d. h. dem VMware vSphere-Client oder Microsoft Hyper-V Manager) sehen. Wenn Sie eine Nichtübereinstimmung finden, starten Sie das Gateway über die Storage-Gateway-Konsole neu, wie unter 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.
	  • Denn VMware ESXi die IP-Adresse der VM finden Sie im vSphere-Client auf der Registerkarte Zusammenfassung.
	  • Für Microsoft Hyper-V, kann die IP-Adresse der VM's gefunden werden, indem man sich auf der lokalen Konsole anmeldet.
	• Überprüfen Sie die Konnektivität Ihres Gateways AWS wie unter beschriebenTesten Sie Ihre Gateway-Verbindung zum Internet.
	• Prüfen Sie die Netzwerkadapterkonfiguration des Gateways und stellen Sie sicher, dass alle Schnittstellen, die Sie für das Gateway aktivieren möchten, aktiviert sind. Um die Netzwerka dapter Konfiguration Ihres Gateways anzuzeigen, befolgen Sie die Anweisungen in Konfigurieren Ihres Gateway-Netzwerks und wählen Sie die Option die die Netzwerkkonfiguration Ihres Gateway anzeigt.
	
	Sie können den Durchsatz zu und von Ihrem Gateway von der CloudWatch Amazon-Konsole aus anzeigen. Weitere Informati onen zur Messung des Durchsatzes zu und von Ihrem Gateway und AWS finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

Problem	Maßnahme
Sie haben Schwierig keiten mit dem Importieren (Bereitstellen) von Storage Gateway auf Microsoft Hyper-V.	Weitere Informationen finden Sie unter Fehlerbehebung bei der Einrichtung von Microsoft Hyper-V, in dem einige der gängigen Themen der Bereitstellung einer Gateway auf Microsoft Hyper-V diskutiert werden.
Sie erhalten die Fehlermel dung: „Die Daten, die in das Volume in Ihrem Gateway geschrieben wurden, sind nicht sicher bei AWS gespeichert.“	Sie erhalten diese Meldung, wenn Ihre Gateway-VM aus einem Klon oder Snapshot eine andere Gateway-VM erstellt wurde. Wenn dies nicht der Fall ist, wenden Sie sich an den Support.

So können Support Sie bei der Fehlerbehebung Ihres lokal gehosteten Gateways helfen

Storage Gateway bietet eine lokale Konsole, mit der Sie verschiedene Wartungsaufgaben ausführen können, einschließlich der Aktivierung Support für den Zugriff auf Ihr Gateway, um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Standardmäßig ist der Support Zugriff auf Ihr Gateway deaktiviert. Dieser Zugriff wird über die lokale Host-Konsole gewährt. Um Support Zugriff auf Ihr Gateway zu gewähren, melden Sie sich zunächst bei der lokalen Konsole für den Host an, navigieren zur Konsole des Storage Gateways und stellen dann eine Verbindung zum Support-Server her.

Um den Support Zugriff auf Ihr Gateway zu ermöglichen

1. Melden Sie sich bei der lokalen Konsole Ihres Hosts an.
   - VMware ESXi — Weitere Informationen finden Sie unterZugreifen auf die lokale Gateway-Konsole mit VMware ESXi.
   - Microsoft Hyper-V: Weitere Informationen finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
2. Geben Sie bei der Eingabeaufforderung die entsprechende Zahl ein, um Gateway-Konsole auszuwählen.

3. Geben Sie **h** ein, um die Liste der verfügbaren Befehle zu öffnen.
4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, geben Sie im Fenster VERFÜGBARE BEFEHLE **`open-support-channel`** ein, um eine Verbindung zum Storage-Gateway-Kundensupport herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.
   - Wenn Ihr Gateway einen VPC-Endpunkt verwendet, geben Sie im Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) **`open-support-channel`** ein. Wenn Ihr Gateway nicht aktiviert ist, geben Sie den VPC-Endpunkt oder die IP-Adresse ein, für die eine Verbindung mit dem Storage-Gateway-Kundensupport hergestellt werden soll. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.

   > **Note**
   >
   > Die Kanalnummer ist keine Portnummer (Transmission ControlProtocol/User Datagram Protocol (TCP/UDP). Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP 22)-Verbindung zu den Storage-Gateway-Servern her und stellt den Support-Kanal für die Verbindung bereit.

5. Nachdem der Support-Kanal eingerichtet wurde, geben Sie Ihre Support-Servicenummer an, Support damit wir Ihnen bei der Problembehebung weiterhelfen Support können.
6. Wenn die Supportsitzung beendet ist, geben Sie **`q`** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn Sie vom Amazon Web Services Support darüber informiert werden, dass die Support-Sitzung abgeschlossen ist.
7. Geben Sie ein**`exit`**, um sich von der Gateway-Konsole abzumelden.
8. Folgen Sie den Eingabeaufforderungen, um die lokale Konsole zu beenden.

Fehlerbehebung bei der Einrichtung von Microsoft Hyper-V

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

Problem	Maßnahme
Sie versuchen, ein Gateway zu importieren und erhalten die folgende Fehlermeldung: „Beim Versuch, die virtuelle Maschine zu importier en, ist ein Serverfehler aufgetreten. Der Import ist fehlgeschlagen. Die Importdateien der virtuelle n Maschine konnten unter dem Speicherort [...] nicht gefunden werden. Sie können eine virtuelle Maschine nur importieren, wenn Sie sie mit Hyper-V erstellt und exportiert haben.“	Dieser Fehler kann aus folgenden Gründen auftreten: • Wenn Sie nicht auf das Stammverzeichnis der entpackten Gateway-Quell-Dateien zeigen. Der letzte Teil des Speicherorts, den Sie im Dialogfeld Virtuelle Maschine importieren angeben, sollte. `AWS-Storage-Gateway` Zum Beispiel: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • Wenn Sie bereits ein Gateway bereitgestellt haben, die Option Copy the virtual machine (virtuelle Maschine kopieren) nicht ausgewählt ist und Sie die Option Duplicate all files (Alle Dateien duplizieren) im Dialogfeld Import Virtual Machine (Virtuelle Maschine importieren) markiert haben, dann wurde die VM an dem Speicherort erstellt, an dem Sie die Dateien entpackt haben, und Sie können nicht erneut von dort importieren. Zur Behebung dieses Problems, erwerben Sie eine neue Kopie der entpackten Gateway Quell-Dateien und kopieren Sie diese an einen neuen Speicherort. Verwenden Sie den neuen Speicherort als Importque lle. Wenn Sie mehrere Gateways von einem Speicherort für entpackte Quelldateien aus erstellen möchten, müssen Sie die Option Virtuelle Maschine kopieren auswählen und im Dialogfeld Virtuelle Maschine importieren das Kontrollkästchen Alle Dateien duplizieren aktivieren.
Sie versuchen, ein Gateway zu importieren, und erhalten die folgende Fehlermeldung:	Wenn Sie bereits ein Gateway bereitgestellt haben und Sie versuchen den Standard-Ordner wiederzuverwenden, der die virtuelle Festplatten Dateien und die virtuelle Maschinen-Konfigur ationsdateien speichert, wird dieser Fehler auftreten. Um dieses

Problem	Maßnahme
„Beim Versuch, die virtuelle Maschine zu importier en, ist ein Serverfehler aufgetreten. Der Import ist fehlgeschlagen. Die Importaufgabe konnte die Datei nicht von [...] kopieren: Die Datei existiert . (0x80070050)“	Problem zu beheben, geben Sie im Bereich auf der linken Seite des Dialogfelds Hyper-V-Einstellungen unter Server neue Speicherorte an.
Sie versuchen, ein Gateway zu importieren, und erhalten die folgende Fehlermeldung: „Beim Versuch, die virtuelle Maschine zu importier en, ist ein Serverfehler aufgetreten. Der Import ist fehlgeschlagen. Der Import ist fehlgeschlagen, da die virtuelle Maschine über eine neue ID verfügen muss. Wählen Sie eine ID und versuchen Sie erneut zu importieren.“	Stellen Sie beim Import des Gateways sicher, dass Sie die Option Virtuelle Maschine kopieren auswählen und im Dialogfeld Virtuelle Maschine importieren das Kontrollkästchen Alle Dateien duplizieren aktivieren, um eine neue eindeutige ID für die VM zu erstellen.

Problem	Maßnahme
Sie versuchen, eine Gateway-VM zu starten und erhalten die folgende Fehlermeldung: „Beim Versuch, die ausgewählten virtuelle n Maschinen zu starten, ist ein Fehler aufgetret en. Die Prozessor-Einstell ung für die untergeordnete Partition ist nicht mit der übergeordneten Partition kompatibel. 'AWS-Stor age-Gateway' konnte nicht initialisiert werden. (ID der virtuellen Maschine [...])“	Dieser Fehler wird wahrscheinlich durch eine CPU-Diskrepanz zwischen den CPUs für das Gateway erforderlichen und den CPUs auf dem Host verfügbaren Werten verursacht. Stellen Sie sicher, dass die VM-CPU-Inventur von der zugrunde liegenden Hypervisor unterstützt wird. Weitere Informationen zu den Anforderungen für Storage Gateway finden Sie unter Voraussetzungen für die Einrichtung von Tape Gateway.

Problem	Maßnahme
Sie versuchen, eine Gateway-VM zu starten und erhalten die folgende Fehlermeldung: „Beim Versuch, die ausgewählten virtuellen Maschinen zu starten, ist ein Fehler aufgetreten. 'AWS-Storage-Gateway' konnte nicht initialisiert werden. (ID der virtuelle n Maschine [...]) Partition konnte nicht erstellt werden: Es sind nicht genügend Systemres sourcen vorhanden, um den angeforderten Dienst abzuschließen. (0x800705 AA)“	Dieser Fehler wird wahrscheinlich durch eine RAM-Abweichungen zwischen dem erforderlichen RAM für das Gateway und den verfügbaren RAM auf dem Host verursacht. Weitere Informationen zu den Anforderungen für Storage Gateway finden Sie unter Voraussetzungen für die Einrichtung von Tape Gateway.
Ihre Snapshots und Gateway-Software-A ktualisierungen treten zu geringfügig anderen Zeiten als erwartet auf.	Die Uhr der Gateway-VM, weicht möglicherweise von der tatsächli chen Uhrzeit ab, dies wird als Ganggenauigkeit bezeichnet. Überprüfen und korrigieren Sie die Uhrzeit der VM, indem Sie die Option Synchronisierung der lokalen Gateway-Konsole verwenden. Weitere Informationen finden Sie unter Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Hostzeit.
Sie müssen die entzippten Microsoft Hyper-V-Dateien für Storage Gateway im Host-Dateisystem ablegen.	Greifen Sie auf den Host zu wie Sie auf einen typischen Microsoft Windows Server zugreifen würden. Zum Beispiel: Wenn der Hypervisor Host-Name `hyperv-server` lautet, dann können Sie den folgenden UNC-Pfad wählen `\\hyperv-server\c$` , dieser geht davon aus, dass der Name `hyperv-server` in Ihrer lokalen Host-Datei aufgelöst oder definiert werden kann.

Problem	Maßnahme
Sie werden aufgefordert Anmeldeinformationen anzugeben, wenn Sie eine Verbindung zum Hyperviso r herstellen.	Fügen Sie Ihre Benutzer-Anmeldeinformationen als lokaler Administrator für den Hypervisor-Host mithilfe des Sconfig.cmd Tool hinzu.
Möglicherweise stellen Sie eine schlechte Netzwerkl eistung fest, wenn Sie die Virtual Machine Queue (VMQ) für einen Hyper-V-Host aktivieren, der einen Broadcom-Netzwerka dapter verwendet.	Informationen zu einer Problemumgehung finden Sie in der Microsoft-Dokumentation unter Schlechte Netzwerkleistung auf virtuellen Maschinen auf einem Windows Server 2012 Hyper-V-H ost, wenn VMQ eingeschaltet ist.

Behebung von Problemen mit Amazon EC2 Gateway

In den folgenden Abschnitten finden Sie typische Probleme, die bei der Arbeit mit Ihrem auf Amazon bereitgestellten Gateway auftreten können EC2. Weitere Informationen zum Unterschied zwischen einem lokalen Gateway und einem in Amazon bereitgestellten Gateway finden Sie EC2 unterStellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit.

Themen

- Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.
- Sie können Ihre EC2 Gateway-Instance nicht in der Instance-Liste finden
- Sie haben ein Amazon EBS-Volume erstellt, können es aber nicht an Ihre EC2 Gateway-Instance anhängen
- 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
- Der Durchsatz zu oder von Ihrem EC2 Gateway sinkt auf Null
- Sie Support möchten bei der Fehlerbehebung Ihres EC2 Gateways helfen

- Sie möchten über die EC2 serielle Amazon-Konsole eine Verbindung zu Ihrer Gateway-Instance herstellen

Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.

Überprüfen Sie in der EC2 Amazon-Konsole Folgendes:

- Port 80 ist in der Sicherheitsgruppe aktiviert, die Sie mit der Instance verknüpft haben. Weitere Informationen zum Hinzufügen einer Sicherheitsgruppenregel finden Sie unter Hinzufügen einer Sicherheitsgruppenregel im EC2 Amazon-Benutzerhandbuch.
- Die Gateway-Instance ist als laufend markiert. In der EC2 Amazon-Konsole sollte der State-Wert für die Instance RUNNING lauten.
- Stellen Sie sicher, dass Ihr EC2 Amazon-Instance-Typ die Mindestanforderungen erfüllt, wie unter beschriebenSpeicheranforderungen.

Versuchen Sie erneut, das Gateway zu aktivieren, nachdem Sie das Problem behoben haben. Öffnen Sie dazu die Storage Gateway Gateway-Konsole, wählen Sie Deploy a new Gateway on Amazon EC2 und geben Sie die IP-Adresse der Instance erneut ein.

Sie können Ihre EC2 Gateway-Instance nicht in der Instance-Liste finden

Wenn Sie die Instance nicht mit einem Ressourcen-Tag versehen haben und viele Instances ausführt werden, ist es schwierig, die von Ihnen gestarteten Instances zu benennen. In diesem Fall können Sie die folgenden Aktionen ausführen, um die Gateway Instance zu finden:

- Prüfen Sie den Namen des Amazon Machine Image (AMI) auf der Registerkarte Description (Beschreibung) der Instance. Eine Instance 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 Ihre EC2 Gateway-Instance anhängen

Stellen Sie sicher, dass sich dieses Amazon-EBS-Volume in derselben Availability Zone wie die Gateway-Instance befindet. Falls eine Abweichung in den Availability Zones besteht, erstellen Sie ein neues Amazon-EBS-Volume, das sich in derselben Availability Zone wie die Instance befindet.

Beim Hinzufügen von Speicher-Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind

Für ein neu aktiviertes Gateway ist kein Volume-Speicher definiert. Bevor Sie Volume-Speicher definieren können, müssen Sie die lokale Festplatten zum Gateway zuweisen, die Sie als Upload-Puffer und Cache-Speicher verwenden. Bei einem auf Amazon bereitgestellten Gateway handelt es sich bei den lokalen Festplatten um Amazon EBS-Volumes EC2, die an die Instance angehängt 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 Stellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit. 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.

Der Durchsatz zu oder von Ihrem 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 von der CloudWatch Amazon-Konsole aus anzeigen. Weitere Informationen zur Messung des Durchsatzes zu und von Ihrem Gateway und AWS finden Sie unter Messung der Leistung zwischen Ihrem Tape Gateway und AWS.

Sie Support möchten bei der Fehlerbehebung Ihres EC2 Gateways helfen

Storage Gateway bietet eine lokale Konsole, mit der Sie verschiedene Wartungsaufgaben ausführen können, einschließlich der Aktivierung Support für den Zugriff auf Ihr Gateway, um Sie bei der Behebung von Gateway-Problemen zu unterstützen. Standardmäßig ist der Support Zugriff auf Ihr Gateway deaktiviert. Sie stellen diesen Zugriff über die EC2 lokale Amazon-Konsole bereit. Sie melden sich über eine Secure Shell (SSH) bei der EC2 lokalen Amazon-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 EC2 Amazon-Sicherheitsgruppen im EC2 Amazon-Benutzerhandbuch.

Um eine Support Verbindung zu Ihrem Gateway herzustellen, melden Sie sich zunächst bei der lokalen Konsole für die EC2 Amazon-Instance an, navigieren zur Konsole des Storage Gateways und gewähren dann den Zugriff.

Um den Support Zugriff auf ein auf einer EC2 Amazon-Instance bereitgestelltes Gateway zu aktivieren

1. Melden Sie sich bei der lokalen Konsole für Ihre EC2 Amazon-Instance an. Anweisungen finden Sie im EC2 Amazon-Benutzerhandbuch unter Connect to your Instance.

   Sie können den folgenden Befehl verwenden, um sich bei der lokalen Konsole der EC2 Instance anzumelden.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > Das *PRIVATE-KEY* ist die `.pem` Datei, die das private Zertifikat des EC2 key pair enthält, das Sie zum Starten der EC2 Amazon-Instance verwendet haben. Weitere Informationen

finden Sie unter Abrufen des öffentlichen Schlüssels für Ihr key pair im EC2 Amazon-Benutzerhandbuch.
Das *INSTANCE-PUBLIC-DNS-NAME* ist der öffentliche DNS-Name (Domain Name System) Ihrer EC2 Amazon-Instance, auf der Ihr Gateway läuft. Sie erhalten diesen öffentlichen DNS-Namen, indem Sie die EC2 Amazon-Instance in der EC2 Konsole auswählen und auf den Tab Beschreibung klicken.

2. Geben Sie an der Eingabeaufforderung **`6 - Command Prompt`** ein, um die Channel-Konsole für Support zu öffnen.
3. Geben Sie **h** ein, um das Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) zu öffnen.
4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, geben Sie im Fenster VERFÜGBARE BEFEHLE **`open-support-channel`** ein, um eine Verbindung zum Storage-Gateway-Kundensupport herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.
   - Wenn Ihr Gateway einen VPC-Endpunkt verwendet, geben Sie im Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) **`open-support-channel`** ein. Wenn Ihr Gateway nicht aktiviert ist, geben Sie den VPC-Endpunkt oder die IP-Adresse ein, für die eine Verbindung mit dem Storage-Gateway-Kundensupport hergestellt werden soll. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.

   Note

   Die Kanalnummer ist keine Portnummer (Transmission ControlProtocol/User Datagram Protocol (TCP/UDP). Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP 22)-Verbindung zu den Storage-Gateway-Servern her und stellt den Support-Kanal für die Verbindung bereit.

5. Nachdem der Support-Kanal eingerichtet wurde, geben Sie Ihre Support-Servicenummer an, Support damit wir Ihnen bei der Problembehebung weiterhelfen Support können.

6. Wenn die Supportsitzung beendet ist, geben Sie **q** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn Sie Support darüber informiert werden, dass die Support-Sitzung abgeschlossen ist.
7. Geben Sie **exit** ein, um die Storage-Gateway-Konsole zu verlassen.
8. Verwenden Sie die Konsolenmenüs, um sich von der Storage-Gateway-Instance abzumelden.

Sie möchten über die EC2 serielle Amazon-Konsole eine Verbindung zu Ihrer Gateway-Instance herstellen

Sie können die EC2 serielle Amazon-Konsole verwenden, um Boot-, Netzwerkkonfigurations- und andere Probleme zu beheben. Anweisungen und Tipps zur Fehlerbehebung finden Sie unter Amazon EC2 Serial Console im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Fehlerbehebung bei Hardware-Appliance-Problemen

In den folgenden Themen werden Probleme, die im Zusammenhang mit der Hardware-Appliance für Storage Gateway auftreten können, sowie Lösungsvorschläge beschrieben.

Festlegen der Service-IP-Adresse nicht möglich

Wenn Sie versuchen, eine Verbindung mit Ihrem Service herzustellen, stellen Sie sicher, dass Sie die Service-IP-Adresse und nicht die Host-IP-Adresse verwenden. Konfigurieren Sie die Service-IP-Adresse in der Servicekonsole und die Host-IP-Adresse in der Hardwarekonsole. Die Hardwarekonsole wird angezeigt, wenn die Hardware-Appliance gestartet wird. Um die Servicekonsole über die Hardwarekonsole zu öffnen, wählen Sie Open Service Console (Servicekonsole öffnen).

Wie lässt sich eine Zurücksetzung auf die Werkseinstellungen durchführen?

Wenn Sie die Appliance auf die Werkseinstellungen zurücksetzen müssen, wenden Sie sich an das Hardware-Appliance-Team für Storage Gateway, um wie im folgenden Support-Abschnitt beschrieben Unterstützung zu erhalten.

Wie erfolgt der Remote-Neustart?

Wenn Sie einen Remote-Neustart Ihrer Appliance durchführen müssen, können Sie dazu die Dell iDRAC-Verwaltungsschnittstelle verwenden. Weitere Informationen finden Sie unter i DRAC9

Virtueller Energiezyklus: Dell EMC PowerEdge Server aus der Ferne ein- und ausschalten auf der InfoHub Website von Dell Technologies.

Wo erhalten Sie Dell iDRAC-Support?

Der Dell PowerEdge Server ist mit der Dell iDRAC-Verwaltungsschnittstelle ausgestattet. Wir empfehlen Folgendes:

- Wenn Sie die iDRAC-Verwaltungsschnittstelle verwenden, sollten Sie das Standardkennwort ändern. Weitere Informationen zu den iDRAC-Anmeldeinformationen finden Sie unter Dell PowerEdge — Was sind die Standardanmeldedaten für iDRAC? .
- Stellen Sie sicher, dass die Firmware Sicherheitslücken verhindern up-to-date soll.
- Wenn die iDRAC-Netzwerkschnittstelle an einen normalen Port (`em`) verschoben wird, kann dies zu Leistungsproblemen führen oder die normale Funktionsweise der Appliance beeinträchtigen.

Die Seriennummer der Hardware-Appliance lässt sich nicht finden

Sie können die Seriennummer für Ihre Storage Gateway Hardware-Appliance in der Storage Gateway Gateway-Konsole finden.

So finden Sie die Seriennummer der Hardware-Appliance:

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsmenü auf der linken Seite Hardware aus.
3. Wählen Sie Ihre Hardware-Appliance aus der Liste aus.
4. Suchen Sie das Feld Seriennummer auf der Registerkarte Details für Ihre Appliance.

Wo Sie Hardware-Appliance-Support erhalten?

AWS Informationen zum technischen Support für Ihre Hardware-Appliance finden Sie unter Support.

Das Support Team bittet Sie möglicherweise, den Support-Kanal zu aktivieren, um Ihre Gateway-Probleme aus der Ferne zu beheben. Dieser Port muss für den normalen Betrieb des Gateways nicht offen sein, für die Fehlerbehebung ist dies jedoch erforderlich. Sie können den Support-Kanal über die Hardware-Konsole aktivieren, wie im folgenden Verfahren dargestellt.

Um einen Support-Kanal zu öffnen für AWS

1. Öffnen Sie die Hardwarekonsole.
2. Wählen Sie unten auf der Hauptseite der Hardwarekonsole die Option Open Support Channel aus, und drücken Sie dann`Enter`.

   Die zugewiesene Portnummer sollte innerhalb von 30 Sekunden angezeigt werden, sofern keine Probleme mit der Netzwerkkonnektivität oder der Firewall vorliegen. Zum Beispiel:

   Status: Auf Port 19599 geöffnet
3. Notieren Sie sich die Portnummer und geben Sie sie an Support.

Beheben von Problemen mit virtuellen Bändern

Informationen über die Aktionen die Sie vornehmen können, wenn Sie unerwartete Probleme mit Ihren virtuellen Bändern haben.

Themen

- Wiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway
- Fehlerbehebung bei nicht wiederherstellbaren Bändern
- High Availability-Zustandsbenachrichtigungen

Wiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway

Obwohl ist es selten vorkommt, könnte in Ihrem Tape Gateway ein schwerwiegender Fehler auftreten. Solche Fehler können in Ihrer Hypervisor-Host, dem Gateway selbst oder in der Cache-Festplatte auftreten. Wenn ein Fehler auftritt, können Sie Ihre Bänder wiederherstellen. Befolgen Sie hierzu die Anweisungen zur Fehlerbehebung in diesem Abschnitt.

Themen

- Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen.
- Sie müssen ein virtuelles Band aus einer fehlerhaften Cache-Festplatte wiederherstellen

Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen.

Wenn Ihr Tape Gateway oder der Hypervisor-Host auf einen nicht behebbaren Fehler stößt, können Sie alle Daten wiederherstellen, die bereits auf ein anderes Tape Gateway hochgeladen wurden. AWS

Beachten Sie, dass die Daten die auf ein Band geschrieben wurden nicht vollständig hochgeladen sein müssen bis dieses Band erfolgreich in VTS archiviert wurde. Die Daten auf den Bändern, die auf einem anderen Gateway wiederhergestellt worden können unvollständig oder leer sein. Wir empfehlen, einen Bestand für alle wiederhergestellten Bänder vorzunehmen, um sicherzustellen, dass diese die erwarteten Inhalte enthalten.

So stellen Sie ein Band auf einem anderen Tape Gateway wieder her

1. Identifizieren Sie ein vorhandenes funktionierendes Tape Gateway, das als Wiederherstellungs-Ziel-Gateway dient. Wenn Sie über kein Tape Gateway verfügen, auf dem Sie ihre Bänder wiederherstellen können, erstellen Sie ein neues Tape Gateway. Weitere Informationen zum Erstellen eines Gateways finden Sie unter Erstellen eines Gateways.
2. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
3. Wählen Sie im Navigationsbereich erst Gateways und dann dasTape Gateway aus, von dem Sie Ihre Bänder wiederherstellen möchten.
4. Wählen Sie die Registerkarte Details. Eine Nachricht über das wiederhergestellte Band wird in der Registerkarte angezeigt.
5. Wählen Sie Wiederherstellungsbänder erstellen aus, um das Gateway zu deaktivieren.
6. Wählen Sie im angezeigten Dialogfeld Disable gateway (Gateway deaktivieren).

   Damit wird der Betrieb des Tape Gateway dauerhaft angehalten und alle verfügbaren Wiederherstellungspunkte werden bereitgestellt. Anweisungen finden Sie unter Deaktivierung Ihres Tape Gateways.
7. Wählen Sie aus den Bändern, die das deaktivierte Gateway anzeigt, das virtuelle Band und den Wiederherstellungspunkt aus, den Sie wiederherstellen möchten. Eine virtuelles Band kann mehrere Wiederherstellungspunkte haben.
8. Um mit dem Wiederherstellen von Bändern zu beginnen, müssen Sie zum Ziel-Tape-Gateway wechseln und Wiederherstellungsband erstellen wählen.

9. Überprüfen Sie im Dialogfeld Create recovery tape (Wiederherstellungsband erstellen) den Barcode des virtuellen Bands, das wiederhergestellt werden soll.
10. wählen Sie für Gateway das Tape Gateway aus, auf dem Sie das virtuelle Band wiederherstellen möchten.
11. Wählen Sie Create recovery tape (Wiederherstellungsband erstellen).
12. Löschen Sie das fehlerhafte Tape Gateway, damit es Ihnen nicht in Rechnung gestellt wird. Detaillierte Anweisungen finden Sie unter Löschen Ihres Gateways und Entfernen der zugehörigen Ressourcen.

Storage Gateway verschiebt das Band vom ausgefallenen Tape Gateway auf das von Ihnen angegebene Tape Gateway. Tape Gateway markiert das Band mit dem Status RECOVERED.

Sie müssen ein virtuelles Band aus einer fehlerhaften Cache-Festplatte wiederherstellen

Wenn in Ihrer Cache-Festplatte ein Fehler auftritt, verhindert das Gateway Lese- und Schreiboptionen auf dem virtuellen Band im Gateway. Beispielsweise kann ein Fehler auftreten, wenn eine Festplatte vom Gateway beschädigt oder entfernt wurde. Die Storage-Gateway-Konsole zeigt eine Meldung über den Fehler an.

In der Fehlermeldung fordert Sie Storage Gateway auf, eine von zwei Aktionen zur Wiederherstellung Ihrer Bänder auszuführen:

- Herunterfahren und erneutes Hinzufügen von Festplatten: Verwenden Sie diesen Ansatz, wenn die Festplatte intakte Daten enthält und entfernt wurde. Wenn der Fehler z. B aufgetreten ist, da der Datenträger versehentlich von Ihrem Host entfernt wurde aber die Festplatte und die Daten intakt sind, können Sie den Datenträger erneut hinzufügen. Um dies durchzuführen, siehe Vorgang zu einem späteren Zeitpunkt in diesem Thema.
- Zurücksetzen des Cache-Datenträgers: Wählen Sie diesen Ansatz, wenn der Cache-Datenträger beschädigt oder nicht verfügbar ist. Wenn der Datenträger Fehler bewirkt, dass das Cache nicht verfügbar, beschädigt oder unbenutzbar ist, können Sie die Datenträger zurücksetzen. Wenn Sie den Cache-Datenträger zurücksetzen, werden Bänder, die bereinigte Daten aufweisen (das sind Bänder, für die Daten auf der Cache-Festplatte und in Amazon S3 synchronisiert werden), weiterhin für Sie verfügbar sein. Jedoch werden Bänder, deren Daten nicht mit Amazon S3 synchronisiert werden, automatisch wiederhergestellt. Der Status dieser Bänder ist auf WIEDERBESCHAFFT gesetzt, doch die Bänder sind schreibgeschützt. Weitere Informationen

zum Entfernen einer Festplatte aus dem Host finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.

> **Important**
>
> Wenn der Cache-Festplatte, den sie zurücksetzen, Daten enthält, die Sie noch nicht in Amazon S3 hochgeladen haben, können diese Daten verloren gehen. Nachdem Sie den Cache-Datenträger neu gesetzt haben, werden keine konfigurierten Cache-Datenträger im Gateway sein, Sie müssen mindestens einen neuen Cache-Datenträger für Ihr Gateway konfigurieren, damit es richtig funktioniert.

Um den Cache-Datenträger neu zu setzen sehen Sie den Vorgang, der später in diesem Thema auftaucht.

Herunterfahren und das erneute hinzufügen einer Festplatte

1. Fahren Sie das Gateway herunter. Weitere Informationen, wie Sie ein Gateway herunterfahren, finden Sie unter Herunterfahren der Gateway-VM.
2. Fügen Sie die Festplatte an Ihren Host zurück, und stellen Sie sicher, dass die Datenträger Knotennummer des Datenträgers nicht verändert wurde. Weitere Informationen zum Hinzufügen eines Datenträgers finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.
3. Starten Sie Ihr Gateway neu. Weitere Informationen wie Sie ein Gateway neu starten finden Sie unter Herunterfahren der Gateway-VM.

Nachdem das Gateway neu gestartet wurde, können Sie den Status der Cache-Festplatten überprüfen. Der Status eines Datenträgers kann einer der folgenden sein:

- vorhanden - Der Datenträger ist verfügbar.
- fehlend – Der Datenträger ist nicht mehr mit dem Gateway verbunden.
- stimmen nicht überein . Der Datenträger-Knoten ist von einem Datenträger belegt, der falsche Metadaten besitzt oder die Inhalte des Datenträgers sind beschädigt.

Einen Cache-Datenträger neu setzen und neu konfigurieren

1. Wählen Sie in der oben abgebildeten Fehlermeldung A disk error has occurred (Ein Festplattenfehler ist aufgetreten) die Option Reset Cache Disk (Cache-Festplatte zurücksetzen).
2. Konfigurieren Sie auf der Seite Gateway konfigurieren die Festplatte als Cache-Speicher. Informationen zur Vorgehensweise finden Sie unter Konfigurieren von Tape Gateway.
3. Nachdem Sie die Cache-Speicherung konfiguriert haben, fahren Sie das Gateway herunter und starten Sie es erneut, wie im Vorgang oben beschrieben.

Das Gateway sollte nach dem Neustart wiederhergestellt sein. Sie können dann den Status der Cache-Festplatte überprüfen.

So prüfen Sie den Status einer Cache-Festplatte

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und wählen Sie dann Ihr Gateway.
3. Wählen Sie für Actions (Aktionen) die Option Configure Local Storage (Lokalen Speicher konfigurieren) aus, um das Dialogfeld Configure Local Storage (Lokalen Speicher konfigurieren) anzuzeigen. In diesem Dialogfeld werden alle lokalen Festplatten in der Gateway angezeigt.

Der Cache-Festplatten-Knoten-Status wird neben der Festplatte angezeigt.

> **Note**
>
> Wenn Sie den Wiederherstellungsprozess nicht abschließen, zeigt das Gateway einen Banner an, der Sie auffordert lokalen Speicher zu konfigurieren.

Fehlerbehebung bei nicht wiederherstellbaren Bändern

Wenn Ihr virtuelles Band unerwartet ausfällt, setzt Storage Gateway den Status des fehlgeschlagen Bands zu IRRECOVERABLE. Die Aktion, die Sie durchführen hängt von den Umständen ab. Sie können Informationen zu einigen Themen finden und wie Sie diese möglicherweise beheben können.

Wiederherstellen von Daten von einem Band mit dem Status IRRECOVERABLE

Wenn Sie ein virtuelles Band mit dem Status IRRECOVERABLE haben und mit diesem arbeiten, versuchen Sie einen der folgenden Schritte:

- Aktivieren Sie ein neues Tape Gateway, sofern Sie noch keines aktiviert haben. Weitere Informationen finden Sie unter Erstellen eines Gateways.
- Deaktivieren Sie das Tape Gateway mit dem nicht wiederherstellbaren Band und stellen Sie das Band von einem Wiederherstellungspunkt auf dem neuen Tape Gateway wieder her. Weitere Informationen finden Sie unter Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen..

> **Note**
>
> Sie müssen Ihren iSCSI-Initiator und Ihre Sicherungsanwendung neu konfigurieren, um das neue Tape Gateway verwenden zu können. Weitere Informationen finden Sie unter Ihre VTL-Geräte anschließen.

Sie nicht benötigen kein IRRECOVERABLE Band das nicht archiviert ist

Wenn Sie ein virtuelles Band mit dem Status IRRECOVERABLE besitzen, brauchen Sie es nicht und das Band war noch nie archiviert, so sollten Sie es löschen. Weitere Informationen finden Sie unter Virtuelle Bänder von Ihrem Tape Gateway löschen.

In einem Cache-Datenträger 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 der Cache-Datenträger nicht zugänglich oder nicht verwendbar ist, löschen Sie den Datenträger aus Ihrer Gateway-Konfiguration.
- Wenn der Cache-Datenträger weiterhin zugänglich und nutzbar ist, verbinden Sie ihn erneut mit Ihrem Gateway.

> **Note**
>
> Wenn Sie einen Cache-Datenträger löschen, sind Bänder oder Volumes mit bereinigten Daten (also Daten, die auf dem Cache-Datenträger und in Amazon S3 synchron sind) weiterhin verfügbar, wenn das Gateway wieder normal funktioniert. Wenn Ihr Gateway beispielsweise über drei Cache-Datenträger 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 Ihr Cache-Datenträger und Amazon S3 nicht synchronisiert werden, kann das Herunterfahren des Gateways zu Datenverlust führen. Aus diesem Grund raten wir von der Verwendung von kurzlebigen Laufwerken oder Datenträgern ab.

High Availability-Zustandsbenachrichtigungen

Wenn Sie Ihr Gateway auf der VMware vSphere High Availability (HA) -Plattform ausführen, erhalten Sie möglicherweise Statusmeldungen. 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, senden alle Gateways die folgenden Integritätsbenachrichtigungen an Ihre konfigurierte CloudWatch Amazon-Protokollgruppe. Diese Benachrichtigungen werden in einem Protokollstream mit dem Namen `AvailabilityMonitor` erfasst.

Themen

- Benachrichtigung: Reboot
- Benachrichtigung: HardReboot
- Benachrichtigung: HealthCheckFailure
- Benachrichtigung: AvailabilityMonitorTest

Benachrichtigung: Reboot

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

Maßnahme

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

Benachrichtigung: HardReboot

Sie können eine `HardReboot`-Benachrichtigung erhalten, wenn die Gateway-VM unerwartet neu gestartet wird. Ein solcher Neustart kann auf Stromausfall, einen Hardwarefehler oder ein anderes Ereignis zurückzuführen sein. Bei VMware Gateways kann ein Reset durch vSphere High Availability Application Monitoring dieses Ereignis auslösen.

Maßnahme

Wenn Ihr Gateway in einer solchen Umgebung ausgeführt wird, überprüfen Sie, ob die `HealthCheckFailure` Benachrichtigung vorhanden ist, und lesen Sie im VMware Ereignisprotokoll für die VM nach.

Benachrichtigung: HealthCheckFailure

Für ein Gateway auf VMware vSphere HA können Sie eine `HealthCheckFailure` Benachrichtigung erhalten, wenn eine Integritätsprüfung fehlschlägt und ein VM-Neustart angefordert wird. Dieses Ereignis tritt auch während eines Tests zum Überwachen der Verfügbarkeit auf, der

durch die Benachrichtigung `AvailabilityMonitorTest` angezeigt wird. In diesem Fall wird die Benachrichtigung `HealthCheckFailure` erwartet.

> **Note**
>
> Diese Benachrichtigung gilt nur für VMware Gateways.

Maßnahme

Wenn dieses Ereignis wiederholt ohne die Benachrichtigung `AvailabilityMonitorTest` auftritt, überprüfen Sie die VM-Infrastruktur auf Probleme (Speicher, Arbeitsspeicher usw.). Wenn Sie zusätzliche Unterstützung benötigen, wenden Support Sie sich an.

Benachrichtigung: AvailabilityMonitorTest

Für ein Gateway auf VMware vSphere HA können Sie eine `AvailabilityMonitorTest` Benachrichtigung erhalten, wenn Sie einen Test des Verfügbarkeits- und Anwendungsüberwachungssystems in VMware ausführen.

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. Einzelheiten zu den Ereignissen erhalten Sie von Ihrer konfigurierten CloudWatch Protokollgruppe.

Bewährte Methoden für Tape Gateway

Dieser Abschnitt enthält die folgenden Themen, die Informationen zu den bewährten Methoden für die Arbeit mit Gateways, lokalen Festplatten, Snapshots und Daten enthalten. Wir empfehlen Ihnen, sich mit den Informationen in diesem Abschnitt vertraut zu machen und zu versuchen, diese Richtlinien zu befolgen, um Probleme mit Ihrem zu vermeiden. AWS Storage Gateway Weitere Hinweise zur Diagnose und Lösung häufiger Probleme, die bei Ihrer Bereitstellung auftreten können, finden Sie unterFehlerbehebung bei Ihrem Gateway.

Themen

- Bewährte Methoden: Wiederherstellung Ihrer Daten
- Säuberung unnötiger Ressourcen

Bewährte Methoden: Wiederherstellung Ihrer Daten

Obwohl ist es selten vorkommt, könnte in Ihrem Gateway ein Dauerfehler aufgetreten sein. Solche Fehler können in Ihrer virtuellen Maschine (VM), im Gateway selbst, dem lokalen Speicher oder an anderer Stelle auftreten. Wenn ein Fehler auftritt, empfehlen wir, dass Sie die Anweisungen im entsprechenden Abschnitt befolgen um Ihre Daten wiederherzustellen.

> **Important**
>
> Storage Gateway unterstützt nicht die Wiederherstellung einer Gateway-VM aus einem Snapshot, der von Ihrem Hypervisor oder von Ihrem Amazon EC2 Amazon Machine Image (AMI) erstellt wurde. Wenn Ihre Gateway VM, ein neues Gateway aktiviert und Ihre Daten auf diesem Gateway wiederhergestellt werden, dann folgen Sie folgenden Anweisungen.

Themen

- 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 Band
- Wiederherstellen Ihrer Daten von einem fehlerhaften Cache-Datenträger
- 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 Sie Ihre Gateway-Verbindung zum Internet.
- Wenn Ihr Gateway in Konfigurationen mit Bändern erreichbar ist, werden Ihre Bänder in den BOOTSTRAPPING-Status versetzt. Diese Funktion stellt sicher, dass Ihre lokal gespeicherten Daten weiterhin mit AWS synchronisiert werden. Weitere Informationen, zu diesem Status, finden Sie unter Grundlegendes zum Bandstatus.
- Wenn Ihre Gateway fehlerhaft ist und Probleme mit Ihren Volumes oder Bändern auftreten und das im Zusammenhang mit einem unerwarteten Herunterfahren steht, dann können Sie Daten wiederherstellen. Weitere Informationen dazu, wie Sie Ihre Daten wiederherstellen, finden Sie in den folgenden Abschnitten, die auf Ihren Fall passen.

Wiederherstellen Ihrer Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM

Wenn in Ihrem Tape Gateway oder im Hypervisor-Host ein Dauerfehler auftritt, können Sie die folgenden Schritte befolgen, um die Bänder von einem fehlerhaften Tape Gateway auf einem anderen Tape Gateway wiederherzustellen:

1. Legen Sie fest, welches Tape Gateway als Wiederherstellungsziel verwendet werden soll, oder erstellen Sie ein neues.
2. Deaktivieren Sie das defekte Gateway.
3. Erstellen Sie Wiederherstellungsbänder für jedes Band, dass Sie wiederherstellen möchten, und geben Sie das Ziel-Tape-Gateway an.
4. Löschen Sie die nicht funktionsfähige Tape Gateway.

Detaillierte Informationen zur Wiederherstellung der Bänder von einem fehlerhaften Tape Gateway auf einem anderen Tape Gateway finden Sie unter Sie müssen ein virtuelles Band von einem fehlerhaften Tape Gateway wiederherstellen..

Wiederherstellung Ihrer Daten von einem nicht wiederherstellbaren Band

Wenn in Ihrem Band ein Fehler auftritt und der Status des Bands IRRECOVERABLE ist, empfehlen wir, dass Sie eine der folgenden Optionen zum Wiederherstellen Ihrer Daten verwenden oder lösen Sie den Fehler je nach Situation:

- Wenn Sie die Daten auf dem irreparablen Band benötigen, können Sie das Band auf einem neuen Gateway wiederherstellen.
- Wenn Sie diese Daten nicht auf dem Band benötigen und das Band noch nie archiviert wurde, können sie dieses Band einfach von Ihrem Tape Gateway löschen.

  Detaillierte Informationen, wie Sie Ihre Daten wiederherstellen oder den Fehler lösen, wenn Ihr Band IRRECOVERABLE ist, finden Sie unter Fehlerbehebung bei nicht wiederherstellbaren Bändern.

Wiederherstellen Ihrer Daten von einem fehlerhaften Cache-Datenträger

Wenn in Ihrer Cache-Festplatte ein Fehler auftritt, empfehlen wir die folgenden Schritte zum Wiederherstellen Ihrer Daten je nach Situation, zu befolgen:

- Wenn der Fehler aufgetreten ist, weil eine Cache-Festplatte aus Ihrem Host entnommen wurde, fahren Sie das Gateway herunter, fügen Sie die Festplatte wieder ein und starten Sie das Gateway.
- Wenn der Cache-Datenträger beschädigt ist oder wenn nicht auf ihn zugegriffen werden kann, setzen Sie den Cache-Datenträger, konfigurieren Sie die Festplatte für den Cache-Speicher neu und starten Sie das Gateway neu.

Weitere Informationen hierzu finden Sie unter Sie müssen ein virtuelles Band aus einer fehlerhaften Cache-Festplatte wiederherstellen.

Wiederherstellen Ihrer Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann

Wenn Ihr Gateway oder Rechenzentrum aus irgendeinem Grund nicht mehr zugänglich ist, können Sie Ihre Daten auf einem anderen Gateway in einem anderen Rechenzentrum oder auf einem Gateway wiederherstellen, das auf einer EC2 Amazon-Instance gehostet wird. Wenn Sie keinen Zugriff auf ein anderes Rechenzentrum haben, empfehlen wir, das Gateway auf einer EC2 Amazon-Instance zu erstellen. Die weiteren Schritte sind abhängig vom Gateway-Typ, von dem aus Sie die Daten wiederherstellen.

So stellen Sie Daten von einem Tape Gateway in einem Rechenzentrum wieder her, auf das nicht zugegriffen werden kann

1. Erstellen und aktivieren Sie ein neues Tape Gateway auf einem EC2 Amazon-Host. Weitere Informationen finden Sie unter Stellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit.
2. Stellen Sie die Bänder vom Quell-Gateway im Rechenzentrum auf das neue Gateway wieder her, das Sie bei Amazon erstellt haben. EC2 Weitere Informationen finden Sie unterWiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway.

   Ihre Bänder sollten bis zum neuen EC2 Amazon-Gateway abgedeckt sein.

Säuberung unnötiger Ressourcen

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

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

So bereinigen Sie nicht benötigte Ressourcen

1. Löschen Sie Bänder aus der Virtual Tape Library (VTL) Ihres Gateways und aus dem Archiv. Weitere Informationen finden Sie unter Löschen Ihres Gateways und Entfernen der zugehörigen Ressourcen.

   a. Archivieren Sie alle Bänder, die in der VTL Ihres Gateways den Status RETRIEVED haben. Detaillierte Anweisungen finden Sie unter Archivieren von Bändern.

   b. Löschen Sie alle verbleibenden Bänder aus der Gateway-VTL. Detaillierte Anweisungen finden Sie unter Virtuelle Bänder von Ihrem Tape Gateway löschen.

   c. Löschen Sie alle Bänder im Archiv. Detaillierte Anweisungen finden Sie unter Virtuelle Bänder von Ihrem Tape Gateway löschen.

2. Löschen Sie das Tape Gateway, sofern Sie nicht vorhaben, es weiter zu verwenden. Anweisungen finden Sie unter Löschen Ihres Gateways und Entfernen der zugehörigen Ressourcen.

3. Löschen Sie die Storage Gateway VM von Ihrem On-Premises-Host. Wenn Sie Ihr Gateway auf einer EC2 Amazon-Instance erstellt haben, beenden Sie die Instance.

Zusätzliche Storage-Gateway-Ressourcen

In diesem Abschnitt werden Software, Tools AWS und Ressourcen von Drittanbietern beschrieben, mit denen Sie Ihr Gateway einrichten oder verwalten können, sowie Storage Gateway Gateway-Kontingente.

Topics

- Bereitstellung und Konfiguration des Gateway-VM-Hosts- Erfahren Sie, wie Sie einen Host für virtuelle Maschinen für Ihr Gateway bereitstellen und konfigurieren.
- Arbeiten mit Tape Gateway-Speicherressourcen- Erfahren Sie mehr über Verfahren im Zusammenhang mit Tape Gateway-Speicherressourcen, wie z. B. das Entfernen lokaler Festplatten, das Verwalten von Amazon EBS-Volumes, das Arbeiten mit virtuellen Bandbibliotheksgeräten und das Verwalten der Bänder in Ihrer virtuellen Bandbibliothek.
- Abrufen eines Aktivierungsschlüssels für das Gateway- Erfahren Sie, wo Sie den Aktivierungsschlüssel finden, den Sie bei der Bereitstellung eines neuen Gateways angeben müssen.
- Verbinden von iSCSI-Initiatoren- Erfahren Sie, wie Sie mit Volumes oder VTL-Geräten (Virtual Tape Library) arbeiten, die als iSCSI-Ziele (Internet Small Computer System Interface) verfügbar sind.
- Verwendung AWS Direct Connect mit Storage Gateway- Erfahren Sie, wie Sie eine dedizierte Netzwerkverbindung zwischen Ihrem lokalen Gateway und der Cloud herstellen. AWS
- Abrufen der IP-Adresse für Ihre Gateway-Appliance- Erfahren Sie, wo Sie die Host-IP-Adresse des Gateways für die virtuelle Maschine finden, die Sie bei der Bereitstellung eines neuen Gateways angeben müssen.
- Grundlegendes zu Storage Gateway Gateway-Ressourcen und -Ressourcen IDs- Erfahren Sie, wie die Ressourcen und Unterressourcen AWS identifiziert werden, die von Storage Gateway erstellt wurden.
- Kennzeichnen der Storage Gateway-Ressourcen- Erfahren Sie, wie Sie mithilfe von Metadaten-Tags Ihre Ressourcen kategorisieren und einfacher verwalten können.
- Arbeiten mit Open-Source-Komponenten für Storage Gateway- Erfahren Sie mehr über die Tools und Lizenzen von Drittanbietern, die zur Bereitstellung der Storage Gateway Gateway-Funktionalität verwendet werden.

- AWS Storage Gateway Kontingente- Erfahren Sie mehr über die Beschränkungen und Kontingente für Tape Gateway, einschließlich der maximalen Beschränkungen für Bandgröße und -menge sowie Empfehlungen zur Größe lokaler Festplatten.

Bereitstellung und Konfiguration des Gateway-VM-Hosts

In den Themen in diesem Abschnitt wird beschrieben, wie Sie den Host für virtuelle Maschinen für Ihre Storage Gateway Gateway-Appliance einrichten und verwalten, einschließlich lokaler Geräte, die auf VMware Hyper-V- oder Linux-KVM ausgeführt werden, und Appliances, die auf EC2 Amazon-Instances in der Cloud ausgeführt werden. AWS

Topics

- Stellen Sie einen EC2 Amazon-Standardhost für Tape Gateway bereit- Erfahren Sie, wie Sie ein Tape Gateway auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mithilfe der Standardspezifikationen bereitstellen und aktivieren.
- Stellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit- Erfahren Sie, wie Sie ein Tape Gateway auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mithilfe benutzerdefinierter Einstellungen bereitstellen und aktivieren.
- Metadatenoptionen für EC2 Amazon-Instances ändern- Erfahren Sie, wie Sie Ihre Amazon EC2 Gateway-Instance so konfigurieren, dass sie eingehende Metadatenanfragen akzeptiert, die IMDS Version 1 (IMDSv1) verwenden oder voraussetzen, dass alle Metadatenanfragen IMDS Version 2 verwenden (IMDSv2).
- Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Hostzeit- Erfahren Sie, wie Sie die Uhrzeit einer lokalen virtuellen Hyper-V- oder Linux-KVM-Gateway-Maschine anzeigen und mit einem Network Time Protocol (NTP) -Server synchronisieren können.
- Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit- Erfahren Sie, wie Sie die Host-Zeit für eine virtuelle VMware Gateway-Maschine überprüfen und bei Bedarf die Uhrzeit festlegen und den Host so konfigurieren, dass seine Uhrzeit automatisch mit einem Network Time Protocol (NTP) -Server synchronisiert wird.
- Konfiguration der Paravirtualisierung auf einem Host VMware - Erfahren Sie, wie Sie die VMware Hostplattform für Ihre Storage Gateway Gateway-Appliance so konfigurieren können, dass sie paravirtuelle Internet Small Computer System Interface Protocol (iSCSI) -Controller verwendet.
- Netzwerkadapter für Ihr Gateway konfigurieren- Erfahren Sie, wie Sie Ihr Gateway so umkonfigurieren können, dass es den VMXNET3 (10-GbE-) Netzwerkadapter verwendet oder mehr

als einen Netzwerkadapter verwendet, sodass von mehreren IP-Adressen aus darauf zugegriffen werden kann.

- Verwenden von VMware vSphere High Availability mit Storage Gateway- Erfahren Sie, wie Sie Ihre Storage-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen schützen können, indem Sie Storage Gateway so konfigurieren, dass es mit VMware vSphere High Availability funktioniert.

Stellen Sie einen EC2 Amazon-Standardhost für Tape Gateway bereit

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

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

> **Note**
>
> AMIs Die Storage Gateway Gateway-Community wird veröffentlicht und vollständig unterstützt von AWS. Sie können sehen, dass es sich bei dem Herausgeber um einen verifizierten Anbieter handelt AWS.

1. Um Amazon einzurichten EC2instance, wählen Sie Amazon EC2 als Host-Plattform im Abschnitt Plattformoptionen des Workflows aus. Anweisungen zur Konfiguration der EC2 Amazon-Instance finden Sie unter Bereitstellen einer EC2 Amazon-Instance zum Hosten Ihres Tape Gateways .
2. Wählen Sie Launch Instance aus, um die AWS Storage Gateway AMI-Vorlage in der EC2 Amazon-Konsole zu öffnen und zusätzliche Einstellungen wie Instance-Typen, Netzwerkeinstellungen und Speicher konfigurieren anzupassen.
3. Optional können Sie in der Storage Gateway Gateway-Konsole die Option Standardeinstellungen verwenden auswählen, um eine EC2 Amazon-Instance mit der Standardkonfiguration bereitzustellen.

   Die EC2 Amazon-Instance, die Use default settings erstellt, hat die folgenden Standardspezifikationen:

   - Instance-Typ – m5.xlarge
   - Netzwerkeinstellungen

- Wählen Sie für VPC die VPC aus, in der Ihre EC2 Instance ausgeführt werden soll.
- Geben Sie für Subnet das Subnetz an, in dem Ihre EC2 Instance gestartet werden soll.

> **Note**
>
> VPC-Subnetze werden nur dann in der Drop-down-Liste angezeigt, wenn für sie die Einstellung zur automatischen Zuweisung öffentlicher IPv4 Adressen in der VPC-Managementkonsole aktiviert ist.

- Öffentliche IP automatisch zuweisen – Aktiviert

Eine EC2 Sicherheitsgruppe wird erstellt und der Instanz zugeordnet. EC2 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 Seite mit den EC2 Amazon-Instance-Details navigieren, Sicherheit auswählen, zu Sicherheitsgruppendetails navigieren und die Sicherheitsgruppen-ID auswählen.

Port	Protocol (Protokoll)	Dateisystem-Protokoll				
80	TCP	HTTP-Zugriff zur Aktivierung				

Port	Protocol (Protokoll)	Dateisystem-Protokoll				
3260	TCP	iSCSI				

- Speicher konfigurieren

Standardeinstellungen	AMI-Root-Volume	Volume 2 Cache	Volume 3 Cache			
Gerätename		/dev/sdf	/dev/sdf			
Größe	80 GiB	250 GiB	250 GiB			
Volume-Typ	gp3	gp3	gp3			
IOPS	3000	3000	3000			
Beim Beenden löschen	Ja	Ja	Ja			
Encrypted	Nein	Nein	Nein			
Durchsatz	125	125	125			

Stellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit

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

> **Note**
>
> AMIs Die Storage Gateway Gateway-Community wird veröffentlicht und vollständig unterstützt von AWS. Sie können sehen, dass es sich bei dem Herausgeber um einen verifizierten Anbieter handelt AWS.
> Tape Gateway AMIs verwendet die folgende Namenskonvention. Die an den AMI-Namen angehängte Versionsnummer ändert sich mit jeder Versionsversion.
> `aws-storage-gateway-CLASSIC-2.9.0`

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

1. Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter Einrichten eines Tape Gateways . Wenn Sie den Bereich Plattformoptionen erreichen, wählen Sie Amazon EC2 als Host-Plattform aus und starten Sie dann mit den folgenden Schritten die EC2 Amazon-Instance, die Ihr Tape Gateway hosten wird.
2. Wählen Sie Launch instance, um die AWS Storage Gateway AMI-Vorlage in der EC2 Amazon-Konsole zu öffnen, wo Sie zusätzliche Einstellungen konfigurieren können.

   Verwenden Sie Quicklaunch, um die EC2 Amazon-Instance mit Standardeinstellungen zu starten. Weitere Informationen zu den Standardspezifikationen von Amazon EC2 Quicklaunch finden Sie unter Quicklaunch-Konfigurationsspezifikationen für Amazon. EC2
3. Geben Sie unter Name einen Namen für die EC2 Amazon-Instance ein. Nachdem die Instance bereitgestellt wurde, können Sie nach diesem Namen suchen, um Ihre Instance auf Listenseiten in der EC2 Amazon-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 EC2 Amazon-Instance-Typen.

   Sie können die Größe der Instance nach dem Start bei Bedarf ändern. Weitere Informationen finden Sie unter Größenänderung Ihrer Instance im EC2 Amazon-Benutzerhandbuch.

> **Note**
>
> Bestimmte Instance-Typen, insbesondere i3 EC2, verwenden NVMe SSD-Festplatten. Dies kann zu Problemen führen, wenn Sie ein Tape Gateway starten oder beenden. Beispielsweise können Sie Daten aus dem Cache verlieren. Überwachen Sie die `CachePercentDirty` CloudWatch Amazon-Metrik und starten oder stoppen Sie Ihr System nur, wenn dieser Parameter aktiviert ist`0`. Weitere Informationen zu Monitoring-Metriken für Ihr Gateway finden Sie in der CloudWatch Dokumentation unter Storage Gateway Gateway-Metriken und -Dimensionen.

5. Wählen Sie im Abschnitt Schlüsselpaar (Anmeldung) für Schlüsselpaarname – erforderlich das Schlüsselpaar aus, das Sie für die sichere Verbindung mit Ihrer Instance verwenden möchten. Bei Bedarf können Sie ein neues Schlüsselpaarname erstellen. Weitere Informationen dazu finden Sie unter Erstellen eines Schlüsselpaares im Amazon-Elastic-Compute-Cloud-Benutzerhandbuch für Linux-Instances.
6. Überprüfen Sie im Abschnitt Netzwerkeinstellungen die vorkonfigurierten Einstellungen und wählen Sie Bearbeiten, um Änderungen an den folgenden Feldern vorzunehmen:

   a. Wählen Sie für VPC — erforderlich die VPC aus, in der Sie Ihre EC2 Amazon-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 EC2 Amazon-Instance starten möchten.

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

> **Note**
>
> Tape Gateway setzt voraus, dass der TCP-Port 80 für eingehenden Datenverkehr und für einmaligen HTTP-Zugriff während der Gateway-Aktivierung geöffnet ist. Nach der Aktivierung können Sie diesen Port schließen.
> Darüber hinaus müssen Sie den TCP-Port 3260 für den iSCSI-Zugriff öffnen.

9. Überprüfen Sie im Unterabschnitt Erweiterte Netzwerkkonfiguration die vorkonfigurierten Einstellungen und nehmen Sie gegebenenfalls Änderungen vor.
10. Wählen Sie im Abschnitt Speicher hinzufügen die Option Neues Volume hinzufügen, um der Gateway-Instance Speicher hinzuzufügen.

> **Important**
>
> Sie müssen zusätzlich zum vorkonfigurierten Root-Volume mindestens ein Amazon EBS-Volume mit mindestens 165 GiB Kapazität für den Cache-Speicher und mindestens ein Amazon EBS-Volume mit mindestens 150 GiB Kapazität für den Upload-Puffer hinzufügen. Für eine höhere Leistung empfehlen wir, mehrere EBS-Volumes für den Cache-Speicher mit jeweils mindestens 150 GiB zuzuweisen.

11. Überprüfen Sie im Abschnitt Erweiterte Details die vorkonfigurierten Einstellungen und nehmen Sie gegebenenfalls Änderungen vor.
12. Wählen Sie Launch instance, 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 EC2 Amazon-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 Gateway-Konsole zurück, um mit der Einrichtung Ihres Tape Gateways fortzufahren.

Sie können die AMI-ID ermitteln, die für den Start eines Tape Gateway Gateways verwendet werden soll, indem Sie die Storage Gateway Gateway-Konsole verwenden oder den AWS Systems Manager Parameterspeicher abfragen.

Um die AMI-ID zu ermitteln, führen Sie einen der folgenden Schritte aus:

- Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter Einrichten eines Tape Gateways . Wenn Sie den Bereich Plattformoptionen erreichen, wählen Sie Amazon EC2 als Host-Plattform und dann Launch Instance aus, um die AWS Storage Gateway AMI-Vorlage in der EC2 Amazon-Konsole zu öffnen.

  Sie werden zur EC2 AMI-Community-Seite weitergeleitet, auf der Sie die AMI-ID für Ihre AWS Region in der URL sehen können.
- Führen Sie eine Abfrage des Systems Manager-Parameterspeichers durch. Sie können die AWS CLI oder Storage Gateway Gateway-API verwenden, um den öffentlichen Parameter von Systems Manager unter dem Namespace `/aws/service/storagegateway/ami/VTL/latest` abzufragen. Wenn Sie beispielsweise den folgenden CLI-Befehl verwenden, wird die ID des aktuellen AMI in der von AWS-Region Ihnen angegebenen zurückgegeben.

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/
  latest
  ```

  Dieser CLI-Befehl gibt etwa die folgende Ausgabe zurück:

  ```
  {
      "Parameter": {
          "Type": "String",
          "LastModifiedDate": 1561054105.083,
          "Version": 4,
          "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/VTL/
  latest",
          "Name": "/aws/service/storagegateway/ami/VTL/latest",
          "Value": "ami-123c45dd67d891000"
      }
  }
  ```

Metadatenoptionen für EC2 Amazon-Instances ändern

Der Instance-Metadaten-Service (IMDS) ist eine On-Instance-Komponente, die sicheren Zugriff auf EC2 Amazon-Instance-Metadaten bietet. Eine Instance kann so konfiguriert werden, dass sie eingehende Metadatenanfragen akzeptiert, die IMDS Version 1 (IMDSv1) verwenden, oder verlangt, dass alle Metadatenanfragen IMDS Version 2 verwenden (). IMDSv2 IMDSv2 verwendet sitzungsorientierte Anfragen und behebt verschiedene Arten von Sicherheitslücken, die beim Versuch, auf das IMDS zuzugreifen, genutzt werden könnten. Weitere Informationen dazu IMDSv2 finden Sie unter So funktioniert Instance Metadata Service Version 2 im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Wir empfehlen, dass Sie IMDSv2 für alle EC2 Amazon-Instances, die Storage Gateway hosten, Folgendes benötigen. IMDSv2 ist standardmäßig für alle neu gestarteten Gateway-Instances erforderlich. Wenn Sie über bestehende Instances verfügen, die noch so konfiguriert sind, dass sie IMDSv1 Metadatenanfragen akzeptieren, finden Sie unter Verwendung von erforderlich IMDSv2 im Amazon Elastic Compute Cloud-Benutzerhandbuch Anweisungen, wie Sie Ihre Instance-Metadatenoptionen so ändern können, dass sie die Verwendung von erfordern IMDSv2. Für die Anwendung dieser Änderung ist kein Neustart der Instance erforderlich.

Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Hostzeit

Für ein Gateway, das auf bereitgestellt wird VMware ESXi, reicht es aus, die Hypervisor-Host-Zeit einzustellen und die Zeit der virtuellen Maschine mit dem Host zu synchronisieren, um Zeitabweichungen zu vermeiden. Weitere Informationen finden Sie unter Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit. Für ein Gateway, das auf Microsoft Hyper-V oder Linux KVM bereitgestellt wird, empfehlen wir, die Uhrzeit der virtuellen Maschine regelmäßig mit dem unten beschriebenen Verfahren zu überprüfen.

Um die Uhrzeit einer virtuellen Hypervisor-Gateway-Maschine anzuzeigen und mit einem NTP-Server (Network Time Protocol) zu synchronisieren

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

   - Weitere Informationen zum Anmelden bei der lokalen Microsoft Hyper-V-Konsole finden Sie unter Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V.
   - Weitere Informationen zur Anmeldung an der lokalen Konsole für Linux Kernel-based Virtual Machine (KVM) finden Sie unter. Zugreifen auf die lokale Konsole des Gateways mit Linux KVM

2. Geben Sie auf dem Hauptmenübildschirm der Storage Gateway Gateway-Konfiguration die entsprechende Zahl ein, um System Time Management auszuwählen.
3. Geben Sie auf dem Menübildschirm System Time Management die entsprechende Ziffer ein, um Systemzeit anzeigen und synchronisieren auszuwählen.

   Die lokale Gateway-Konsole zeigt die aktuelle Systemzeit an und vergleicht sie mit der vom NTP-Server gemeldeten Zeit. Anschließend wird die genaue Abweichung zwischen den beiden Zeiten in Sekunden gemeldet.
4. Wenn die Zeitabweichung mehr als 60 Sekunden beträgt, geben Sie ein, um die Systemzeit mit der NTP-Zeit **y** zu synchronisieren. Geben Sie andernfalls **n** ein.

   Die Zeitsynchronisierung kann einige Augenblicke dauern.

Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit

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

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

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

1. Konfigurieren Sie Ihre VM-Zeit.

   a. Klicken Sie im vSphere-Client im Bereich auf der linken Seite des Anwendungsfensters mit der rechten Maustaste auf den Namen Ihrer Gateway-VM, um das Kontextmenü für die VM zu öffnen, und wählen Sie dann Einstellungen bearbeiten.

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

   b. Wählen Sie die Registerkarte Optionen und dann in der Optionsliste VMware Tools aus.

c. Aktivieren Sie im Bereich „Erweitert“ auf der rechten Seite des Dialogfelds „Eigenschaften der virtuellen Maschine“ die Option „Gastzeit mit Host synchronisieren“ und wählen Sie dann „OK“.

   Die VM synchronisiert ihre Zeit mit dem Host.

2. Konfigurieren Sie die Host-Zeit.

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

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

      Das Dialogfeld Time Configuration (Zeitkonfiguration) wird geöffnet.
   c. Stellen Sie unter Datum und Uhrzeit Datum und Uhrzeit für Ihren vSphere-Host ein.
   d. Konfigurieren Sie den Host so, dass seine Zeit automatisch mit einem NTP-Server synchronisiert wird.

      i. Wählen Sie im Dialogfeld „Zeitkonfiguration“ die Option „Optionen“ und wählen Sie dann im linken Bereich im Dialogfeld „NTP-Daemon (ntpd) -Optionen“ die Option „NTP-Einstellungen“ aus.
      ii. Wählen Sie Add (Hinzufügen), um einen neuen NTP-Server hinzuzufügen.
      iii. Geben Sie im Dialogfeld Add NTP Server (NTP-Server hinzufügen) die IP-Adresse oder den vollqualifizierten Domänennamen eines NTP-Servers ein und wählen Sie dann OK.

         Sie können es `pool.ntp.org` als Domainnamen verwenden.
      iv. Wählen Sie im Dialogfeld mit den Optionen für NTP Daemon (ntpd) im linken Bereich die Option Allgemein aus.
      v. Wählen Sie unter Dienstbefehle die Option Start aus, um den Dienst zu starten.

         Hinweis: Wenn Sie diese NTP-Serverreferenz ändern oder später einen anderen Server hinzufügen, müssen Sie den Service neu starten, um den neuen Server zu verwenden.
   e. Wählen Sie OK, um das Dialogfeld NTP Daemon (ntpd) Options (NTP Daemon(ntpd)-Optionen) zu schließen.

f. Wählen Sie OK, um das Dialogfeld Time Configuration (Zeitkonfiguration) zu schließen.

Konfiguration der Paravirtualisierung auf einem Host VMware

Das folgende Verfahren beschreibt, wie Sie die VMware Hostplattform für Ihre Storage Gateway Gateway-Appliance so konfigurieren, dass sie paravirtuelle Internet Small Computer System Interface Protocol (iSCSI) -Controller verwendet. Paravirtuelle iSCSI-Controller sind leistungsstarke Speichercontroller, die zu einem höheren Durchsatz und einer geringeren CPU-Auslastung führen können. Diese Controller eignen sich am besten für Hochleistungsspeicherumgebungen. Wenn Sie iSCSI-Controller auf diese Weise konfigurieren, arbeitet die virtuelle Storage Gateway Gateway-Maschine mit dem Host-Betriebssystem zusammen, sodass die Gateway-Konsole die virtuellen Laufwerke identifizieren kann, die Sie Ihrer virtuellen Maschine hinzufügen.

> **Note**
>
> Sie müssen diesen Schritt ausführen, um Probleme bei der Identifizierung dieser Festplatten zu vermeiden, wenn Sie sie in der Gateway-Konsole konfigurieren.

So konfigurieren Sie Ihre VMware Host-Plattform für die Verwendung paravirtualisierter Controller

1. Klicken Sie im VMware vSphere-Client im Navigationsbereich auf der linken Seite des Anwendungsfensters mit der rechten Maustaste auf den Namen Ihrer virtuellen Gateway-Maschine, um das Kontextmenü zu öffnen, und wählen Sie dann Einstellungen bearbeiten.
2. Wählen Sie im Dialogfeld Eigenschaften der virtuellen Maschine die Registerkarte Hardware aus.
3. Wählen Sie auf der Registerkarte Hardware die Option SCSI-Controller 0 und dann Typ ändern aus.
4. Wählen Sie im Dialogfeld SCSI-Controllertyp ändern den VMware Paravirtual SCSI-Controllertyp aus, und klicken Sie dann auf OK, um die Konfiguration zu speichern.

Netzwerkadapter für Ihr Gateway konfigurieren

Standardmäßig ist Storage Gateway für die Verwendung des Netzwerkadaptertyps E1000 konfiguriert. Sie können Ihr Gateway jedoch so umkonfigurieren, dass es den Netzwerkadapter VMXNET3 (10 GbE) verwendet. Sie können Storage Gateway auch so konfigurieren, dass mehrere

IP-Adressen darauf zugreifen können. Konfigurieren Sie hierzu Ihr Gateway für die Verwendung mehrerer Netzwerkadapter.

Themen

- Konfigurieren Sie Ihr Gateway für die Verwendung des Netzwerkadapters VMXNET3
- Konfiguration Ihres Gateways für mehrere NICs

Konfigurieren Sie Ihr Gateway für die Verwendung des Netzwerkadapters VMXNET3

Storage Gateway unterstützt den Netzwerkadaptertyp E1000 sowohl in Microsoft Hyper-V-Hypervisor-Hosts als VMware ESXi auch in Microsoft Hypervisor-Hosts. Der Netzwerkadaptertyp VMXNET3 (10 GbE) wird jedoch nur im VMware ESXi Hypervisor unterstützt. Wenn Ihr Gateway auf einem VMware ESXi Hypervisor gehostet wird, können Sie Ihr Gateway so umkonfigurieren, dass es den Adaptertyp VMXNET3 (10 GbE) verwendet. Weitere Informationen zu diesen Adaptern finden Sie unter Auswählen eines Netzwerkadapters für Ihre virtuelle Maschine auf der Broadcom () VMware - Website.

> **Important**
>
> Zur Auswahl VMXNET3 muss Ihr Gastbetriebssystemtyp Anderes Linux64 sein.

Im Folgenden finden Sie die Schritte, die Sie ausführen, um Ihr Gateway für die Verwendung des VMXNET3 Adapters zu 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.

Um den Standard-E1000-Adapter zu entfernen und Ihr Gateway für die Verwendung des VMXNET3 Adapters zu konfigurieren

1. Öffnen Sie in VMware das Kontextmenü (Rechtsklick) für Ihr Gateway und wählen Sie 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. Sie werden diesen Adapter durch den VMXNET3 Adapter ersetzen.
4. Wählen Sie den E1000-Netzwerkadapter und wählen Sie Remove (Entfernen). In diesem Beispiel ist der E1000-Netzwerkadapter Network Adapter 1 (Netzwerkadapter 1).

   > **Note**
   >
   > Sie können den E1000 und die VMXNET3 Netzwerkadapter zwar gleichzeitig in Ihrem Gateway ausführen, wir empfehlen jedoch nicht, dies zu tun, da dies zu Netzwerkproblemen führen 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. Vergewissern Sie sich im Assistenten für die Eigenschaften virtueller Maschinen im Abschnitt Adaptertyp, dass Aktueller Adapter auf eingestellt ist VMXNET3, und wählen Sie dann OK aus.
9. Fahren Sie im VMware VSphere Client Ihr Gateway herunter.
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 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.

Konfiguration Ihres Gateways für mehrere NICs

Wenn Sie Ihr Gateway für die Verwendung mehrerer Netzwerkadapter (NICs) konfigurieren, kann über mehr als eine IP-Adresse darauf zugegriffen werden. 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 wird ein Adapter als Route konfiguriert, mit der das Gateway 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, mit dem kommuniziert wird AWS, fließt der iSCSI-Verkehr für dieses Ziel und der AWS Datenverkehr über denselben Adapter.

Wenn Sie einen Adapter so konfigurieren, das er eine Verbindung mit der Storage-Gateway-Konsole herstellt, und wenn Sie dann einen zweiten Adapter hinzufügen, konfiguriert das Storage Gateway

die Routing-Tabelle automatisch so, dass der zweite Adapter als bevorzugte Route verwendet wird. Anleitungen zur Konfiguration von Mehrfachadaptern finden Sie in den folgenden Abschnitten.

- Konfiguration mehrerer Netzwerkadapter auf einem Host VMware ESXi
- Konfiguration mehrerer Netzwerkadapter auf dem Microsoft Hyper-V-Host

Konfiguration mehrerer Netzwerkadapter auf einem Host VMware ESXi

Das folgende Verfahren geht davon aus, dass für Ihre Gateway-VM bereits ein Netzwerkadapter definiert ist, und es wird beschrieben, wie ein Adapter hinzugefügt wird VMwareESXi.

So konfigurieren Sie Ihr Gateway für die Verwendung eines zusätzlichen Netzwerkadapters im VMware ESXi Host

1. Fahren Sie das Gateway herunter.
2. Wählen Sie im VMware vSphere-Client Ihre Gateway-VM aus.

   Die VM kann für die Dauer dieses Verfahrens aktiviert bleiben.
3. Öffnen Sie im Client das Kontextmenü (Klick mit der rechten Maustaste) für Ihre Gateway-VM, und wählen Sie Edit Settings (Einstellungen bearbeiten).
4. Wählen Sie auf der Registerkarte Hardware im Dialogfeld Virtual Machine Properties (Eigenschaften der virtuellen Maschine) die Option Add (Hinzufügen), um ein Gerät hinzuzufügen.
5. Befolgen Sie die Anweisungen des Hardware-Assistenten zum Hinzufügen eines Netzwerkadapters.

   a. Wählen Sie im Fenster Device Type (Gerätetyp) die Option Ethernet Adapter, um einen Adapter hinzuzufügen, und wählen Sie dann Next (Weiter).

   b. Stellen Sie sicher, dass im Fenster Network Type (Netzwerktyp) die Option Connect at power on (Verbindung bei Einschalten der Energie herstellen) für Type (Typ) ausgewählt ist, und wählen Sie dann Next (Weiter).

      Wir empfehlen, den VMXNET3 Netzwerkadapter mit Storage Gateway zu verwenden. Weitere Informationen zu den Adaptertypen, die möglicherweise in der Adapterliste erscheinen, finden Sie unter Netzwerkadaptertypen in der ESXi und der vCenter Server-Dokumentation.

c. Prüfen Sie im Fenster Ready to Complete (Bereit zum Abschließen) die Informationen und wählen Sie Finish (Fertigstellen).

6. Wählen Sie die Registerkarte Übersicht der VM und anschließend Alle anzeigen neben dem Kontrollkästchen IP-Adresse. Das Fenster IP-Adresse der virtuellen Maschine zeigt alle IP-Adressen an, die Sie für den Zugriff auf das Gateway verwenden können. Vergewissern Sie sich, dass für das Gateway eine zweite IP-Adresse gelistet ist.

> **Note**
>
> Es kann einige Minuten dauern, bis die Adapteränderungen wirksam und die zusammenfassenden VM-Informationen aktualisiert werden.

7. Schalten Sie in der Storage-Gateway-Konsole das Gateway ein.
8. Wählen Sie im Fenster Navigation der Storage-Gateway-Konsole die Option Gateways und anschließend das Gateway, dem Sie den Adapter hinzugefügt haben. Vergewissern Sie sich, dass die zweite IP-Adresse in der Registerkarte Details aufgeführt wird.

Informationen zu lokalen Konsolenaufgaben VMware, die bei Hyper-V- und KVM-Hosts häufig auftreten, finden Sie unter Ausführen von Aufgaben in der lokalen VM-Konsole von

Konfiguration mehrerer Netzwerkadapter auf dem Microsoft Hyper-V-Host

Im folgenden Verfahren wird davon ausgegangen, dass für Ihre Gateway-VM bereits ein Netzwerkadapter definiert wurde und Sie einen zweiten Adapter hinzufügen. In diesem Verfahren wird zeigt, wie Sie einen Adapter für einen Microsoft Hyper-V-Host hinzufügen.

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

1. Schalten Sie in der Storage-Gateway-Konsole das Gateway aus.
2. Wählen Sie im Microsoft Hyper-V Manager Ihre Gateway-VM im Bereich Virtuelle Maschinen aus.
3. Wenn die Gateway-VM noch nicht ausgeschaltet ist, klicken Sie mit der rechten Maustaste auf den VM-Namen, um das Kontextmenü zu öffnen, und wählen Sie dann Ausschalten.
4. Klicken Sie mit der rechten Maustaste auf den Namen der Gateway-VM, um das Kontextmenü zu öffnen, und wählen Sie dann Einstellungen.
5. Wählen Sie im Dialogfeld Einstellungen unter Hardware die Option Hardware hinzufügen aus.

6. Wählen Sie im Bereich „Hardware hinzufügen“ auf der rechten Seite des Dialogfelds „Einstellungen“ die Option „Netzwerkadapter“ und dann „Hinzufügen“, um ein Gerät hinzuzufügen.
7. Konfigurieren Sie den Netzwerkadapter, und wählen Sie dann Apply (Anwenden), um die Einstellungen anzuwenden.
8. Vergewissern Sie sich im Dialogfeld Einstellungen unter Hardware, dass der neue Netzwerkadapter zur Hardwareliste hinzugefügt wurde, und klicken Sie dann auf OK.
9. Schalten Sie das Gateway über die Storage Gateway Gateway-Konsole ein.
10. Wählen Sie im Navigationsbereich der Storage Gateway Gateway-Konsole Gateways und dann das Gateway aus, zu dem Sie den Adapter hinzugefügt haben. Vergewissern Sie sich, dass auf der Registerkarte Details eine zweite IP-Adresse aufgeführt ist.

Informationen zu Aufgaben auf lokalen Konsolen VMware, die bei Hyper-V- und KVM-Hosts häufig auftreten, finden Sie unter Ausführen von Aufgaben in der lokalen VM-Konsole von

Verwenden von VMware vSphere High Availability mit Storage Gateway

Storage Gateway bietet Hochverfügbarkeit VMware durch eine Reihe von Integritätsprüfungen auf Anwendungsebene, die in VMware vSphere High Availability (VMware HA) integriert sind. Dieser Ansatz schützt Speicher-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen. Darüber hinaus schützt er vor Softwarefehlern wie beispielsweise Timeouts während der Verbindung und Nichtverfügbarkeit von Dateifreigaben oder Volumes.

vSphere HA bündelt virtuelle Maschinen und die Hosts, auf denen sie sich befinden, aus Redundanzgründen in einem Cluster. Die Hosts im Cluster werden überwacht, und im Falle eines Fehlers 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 in der Dokumentation unter So funktioniert vSphere HA. VMware

> **Note**
>
> Die Zeit, die benötigt wird, um eine ausgefallene virtuelle Maschine neu zu starten und die iSCSI-Verbindung auf einem neuen Host wiederherzustellen, hängt von vielen Faktoren ab, z. B. vom Host-Betriebssystem und der Ressourcenauslastung, der Festplattengeschwindigkeit, der Netzwerkverbindung und der SAN-/Speicherinfrastruktur. Um Ausfallzeiten beim Failover

zu minimieren, sollten Sie die unter Optimierung der Gateway-Leistung — aufgeführten Empfehlungen umsetzen.

Um Storage Gateway mit VMware HA zu verwenden, empfehlen wir die folgenden Schritte:

- Stellen Sie das `.ova` herunterladbare VMware ESX-Paket, das die Storage Gateway Gateway-VM enthält, auf nur 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.

In den folgenden Themen wird beschrieben, wie Storage Gateway in einem VMware HA-Cluster bereitgestellt wird:

Themen

- Konfigurieren Sie Ihren vSphere VMware HA-Cluster
- Herunterladen des OVA-Image von der Storage-Gateway-Konsole
- Bereitstellen des Gateways
- (Optional) Fügen Sie in Ihrem Cluster Überschreibungsoptionen für andere Optionen hinzu VMs
- Aktivieren des Gateways

- Testen Sie Ihre VMware Hochverfügbarkeitskonfiguration

Konfigurieren Sie Ihren vSphere VMware HA-Cluster

Wenn Sie noch keinen VMware Cluster erstellt haben, erstellen Sie zunächst einen. Informationen zum Erstellen eines VMware Clusters finden Sie in der VMware Dokumentation unter Erstellen eines vSphere HA-Clusters.

Als Nächstes konfigurieren Sie Ihren VMware Cluster so, dass er mit Storage Gateway funktioniert.

Um Ihren VMware Cluster zu konfigurieren

1. Stellen Sie auf der Seite Clustereinstellungen bearbeiten in VMware vSphere sicher, dass die VM-Überwachung für die VM- und Anwendungsüberwachung konfiguriert ist. Stellen Sie dazu für jede Option die folgenden Werte ein:

   - Antwort auf einen Hostfehler: Neustart VMs
   - Reaktion auf die Hostisolierung: Herunterfahren und neu starten VMs
   - Datastore with PDL (Datenspeicher mit PDL): Disabled (Deaktiviert)
   - Datastore with APD (Datenspeicher mit APD): Disabled (Deaktiviert)
   - VM Monitoring (VM-Überwachung): VM and Application Monitoring (VM- und Anwendungsüberwachung)
2. Optimieren Sie die Empfindlichkeit des Clusters, indem Sie die folgenden Werte anpassen:

   - Fehlerintervall: Nach diesem Intervall wird die VM neu gestartet, wenn kein VM-Heartbeat empfangen wird.
   - Mindestbetriebszeit: Der Cluster wartet so lange nach dem Start einer VM, bevor mit der Überwachung des Heartbeat von VM-Tools begonnen wird.
   - Maximale Zurücksetzungen pro VM: Der Cluster startet die VM innerhalb des Zeitfensters für maximale Zurücksetzungen höchstens so viele Male.
   - Zeitfenster für maximale Zurücksetzungen: Das Zeitfenster, in dem die maximalen Zurücksetzungen pro VM gezählt werden sollen.

   Wenn Sie nicht sicher sind, welche Werte Sie festlegen sollen, verwenden Sie die folgenden Beispieleinstellungen:

   - Failure interval (Fehlerintervall): **30** Sekunden

- Minimum uptime (Mindestbetriebszeit): **120** Sekunden
- Maximum per-VM resets (Maximale Zurücksetzungen pro VM): **3**
- Maximum resets time window (Zeitfenster für maximale Zurücksetzungen): **1** Stunde

Wenn andere auf dem Cluster VMs ausgeführt werden, sollten Sie diese Werte möglicherweise speziell für Ihre VM festlegen. Dies ist erst möglich, wenn Sie die VM über das OVA-Image bereitstellen. Weitere Hinweise zum Festlegen dieser Werte finden Sie unter (Optional) Fügen Sie in Ihrem Cluster Überschreibungsoptionen für andere Optionen hinzu VMs .

Herunterladen des OVA-Image von der Storage-Gateway-Konsole

So laden Sie das OVA-Image für Ihren Gateway-Typ herunter

- Wählen Sie auf der Seite Gateway einrichten in der Storage-Gateway-Konsole Ihren Gateway-Typ und Ihre Host-Plattform aus und verwenden Sie dann den Link in der Konsole, um die OVA-Datei herunterzuladen, wie unter Einrichten von Tape Gateway beschrieben.

Bereitstellen des Gateways

Stellen Sie das OVA-Image in Ihrem konfigurierten Cluster auf einem der Cluster-Hosts bereit.

So stellen Sie das OVA-Image des Gateways bereit

1. Stellen Sie das OVA-Image auf einem der Hosts im Cluster bereit.
2. Stellen Sie sicher, dass die Datenspeicher, die Sie für den Stamm-Datenträger und den Cache wählen, für alle Hosts im Cluster verfügbar sind. Bei der Bereitstellung der Storage Gateway Gateway-.ova-Datei in einer VMware oder einer lokalen 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 (Rechtsklick) für Ihre Gateway-VM und wählen Sie dann Einstellungen bearbeiten aus.

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 SCSI-Controllertyp ändern den VMware Paravirtual SCSI-Controllertyp und dann OK aus.

(Optional) Fügen Sie in Ihrem Cluster Überschreibungsoptionen für andere Optionen hinzu VMs

Wenn andere auf Ihrem Cluster VMs ausgeführt werden, möchten Sie die Clusterwerte möglicherweise speziell für jede VM festlegen. Anweisungen finden Sie unter Anpassen einer einzelnen virtuellen Maschine in der VMware vSphere-Online-Dokumentation.

Um Optionen zum Außerkraftsetzen für andere Optionen VMs in Ihrem Cluster hinzuzufügen

1. Wählen Sie auf der Übersichtsseite in VMware vSphere Ihren Cluster aus, um die Clusterseite zu öffnen, und wählen Sie dann Configure aus.
2. Wählen Sie die Registerkarte Configuration (Konfiguration) und dann VM Overrides (VM-Überschreibungen)aus.
3. Fügen Sie eine neue VM-Überschreibungsoption hinzu, um die einzelnen Werte zu ändern.

   Legen Sie die folgenden Werte für jede Option unter vSphere HA — VM-Überwachung fest:

   - VM-Überwachung: Override Enabled — VM- und Anwendungsüberwachung
   - Empfindlichkeit der VM-Überwachung: Override aktiviert — VM- und Anwendungsüberwachung
   - VM-Überwachung: Benutzerdefiniert
   - Ausfallintervall: **30** Sekunden
   - Minimale Betriebszeit: Sekunden **120**
   - Maximum per-VM resets (Maximale Zurücksetzungen pro VM): **5**
   - Maximales Zeitfenster für das Zurücksetzen: Innerhalb von Stunden **1**

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. Connect Ihr Tape Gateway mit AWS
  b. Überprüfen der Einstellungen und Aktivieren von Tape Gateway
  c. Konfigurieren von Tape Gateway

Testen Sie Ihre VMware Hochverfügbarkeitskonfiguration

Testen Sie Ihre Konfiguration, nachdem Sie Ihr Gateway aktiviert haben.

Um Ihre VMware HA-Konfiguration zu testen

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und dann das Gateway aus, das Sie auf VMware HA testen möchten.
3. Wählen Sie für Aktionen die Option Verify VMware HA aus.
4. Wählen Sie im daraufhin angezeigten Feld „ VMware Hochverfügbarkeitskonfiguration überprüfen“ die Option OK aus.

   > **Note**
   >
   > Beim Testen Ihrer VMware HA-Konfiguration wird Ihre Gateway-VM neu gestartet und die Konnektivität zu Ihrem Gateway unterbrochen. Der Test kann einige Minuten in Anspruch nehmen.

   Wenn der Test erfolgreich abgeschlossen wurde, wird der Status Verified (Überprüft) auf der Registerkarte „Details“ des Gateways in der Konsole angezeigt.
5. Wählen Sie Exit (Beenden) aus.

Informationen zu VMware HA-Ereignissen finden Sie in den CloudWatch Amazon-Protokollgruppen. Weitere Informationen finden Sie unter Abrufen von Tape Gateway-Integritätsprotokollen mit CloudWatch Protokollgruppen .

Arbeiten mit Tape Gateway-Speicherressourcen

In den Themen dieses Abschnitts wird beschrieben, wie Sie die mit Ihrem Tape Gateway verbundenen Speicherressourcen verwalten, wie z. B. die physischen Festplatten, die an die virtuelle Hostplattform eines Gateways angeschlossen sind, die Amazon EBS-Volumes, die mit der EC2 Amazon-Instance eines Gateways verbunden sind, Ihre virtuellen Bandbibliotheksgeräte wie Medienwechsler und die Bänder in Ihren virtuellen Bandbibliotheken.

Topics

- Entfernen von Datenträgern aus dem Gateway- Erfahren Sie, was zu tun ist, wenn Sie eine Festplatte von der virtuellen Hostplattform für Ihr Gateway entfernen müssen, z. B. wenn Ihre Festplatte ausgefallen ist.
- Verwaltung von Amazon EBS-Volumes auf Amazon Gateways EC2- Erfahren Sie, wie Sie die Menge der Amazon EBS-Volumes erhöhen oder reduzieren können, die für die Verwendung als Upload-Puffer oder Cache-Speicher für ein Gateway reserviert sind, das auf einer Amazon-Instance gehostet wird. EC2
- Arbeiten mit VTL-Geräten- Erfahren Sie, wie Sie Ihre virtuellen Bandbibliotheksgeräte verwalten, einschließlich der Auswahl eines Medienwechsels für ein Tape Gateway, der Aktualisierung des Gerätetreibers für einen Medienwechsler und der Anzeige von Barcodes für Bänder in Microsoft System Center Data Protection Manager.
- Bänder in Ihrer virtuellen Bandbibliothek verwalten- Erfahren Sie, wie Sie die mit Ihrem Tape Gateway verknüpften Bänder und virtuellen Bandbibliotheken verwalten und wie Sie Bänder manuell archivieren und die laufende Bandarchivierung abbrechen.

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 einer Festplatte von einem Gateway, auf dem gehostet wird VMware ESXi

Sie können das folgende Verfahren verwenden, um eine Festplatte von Ihrem Gateway zu entfernen, die auf dem VMware Hypervisor gehostet wird.

Um eine Festplatte zu entfernen, die dem Upload-Puffer zugewiesen ist () VMware ESXi

1. Öffnen Sie im vSphere-Client das Kontextmenü (Klick mit der rechten Maustaste), wählen Sie den Namen der Gateway-VM und dann Einstellungen bearbeiten.
2. Klicken Sie auf der Registerkarte Hardware im Dialogfeld Eigenschaften der virtuellen Maschine auf den als Upload-Pufferspeicher zugewiesenen Datenträger und wählen Sie dann Entfernen.

   Stellen Sie sicher, dass der Wert Virtueller Geräteknoten im Dialogfeld Eigenschaften der virtuellen Maschine den gleichen Wert hat, den Sie zuvor notiert haben. Auf diese Weise stellen Sie sicher, dass Sie den richtigen Datenträger entfernen.
3. Wählen Sie eine Option im Bereich Optionen zum Entfernen und wählen Sie dann OK, um den Datenträger vollständig zu entfernen.

Entfernen eines Datenträgers aus einem auf Microsoft Hyper-V gehosteten Gateway

Sie können mit dem folgenden Verfahren einen Datenträger aus dem auf Microsoft Hyper-V gehosteten Gateway entfernen.

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

1. Öffnen Sie im Microsoft Hyper-V-Manager das Kontextmenü (Klick mit der rechten Maustaste), wählen Sie den Namen der Gateway-VM und dann Einstellungen.
2. Klicken Sie in der Liste Hardware auf das Dialogfeld Einstellungen, wählen Sie den zu entfernenden Datenträger, und klicken Sie auf Entfernen.

   Die Datenträger, die Sie einem Gateway hinzufügen, werden unter dem Eintrag SCSI-Controller in der Liste Hardware angezeigt. Überprüfen Sie, ob die Werte Controller und Speicherort denselben Wert haben, den Sie zuvor notiert haben. Auf diese Weise stellen Sie sicher, dass Sie den richtigen Datenträger entfernen.

   Der erste SCSI-Controller im Microsoft Hyper-V-Manager ist Controller 0.
3. Klicken Sie auf OK, um die Änderungen anzuwenden.

Entfernen eines Datenträgers aus einem auf Linux KVM gehosteten Gateway

Um eine Festplatte von Ihrem Gateway zu trennen, das auf einem Linux KVM-Hypervisor (kernelbasierte 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.

Verwaltung von Amazon EBS-Volumes auf Amazon Gateways EC2

Als Sie Ihr Gateway ursprünglich für die Ausführung als EC2 Amazon-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 EC2 Amazon-Benutzerhandbuch.

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 Anweisungen finden Sie unter Erstellen oder Wiederherstellen eines Amazon EBS-Volumes im EC2 Amazon-Benutzerhandbuch.
2. Hängen Sie das Amazon EBS-Volume an Ihre EC2 Amazon-Instance an. Anweisungen finden Sie unter Anhängen eines Amazon EBS-Volumes an eine Instance im EC2 Amazon-Benutzerhandbuch.
3. Konfigurieren Sie das von Ihnen hinzugefügte Amazon-EBS-Volume als Upload-Puffer oder Cache-Speicher. Detaillierte Anweisungen finden Sie unter Verwaltung von lokalen Festplatten für Ihr Storage Gateway.

In manchen Fällen stellen Sie möglicherweise fest, dass die Speicherkapazität, die Sie für den Upload-Puffer konfiguriert haben, nicht benötigt wird.

So entfernen Sie ein Amazon-EBS-Volume

> **Warning**
>
> Diese Schritte gelten nur für Amazon-EBS-Volumes, die als Upload-Pufferspeicher zugewiesen wurden, nicht für Volumes, die dem Cache zugewiesen sind. Wenn Sie ein Amazon-EBS-Volume, das als Cache-Speicher zugeordnet ist, von einem Tape Gateway entfernen, haben die virtuellen Bänder des Gateways den Status IRRECOVERABLE und es besteht das Risiko von Datenverlust. Weitere Informationen zum Status IRRECOVERABLE finden Sie unter Grundlegendes zu Bandstatusinformationen in einer VTL.

1. Fahren Sie das Gateway mit dem im Abschnitt Herunterfahren der Gateway-VM beschriebenen Verfahren herunter.
2. Trennen Sie das Amazon EBS-Volume von Ihrer EC2 Amazon-Instance. Anweisungen finden Sie unter Trennen eines Amazon EBS-Volumes von einer Instance im EC2 Amazon-Benutzerhandbuch.
3. Löschen Sie das Amazon-EBS-Volume. Anweisungen finden Sie unter Löschen eines Amazon EBS-Volumes im EC2 Amazon-Benutzerhandbuch.
4. Starten Sie das Gateway mit dem im Abschnitt Herunterfahren der Gateway-VM beschriebenen Verfahren.

Arbeiten mit VTL-Geräten

Bei der Aktivierung Ihres Tape Gateways wählen Sie Ihre Backup-Anwendung aus der Liste aus und verwenden den entsprechenden Medienwechsler. Wenn Ihre Sicherungsanwendung nicht aufgeführt ist, wählen Sie Other (Sonstiges) und dann den Medienwechsler aus, der mit der Sicherungsanwendung funktioniert. Eine Liste der empfohlenen Medienwechsler für unterstützte Backup-Anwendungen finden Sie unter. https://docs.aws.amazon.com/storagegateway/latest/tgw/Requirements.html#requirements-backup-sw-for-vtl

Ihr Tape Gateway-Setup bietet die folgenden iSCSI-Geräte, die Sie bei der Aktivierung Ihres Gateways auswählen.

Mittlere Wechsler:

- AWS-Gateway-VTL: Dieses Gerät wird mit dem Gateway bereitgestellt.
- STK-L700: Diese Geräteemulation wird mit dem Gateway bereitgestellt.

Bandlaufwerke:

- IBM- ULT358 0- TD5 — Diese Geräteemulation ist im Lieferumfang des Gateways enthalten.

Themen

- Auswählen eines Medienwechslers nach der Gateway-Aktivierung
- Aktualisieren des Gerätetreibers für den Medienwechsler
- Anzeigen von Barcodes für Bänder in Microsoft System Center DPM

Auswählen eines Medienwechslers nach der Gateway-Aktivierung

Nach der Aktivierung des Gateways können Sie einen anderen Medienwechslertyp auswählen.

So wählen Sie einen anderen Medienwechsler nach der Gateway-Aktivierung aus

1. Stoppen Sie alle zugehörigen Aufträge, die in der Sicherungssoftware ausgeführt werden.
2. Öffnen Sie auf dem Windows-Server das Fenster mit den iSCSI-Initiator-Eigenschaften.
3. Wählen Sie die Registerkarte Targets (Ziele), um die erkannten Ziele anzuzeigen.
4. Wählen Sie im Bereich mit den erkannten Zielen den Medienwechsler, den Sie ändern möchten, wählen Sie Disconnect (Verbindung trennen) und dann OK.
5. Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Gateways und dann das Gateway aus, dessen Medienwechsler Sie ändern möchten.
6. Wählen Sie die Registerkarte VTL Devices (VTL-Geräte) aus, wählen Sie den Medienwechsler, den Sie ändern möchten, und klicken Sie dann auf die Schaltfläche Change Media Changer (Medienwechsler ändern).
7. Wählen Sie im angezeigten Dialogfeld zum Ändern des Medienwechslertyps den gewünschten Medienwechsler aus dem Dropdown-Listenfeld aus und klicken Sie dann auf Save (Speichern).

Aktualisieren des Gerätetreibers für den Medienwechsler

1. Öffnen Sie den Geräte-Manager auf dem Windows-Server und erweitern Sie die Struktur Medium Changer devices (Wechselmediengeräte) .

2. Öffnen Sie das Kontextmenü (rechte Maustaste) für Unbekannte Medienwechsler und wählen Sie Treibersoftware aktualisieren, um das Fenster Treibersoftware aktualisieren-unbekannter Medienwechsler zu öffnen.
3. Wählen Sie im Abschnitt How do you want to search for driver software? (Wie möchten Sie nach Treibersoftware suchen?) die Option Browse my computer for driver software (Auf dem Computer nach Treibersoftware suchen).
4. Wählen Sie Let me pick from a list of device drivers on my computer (Aus einer Liste von Gerätetreibern auf dem Computer auswählen).

> **Note**
>
> Wir empfehlen die Verwendung des Sony TSL-A500C-Autoloader-Treibers mit der Sicherungssoftware Veeam Backup & Replication 11A und Microsoft System Center Data Protection Manager. Dieser Treiber von Sony wurde mit diesen Arten von Sicherungssoftware bis einschließlich Windows Server 2019 getestet.

5. Deaktivieren Sie im Bereich Select the device driver you want to install for this hardware (Wählen Sie den für diese Hardware zu installierenden Gerätetreiber.) das Kontrollkästchen Show compatible hardware (Kompatible Hardware anzeigen), wählen Sie Sony in der Liste Manufacturer (Hersteller), wählen Sie Sony TSL-A500C-Autoloader in der Liste Model (Modell) und klicken Sie dann auf Next (Weiter).
6. Ein Warnungsfeld wird angezeigt. Klicken Sie in diesem Feld auf Yes (Ja). Wenn der Treiber erfolgreich installiert wurde, schließen Sie das Fenster Update drive software (Treibersoftware aktualisieren).

Anzeigen von Barcodes für Bänder in Microsoft System Center DPM

Wenn Sie den Medienwechslertreiber für Sony TSL-A500C Autoloader verwenden, zeigt Microsoft System Center Data Protection Manager nicht automatisch Barcodes für virtuelle Bänder an, die in Storage Gateway erstellt wurden. Um die Barcodes für Ihre Bänder korrekt anzuzeigen, ändern Sie den Media Changer-Treiber auf Sun/ Library. StorageTek

Anzeigen von Barcodes

1. Stellen Sie sicher, dass alle Sicherungsaufträge abgeschlossen sind und keine Aufgaben ausstehend oder in Bearbeitung sind.

2. Werfen Sie die Bänder aus, verschieben Sie sie zum Offline-Speicher („S3 Glacier Flexible Retrieval“ oder „S3 Glacier Deep Archive“) und beenden Sie die DPM-Administratorkonsole. Weitere Informationen zum Auswerfen eines Bands in DPM finden Sie unter Archivieren eines Bands mithilfe von DPM.
3. Wählen Sie unter Administrative Tools die Option Services aus und öffnen Sie das Kontextmenü (rechte Maustaste) für DPM Service im Bereich Detail. Wählen Sie dann Properties (Eigenschaften) aus.
4. Stellen Sie auf der Registerkarte General (Allgemein) sicher, dass der Startup type (Starttyp) auf Automatic (Automatisch) festgelegt ist, und wählen Sie Stop (Stopp) aus, um den DPM-Dienst zu stoppen.
5. Holen Sie sich die StorageTek Treiber aus dem Microsoft Update Catalog auf der Microsoft-Website.

   > **Note**
   >
   > Beachten Sie die unterschiedlichen Treiber für die verschiedenen Größen.

   Wählen Sie für Größe 18K x86-Treiber.

   Wählen Sie für Größe 19K, x64-Treiber.
6. Öffnen Sie den Geräte-Manager auf Ihrem Windows-Server und erweitern Sie die Struktur Medium Changer Devices (Wechselmediengeräte).
7. Öffnen Sie das Kontextmenü (rechte Maustaste) für Unbekannte Medienwechsler und wählen Sie Treibersoftware aktualisieren, um das Fenster Treibersoftware aktualisieren-unbekannter Medienwechsler zu öffnen.
8. Navigieren Sie zum Pfad des neuen Treiberortes und installieren Sie ihn. Der Treiber wird als StorageTek Sun/Library angezeigt. Bei den Bandlaufwerken handelt es sich weiterhin um ULT358 sequentielle IBM TD5 0-SCSI-Geräte.
9. Starten Sie den DPM-Server neu.
10. Erstellen Sie in der Storage-Gateway-Konsole neue Bänder.
11. Öffnen Sie die DPM-Administratorkonsole und wählen Sie Management und dann Rescan for new tape libraries (Nach neuen Bandbibliotheken suchen) aus. Sie sollten die StorageTek Sun/Library sehen.
12. Wählen Sie die Bibliothek und dann Inventory (Bestand) aus.

13. Wählen Sie Add Tapes (Bänder hinzufügen) aus, um neue Bänder in DPM hinzuzufügen. Für die neuen Bänder sollte nun der Barcode angezeigt werden.

Bänder in Ihrer virtuellen Bandbibliothek verwalten

Storage Gateway stellt für jedes Tape Gateway, das Sie aktivieren, eine virtuelle Bandbibliothek (Virtual Tape Library, VTL) bereit. Die Bibliothek enthält anfangs keine Bänder, aber Sie können jederzeit Bänder erstellen. Ihre Anwendung kann von allen Bändern lesen und auf alle Bänder schreiben, die auf Ihrem Tape Gateway verfügbar sind. Der Status eines Bands muss AVAILABLE sein, damit Sie auf das Band schreiben können. Diese Bänder werden von Amazon Simple Storage Service (Amazon S3) unterstützt. Wenn Sie also auf diese Bänder schreiben, speichert das Tape Gateway Daten in Amazon S3. Weitere Informationen finden Sie unter Grundlegendes zu Bandstatusinformationen in einer VTL.

Themen

- Archivieren von Bändern
- Abbrechen der Bandarchivierung

Die Bandbibliothek zeigt Bänder in Ihrem Tape Gateway an. Die Bibliothek zeigt den Barcode, den Status und die Größe, die verwendete Menge des Bands und das Gateway, dem das Band zugeordnet ist.

Wenn Sie über eine große Anzahl von Bändern in der Bibliothek verfügen, unterstützt die Konsole die Suche nach Bändern anhand des Barcodes, des Status oder beider. Wenn Sie nach Barcode suchen, können Sie nach Status und Gateway filtern.

So suchen Sie nach Barcode, Status und Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Tapes (Bänder) und geben Sie dann einen Wert in das Suchfeld ein. Der Wert kann der Barcode, der Status oder das Gateway sein. Standardmäßig sucht Storage Gateway nach allen virtuellen Bändern. Sie können die Suche jedoch auch nach Status filtern.

   Wenn Sie nach Status filtern, werden Bänder, die Ihren Kriterien entsprechen, in der Bibliothek in der Storage-Gateway-Konsole angezeigt.

Wenn Sie nach Gateway filtern, werden Bänder, die dem Gateway zugeordnet sind, in der Bibliothek in der Storage-Gateway-Konsole angezeigt.

> **Note**
>
> Standardmäßig zeigt Storage Gateway alle Bänder unabhängig vom Status an.

Archivieren von Bändern

Sie können die virtuellen Bänder, die sich in Ihrem Tape Gateway befinden, archivieren. Wenn Sie ein Band archivieren, verschiebt Storage Gateway das Band in das Archiv.

Um ein Band zu archivieren, verwenden Sie Ihre Backup-Software. Der Bandarchivierungsprozess besteht aus drei Phasen entsprechend dem Bandstatus IN TRANSIT TO VTS (IN DER ÜBERTRAGUNG ZU VTS), ARCHIVING (ARCHIVIERUNG WIRD AUSGEFÜHRT) und ARCHIVED (ARCHIVIERT):

- Um ein Band zu archivieren, verwenden Sie den Befehl der von Ihrer Backup Anwendung bereitgestellt wird. Wenn der Archivierungsprozess beginnt, wechselt der Bandstatus zu TRANSIT TO VTS (ÜBERTRAGUNG ZU VTS) und das Band ist für Ihre Backup-Anwendung nicht länger verfügbar. In dieser Phase lädt Ihr Tape Gateway Daten auf AWS. Bei Bedarf können Sie die Archivierung die am laufen ist, abbrechen. Weitere Informationen, über Abbrechen des Archivierens, finden Sie unter Abbrechen der Bandarchivierung.

  > **Note**
  >
  > Die Schritte zum Archivieren eines Bandes hängt von Ihrer Sicherungsanwendung ab. Detaillierte Anweisungen finden Sie in der Dokumentation zu Ihrer Sicherungsanwendung.

- Nachdem der Datenupload AWS abgeschlossen ist, ändert sich der Bandstatus in ARCHIVIERUNG und Storage Gateway beginnt, das Band in das Archiv zu verschieben. Sie können den Archivierungsprozess zu diesem Zeitpunkt nicht abbrechen.
- Nachdem das Band in das Archiv verschoben wurde, ändert sich der Status in ARCHIVED (ARCHIVIERT) und Sie können das Band mit allen Ihren Gateways abrufen. Weitere Informationen, zum Bänderabruf, finden Sie unter Abrufen archivierter Bänder.

Die Schritte zum Archivieren eines Bandes hängen von Ihrer Backup Software ab. Anweisungen zum Archivieren eines Bandes mithilfe der NetBackup Symantec-Software finden Sie unter Archivieren des Bandes.

Abbrechen der Bandarchivierung

Nachdem Sie die Archivierung eines Bandes gestartet haben, kann es vorkommen, dass Sie das Band wieder benötigen. Beispielsweise möchten Sie den Archivierungsprozess abbrechen und das Band zurück haben, weil der Archivierungsprozess zu lange dauert oder Sie Daten von dem Band lesen möchten. Ein Band, das archiviert wird, durchläuft drei Status, wie im Folgenden gezeigt:

- IN TRANSIT TO VTS: Das Tape Gateway lädt Daten in AWS hoch.
- ARCHIVING: Das Hochladen der Daten ist beendet und das Tape Gateway verschiebt das Band ins Archiv.
- ARCHIVED: Das Band wurde ins Archiv verschoben und steht zum Abruf zur Verfügung.

Sie können die Archivierung nur abbrechen, wenn der Status des Bandes IN TRANSIT TO VTS lautet. Abhängig von Faktoren wie Upload-Bandbreite und Menge der Daten, die hochgeladen werden, kann der Status in der Storage-Gateway-Konsole angezeigt werden oder nicht. Um eine Bandarchivierung abzubrechen, verwenden Sie die CancelRetrievalAktion in der API-Referenz.

Abrufen eines Aktivierungsschlüssels für das Gateway

Um einen Aktivierungsschlüssel für Ihr Gateway zu erhalten, stellen Sie eine Webanforderung an die virtuelle Gateway-Maschine (VM). Die VM gibt eine Umleitung zurück, die den Aktivierungsschlüssel enthält, der als einer der Parameter für die `ActivateGateway`-API-Aktion zur Angabe der Konfiguration Ihres Gateways übergeben wird. Weitere Informationen finden Sie ActivateGatewayin der Storage Gateway API-Referenz.

> **Note**
>
> Gateway-Aktivierungsschlüssel laufen nach 30 Minuten ab, wenn sie nicht verwendet werden.

Die Anfrage, die Sie an die Gateway-VM stellen, umfasst die AWS Region, in der die Aktivierung erfolgt. Die URL, die von der Umleitung in der Antwort zurückgegeben wird, enthält einen Abfragezeichenfolgenparameter namens `activationkey`. Dieser

Abfragezeichenfolge-Parameter ist Ihr Aktivierungsschlüssel. Das Format der Abfragezeichenfolge: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. Mit der Ausgabe dieser Abfrage werden sowohl die Aktivierungsregion als auch der Aktivierungsschlüssel zurückgegeben.

Die URL enthält auch `vpcEndpoint`, die VPC-Endpunkt-ID für Gateways, die über den VPC-Endpunkttyp eine Verbindung herstellen.

> **Note**
>
> Die Storage Gateway Gateway-Hardware-Appliance, die VM-Image-Vorlagen und EC2 Amazon Amazon Machine Images (AMI) sind mit den HTTP-Diensten vorkonfiguriert, die für den Empfang und die Beantwortung der auf dieser Seite beschriebenen Webanfragen erforderlich sind. Es ist nicht erforderlich oder empfehlenswert, zusätzliche Dienste auf Ihrem Gateway zu installieren.

Themen

- Linux (curl)
- Linux (bash/zsh)
- Microsoft Windows PowerShell
- Verwenden der lokalen Konsole

Linux (curl)

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

> **Note**
>
> Ersetzen Sie die hervorgehobenen Variablen durch tatsächliche Werte für Ihr Gateway. Zulässige Werte sind:
>
> - *`gateway_ip_address`*- Die IPv4 Adresse Ihres Gateways, zum Beispiel `172.31.29.201`
> - *`gateway_type`*- Der Gateway-Typ, den Sie aktivieren möchten, z. B. `STOREDCACHED`,`VTL`,`FILE_S3`, oder`FILE_FSX_SMB`.

- *region_code*- Die Region, in der Sie Ihr Gateway aktivieren möchten. Weitere Informationen finden Sie unter Regionale Endpunkte im Allgemeinen Referenzhandbuch zu AWS . Wenn dieser Parameter nicht angegeben ist oder wenn der angegebene Wert falsch geschrieben ist oder nicht mit einer gültigen Region übereinstimmt, verwendet der Befehl standardmäßig die `us-east-1` Region.
- *vpc_endpoint*- Zum Beispiel `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com` der VPC-Endpunktname für Ihr Gateway.

So rufen Sie den Aktivierungsschlüssel für einen öffentlichen Endpunkt ab:

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

So rufen Sie den Aktivierungsschlüssel für einen VPC-Endpunkt ab:

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

Linux (bash/zsh)

Das folgende Beispiel zeigt, wie Sie mit Linux (bash/zsh) die HTTP-Antwort abfangen, HTTP-Header analysieren und den Aktivierungsschlüssel abrufen.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
```

```
    return 1
  fi
}
```

Microsoft Windows PowerShell

Das folgende Beispiel zeigt Ihnen, wie Sie Microsoft Windows verwenden, PowerShell um die HTTP-Antwort abzurufen, HTTP-Header zu analysieren und den Aktivierungsschlüssel abzurufen.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Verwenden der lokalen Konsole

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 von einem Windows-Computer aus eine Verbindung zu Ihrer EC2 Amazon-Instance herstellen, melden Sie sich als Administrator 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 die 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 Sie Ihre VTL-Geräte mit einem Windows-Client
- Verbinden Sie Ihre VTL-Geräte 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 auf Windows Server 2022 validiert. Der Initiator ist in das Betriebssystem 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.

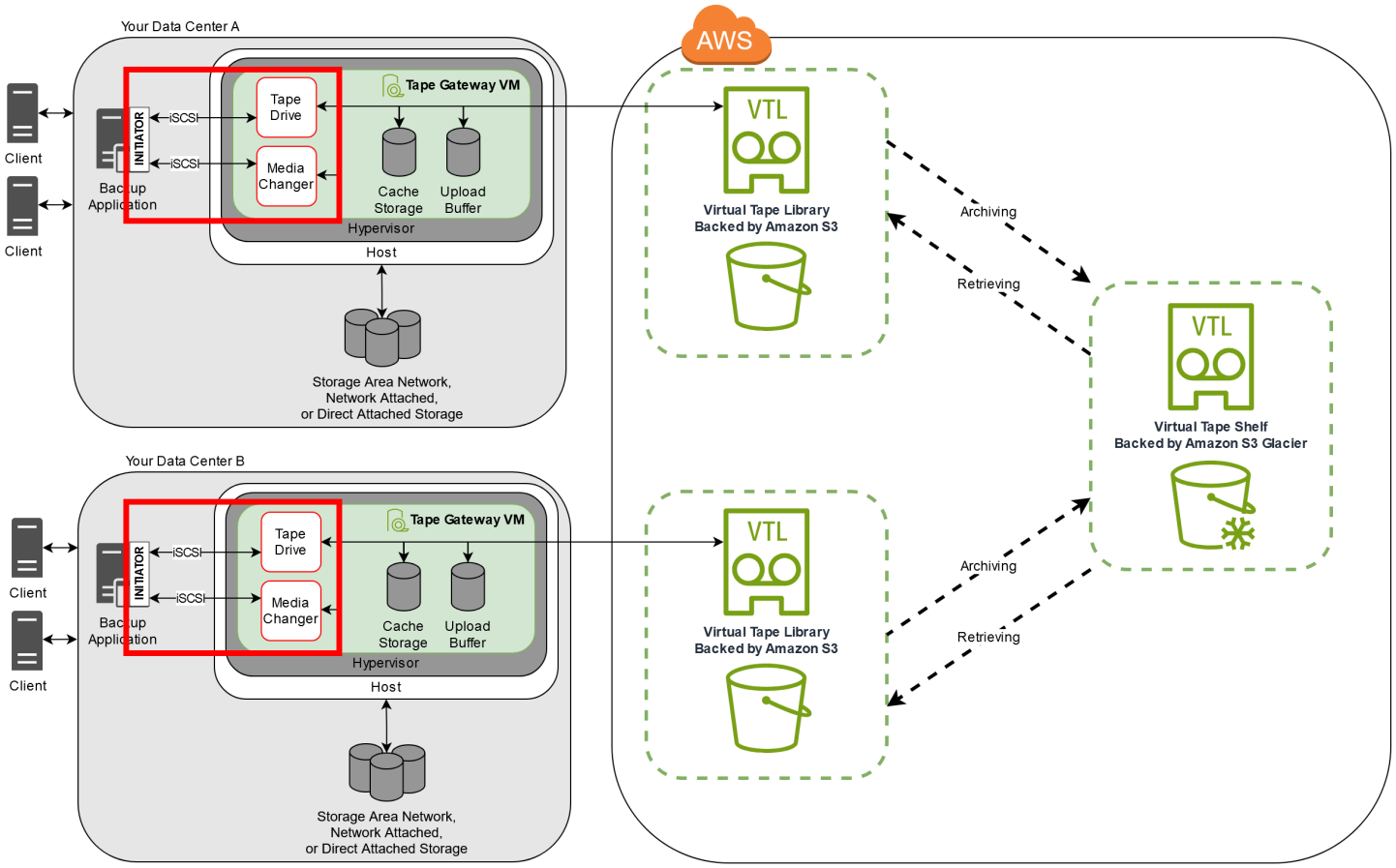
Alle Typen von Gateways lassen sich mit iSCSI-Geräten verbinden und diese Verbindungen können Sie auch anpassen. Die entsprechenden Anleitungen finden Sie nachfolgend.

Verbinden Sie Ihre VTL-Geräte mit einem Windows-Client

Ein Tape Gateway macht mehrere Bandlaufwerke und einen Medienwechsler, zusammenfassend VTL-Geräte genannt, als iSCSI-Ziele verfügbar. Weitere Informationen finden Sie unter Voraussetzungen für die Einrichtung von Tape Gateway.

> **Note**
>
> Mit jedem iSCSI-Ziel darf jeweils maximal eine Anwendung verbunden werden.

Die folgende Abbildung verdeutlicht die Position des iSCSI-Ziels im größeren Zusammenhang der Storage-Gateway-Architektur. Weitere Informationen zur Storage-Gateway-Architektur finden Sie unter Funktionsweise von Tape Gateway (Architektur).



Einen Windows-Client verbinden Sie wie folgt mit VTL-Geräten:

1. Geben Sie im Menü Start Ihres Windows-basierten Client-Computers **`iscsicpl.exe`** in das Feld Programme und Dateien durchsuchen ein, suchen Sie nach dem iSCSI-Initiator-Programm und führen Sie es aus.

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

2. Klicken Sie bei Aufforderung auf Ja, um den Microsoft iSCSI-Initiator-Dienst zu starten.
3. Wählen Sie im Dialogfeld iSCSI Initiator-Eigenschaften die Registerkarte Erkennung aus und klicken Sie dann auf Erkennungsportal.
4. Geben Sie im Dialogfeld Zielportal ermitteln unter IP-Adresse oder DNS-Name die IP-Adresse Ihres Tape Gateway ein und klicken Sie auf OK. Die IP-Adresse Ihres Gateways finden Sie auf der Registerkarte Gateway in der Storage-Gateway-Konsole. Wenn Sie Ihr Gateway auf einer

EC2 Amazon-Instance bereitgestellt haben, finden Sie die öffentliche IP- oder DNS-Adresse auf der Registerkarte Beschreibung auf der EC2 Amazon-Konsole.

> **Warning**
>
> Für Gateways, die auf einer EC2 Amazon-Instance bereitgestellt werden, wird der Zugriff auf das Gateway über eine öffentliche Internetverbindung nicht unterstützt. Die Elastic IP-Adresse der EC2 Amazon-Instance kann nicht als Zieladresse verwendet werden.

5. Wählen Sie die Registerkarte Targets (Ziele) und dann Refresh (Aktualisieren) aus. Anschließend werden im Feld Erkannte Ziele alle 10 Bandlaufwerke und der Medienwechsler angezeigt. Der Status der Ziele ist Inactive (Inaktiv).
6. Wählen Sie das erste Gerät aus und klicken Sie auf Connect (Verbinden). Die einzelnen Geräte müssen nacheinander verbunden werden.
7. Klicken Sie im Dialogfeld Mit Ziel verbinden auf OK.
8. Wiederholen Sie Schritt 6 und Schritt 7 für jedes der Geräte, um sie alle zu verbinden, und klicken Sie anschließend im Dialogfeld Eigenschaften von iSCSI-Initiator auf OK.

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

So überprüfen Sie den Treiberanbieter und aktualisieren (falls erforderlich) den Anbieter und Treiber auf einem Windows-Client

1. Starten Sie auf Ihrem Windows-Client den Geräte-Manager.
2. Erweitern Sie Tape drives (Bandlaufwerke), öffnen Sie mit einem Rechtsklick das Kontextmenü eines der Bandlaufwerke und klicken Sie auf Properties (Eigenschaften).
3. Überprüfen Sie auf der Registerkarte Treiber des Dialogfelds Geräteeigenschaften, ob Microsoft der Treiberanbieter ist.
4. Wenn Treiberanbieter nicht Microsoft lautet, legen Sie den Wert wie folgt fest:

    a. Wählen Sie Update Driver (Treiber aktualisieren) aus.

    b. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Browse my computer for driver software (Auf dem Computer nach Treibersoftware suchen) aus.

c. Wählen Sie im Dialogfeld Update Driver Software (Treibersoftware aktualisieren) die Option Let me pick from a list of device drivers on my computer (Aus einer Liste von Gerätetreibern auf dem Computer auswählen) aus.

d. Wählen Sie LTO Tape drive (LTO-Bandlaufwerk) aus und klicken Sie auf Next (Weiter).

e. Wählen Sie Schließen aus, um das Fenster Treibersoftware aktualisieren zu schließen, und überprüfen Sie, ob Treiberanbieter nun auf den Wert Microsoft festgelegt ist.

5. Aktualisieren Sie jedes Bandlaufwerk, in dem Sie jeweils die Schritte 4.1 bis 4.5 wiederholen.

Verbinden Sie Ihre VTL-Geräte 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 für RHEL 8 oder 9 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 für RHEL 8 oder 9 den folgenden Befehl. In der Regel müssen Sie den `iscsid` Dienst nicht explizit 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 *[GATEWAY_IP]* Variable im vorherigen Befehl durch die IP-Adresse Ihres Gateways. Sie finden die Gateway-IP in der Storage-Gateway-Konsole im Eigenschaftenbereich iSCSI-Zielinfo eines Volumes.

Die Ausgabe des Entdeckungsbefehl gleicht der folgenden Beispielausgabe.

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

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

Ihr qualifizierter iSCSI-Name (IQN) wird nicht mit dem oben angegebenen identisch sein, da IQN-Werte für jede Organisation eindeutig sind. Der Name des Ziels ist der Name, den Sie angegeben haben, als Sie das Volume erstellt haben. Sie finden diesen Zielnamen auch im Eigenschaftenbereich iSCSI-Zielinfo, wenn Sie in der Storage-Gateway-Konsole ein Volume auswählen.

4. Verwenden Sie den nachfolgenden Befehl, um eine Verbindung mit einem Ziel herzustellen.

Beachten Sie, dass Sie im Verbindungsbefehl den richtigen *[GATEWAY_IP]* und den richtigen IQN angeben müssen.

> **Warning**
>
> Für Gateways, die auf einer EC2 Amazon-Instance bereitgestellt werden, wird der Zugriff auf das Gateway über eine öffentliche Internetverbindung nicht unterstützt. Die Elastic IP-Adresse der EC2 Amazon-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 zu anderen bewährten Methoden, die Sie bei der Arbeit mit der Registrierung beachten sollten, finden Sie unter Bewährte Methoden für die Registrierung in der TechNet Microsoft-Bibliothek.

Themen

- Anpassen der Windows iSCSI-Einstellungen
- Anpassen Ihrer Linux iSCSI-Einstellungen

Anpassen der Windows iSCSI-Einstellungen

Um eine Tape-Gateway-Einrichtung mit Ihren VTL-Geräte zu verbinden, indem Sie einen Microsoft iSCSI-Initiator verwenden, besteht aus zwei Schritten:

1. Verbinden Sie die Tape-Gateway-Geräte mit Ihrem Windows Client.
2. Wenn Sie eine Backup-Anwendung verwenden, konfigurieren Sie die Anwendung für die Verwendung der Geräte.

Das Erste-Schritte-Beispiel Einrichtung enthält Anweisungen für beide dieser folgenden Schritte. Es verwendet die NetBackup Symantec-Backup-Anwendung. Weitere Informationen erhalten Sie unter Ihre VTL-Geräte anschließen und Konfiguration von Speichergeräten NetBackup .

Um Ihre Windows iSCSI-Einstellungen anzupassen

1. Erhöhen Sie die maximale Dauer für die Anforderungen in der Warteschlange.

   a. Starten Sie den Registrierungs-Editor (`Regedit.exe`).

   b. Navigieren Sie zu dem globalen eindeutigem Initiator GUID-Schlüssel für die Geräte Klasse mit iSCSI-Controller Einstellungen, wie folgt angezeigt.

   > **Warning**
   >
   > Stellen Sie sicher, dass Sie mit dem CurrentControlSetUnterschlüssel und nicht mit einem anderen Steuersatz wie ControlSet001 oder ControlSet 002 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 Folgenden als angezeigt wird. *`[<Instance Number]`*

   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 überprüfen, ob die Zeichenfolge den Wert enthält. `DriverDesc Microsoft iSCSI Initiator`

d. Um die iSCSI-Einstellungen anzuzeigen, wählen Sie den Unterschlüssel Parameters (Parameter) aus.

e. Öffnen Sie das Kontextmenü (Rechtsklick) für den MaxRequestHoldTimeDWORD-Wert (32-Bit), wählen Sie Ändern und ändern Sie dann den Wert in. **`600`**

MaxRequestHoldTimegibt an, wie viele Sekunden der Microsoft iSCSI-Initiator ausstehende Befehle warten und erneut versuchen soll, bevor die obere Ebene über ein Ereignis informiert wird. `Device Removal` Dieser Wert stellt eine Wartezeit von 600 Sekunden dar.

2. Sie können die maximale Datenmenge erhöhen, die in iSCSI-Paketen gesendet werden kann, indem Sie die folgenden Parameter ändern:

- FirstBurstLengthsteuert die maximale Datenmenge, die in einer unaufgeforderten Schreibanforderung übertragen werden kann. Legen Sie diesen Wert auf **`262144`** oder die Standardeinstellung des Windows-Betriebssystems fest, je nachdem, welcher Wert höher ist.
- MaxBurstLengthist ähnlich wie FirstBurstLength, legt aber die maximale Datenmenge fest, die in angeforderten Schreibsequenzen übertragen werden kann. Legen Sie diesen Wert auf **`1048576`** oder die Standardeinstellung des Windows-Betriebssystems fest, je nachdem, welcher Wert höher ist.
- MaxRecvDataSegmentLengthsteuert die maximale Datensegmentgröße, die einer einzelnen Protokolldateneinheit (PDU) zugeordnet ist. Legen Sie diesen Wert auf **`262144`** oder die Standardeinstellung des Windows-Betriebssystems fest, je nachdem, welcher Wert höher ist.

> **Note**
>
> Unterschiedliche Backup-Software kann optimiert werden, um mit verschiedenen iSCSI-Einstellungen möglichst gut zu funktionieren. Informationen zur Überprüfung, welche

Werte für diese Parameter die beste Leistung bieten, finden Sie in der Dokumentation zu Ihrer Backup-Software.

3. Erhöhen Sie den Datenträger-Timeout-Wert, der wie folgt angezeigt wird:

   a. Starten Sie den Registrierungs-Editor (`Regedit.exe`), falls Sie dies noch nicht getan haben.

   b. Navigieren Sie zum Unterschlüssel Disk im Unterschlüssel Services von (siehe unten CurrentControlSet).

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. Öffnen Sie das Kontextmenü (Rechtsklick) für den TimeOutValueDWORD-Wert (32-Bit), wählen Sie Ändern und ändern Sie dann den Wert in. **`600`**

   TimeOutValuegibt an, wie viele Sekunden der iSCSI-Initiator auf eine Antwort vom Ziel wartet, bevor er versucht, die Sitzung wiederherzustellen, indem er die Verbindung unterbricht und wieder herstellt. Dieser Wert steht für einen Timeout-Zeitraum von 600 Sekunden.

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.

So passen Sie Ihre Linux-Festplatten-Timeout-Einstellungen an

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. Stellen Sie den *[replacement_timeout_value]* Wert auf ein. **600**

   Stellen Sie den *[noop_out_interval_value]* Wert auf ein**60**.

   Stellen Sie den *[noop_out_timeout_value]* Wert auf ein**600**.

   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.

   Setzen Sie den *[replacement_first_burst_length_value]* Wert auf **262144** oder die Standardeinstellung des Linux-Betriebssystems, je nachdem, welcher Wert höher ist.

   Setzen Sie den *[replacement_max_burst_length_value]* Wert auf **1048576** oder die Standardeinstellung des Linux-Betriebssystems, je nachdem, welcher Wert höher ist.

   Setzen Sie den *[replacement_segment_length_value]* Wert auf **262144** oder die Standardeinstellung des Linux-Betriebssystems, 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.

Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele

Storage Gateway unterstützt die Authentifizierung zwischen Ihrem Gateway und iSCSI-Initiatoren mithilfe des Challenge-Handshake Authentication Protocol (CHAP). CHAP bietet Schutz vor

Playback-Angriffen, indem die Identität eines iSCSI-Initiators, der für den Zugriff auf ein Volume und ein VTL-Gerätеziel authentifiziert wurde, regelmäßig überprüft wird.

> **Note**
>
> Die CHAP-Konfiguration ist optional, wird jedoch dringend empfohlen.

Zur Einrichtung von CHAP müssen Sie das Protokoll sowohl in der Storage-Gateway-Konsole als auch in der iSCSI-Initiator-Software konfigurieren, über die Sie die Verbindung mit dem Ziel herstellen. Storage Gateway arbeitet mit wechselseitiger CHAP-Authentifizierung: Der Initiator authentifiziert das Ziel und das Ziel authentifiziert den Initiator.

Eine wechselseitige CHAP-Authentifizierung richten Sie wie folgt für Ihre Ziele ein:

1. Konfigurieren Sie CHAP in der Storage-Gateway-Konsole wie unter So konfigurieren Sie CHAP für ein VTL-Gerät in der Storage-Gateway-Konsole beschrieben.
2. Konfigurieren Sie CHAP in der Initiator-Software auf Ihrem Client:
   - Wie Sie die wechselseitige CHAP-Authentifizierung auf einem Windows-Client konfigurieren, erfahren Sie unter Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.
   - Wie Sie die wechselseitige CHAP-Authentifizierung auf einem Red Hat Linux-Client konfigurieren, erfahren Sie unter Auf einem Red Hat Linux-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.

So konfigurieren Sie CHAP für ein VTL-Gerät in der Storage-Gateway-Konsole

In dieser Anleitung geben Sie zwei geheime Schlüssel an, die verwendet werden, um von dem virtuellen Bandlaufwerk zu lesen und auf das virtuelle Bandlaufwerk zu schreiben. Dieselben Schlüssel werden auch in der Anleitung zur Konfiguration des Client-Initiators verwendet.

1. Wählen Sie im Navigationsbereich Gateways aus.
2. Wählen Sie Ihr Gateway aus und wechseln Sie dann auf die Registerkarte VTL Devices (VTL-Geräte). Hier werden alle Ihre VTL-Geräte aufgeführt.
3. Wählen Sie das Gerät aus, für das Sie CHAP konfigurieren möchten.
4. Geben Sie alle erforderlichen Informationen im Dialogfeld CHAP-Authentifizierung konfigurieren ein, abgebildet im Screenshot unten:

a. Geben Sie im Feld Initiatorname den Namen Ihres iSCSI-Initiators ein. Dieser Name ist ein qualifizierter Amazon-iSCSI-Name (IQN), dem `iqn.1997-05.com.amazon:` vorangestellt wird und der Name des Ziels folgt. Im Folgenden wird ein Beispiel gezeigt.

   `iqn.1997-05.com.amazon:`*`your-tape-device-name`*

   Den Namen des Initiators finden Sie in Ihrer iSCSI-Initiator-Software. Auf Windows-Clients beispielsweise ist der Name der Wert auf der Registerkarte Konfiguration des iSCSI-Initiators. Weitere Informationen finden Sie unter Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.

   > **Note**
   >
   > Wenn Sie den Namen des Initiators ändern möchten, müssen Sie zunächst CHAP deaktivieren. Anschließend ändern Sie den Namen des Initiators in Ihrer iSCSI-Initiator-Software und aktivieren dann CHAP mit dem neuen Namen.

b. Geben Sie unter Für Authentifizierung des Initiators verwendeter geheimer Schlüssel den entsprechenden geheimen Schlüssel ein.

   Dieser geheime Schlüssel muss mindestens 12 Zeichen lang sein und darf höchstens 16 Zeichen lang sein. Dieser Wert ist der geheime Schlüssel, den der Initiator (Windows-Client) kennen muss, um an der CHAP-Authentifizierung mit dem Ziel teilnehmen zu können.

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

   Dieser geheime Schlüssel muss mindestens 12 Zeichen lang sein und darf höchstens 16 Zeichen lang sein. Dieser Wert ist der geheime Schlüssel, den das Ziel kennen muss, um an der CHAP-Authentifizierung mit dem Initiator teilnehmen zu können.

   > **Note**
   >
   > Für die Authentifizierung des Ziels müssen Sie einen anderen geheimen Schlüssel verwenden als für die Authentifizierung des Initiators.

d. Wählen Sie Save (Speichern) aus.

5. Vergewissern Sie sich, dass auf der Registerkarte VTL Devices (VTL-Geräte) für das Feld "iSCSI CHAP authentication (iSCSI CHAP-Authentifizierung)" der Wert auf true (wahr) gesetzt ist.

Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:

In dieser Anleitung konfigurieren Sie CHAP im Microsoft iSCSI-Initiator. Hierzu verwenden Sie dieselben Schlüssel wie bei der konsolenbasierten Konfiguration von CHAP für das Volume.

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

   a. Wählen Sie die Registerkarte Konfiguration aus.

   > **Note**
   >
   > Der Wert im Feld Initiatorname ist für Ihren Initiator und Ihre Firma eindeutig. Der Name im Screenshot oben ist der Wert, den Sie im Dialogfeld CHAP-Authentifizierung konfigurieren in der Storage-Gateway-Konsole verwendet haben. Der Name auf dem Screenshot dient ausschließlich Demonstrationszwecken.

   b. Klicken Sie auf CHAP.

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

      In diesem Dialogfeld geben Sie den geheimen Schlüssel ein, den der Initiator (Windows-Client) zur Authentifizierung des Ziels (Speicher-Volume) verwendet. Dieser geheime Schlüssel gewährt dem Ziel Lese- und Schreibrechte für den Initiator. Es handelt sich hierbei um denselben geheimen Schlüssel, den Sie im Feld Für Authentifizierung des Ziels verwendeter geheimer Schlüssel (wechselseitige CHAP-Authentifizierung) im Dialogfeld CHAP-Authentifizierung konfigurieren eingegeben haben. Weitere Informationen finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.

   d. Falls Sie einen Schlüssel eingeben, der weniger als 12 Zeichen oder mehr als 16 Zeichen umfasst, wird das Fehlerdialogfeld Geheimer CHAP-Schlüssel des Initiators angezeigt.

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

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

a. Wählen Sie die Registerkarte Ziele.

b. Falls das Ziel, das Sie für CHAP konfigurieren möchten, aktuell verbunden ist: Wählen Sie das Ziel aus und klicken Sie auf Disconnect (Trennen), um die Verbindung mit dem Ziel zu trennen.

c. Wählen Sie das Ziel aus, das Sie für CHAP konfigurieren möchten, und klicken Sie auf Connect (Verbinden).

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

e. Konfigurieren Sie CHAP im Dialogfeld Advanced Settings (Erweiterte Einstellungen).

   i. Wählen Sie CHAP-Anmeldung aktivieren aus.

   ii. Geben Sie den zum Authentifizieren des Initiators erforderlichen geheimen Schlüssel ein. Es handelt sich hierbei um denselben geheimen Schlüssel, den Sie im Feld Für Authentifizierung des Initiators verwendeter geheimer Schlüssel im Dialogfeld CHAP-Authentifizierung konfigurieren eingegeben haben. Weitere Informationen finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.

   iii. Wählen Sie Perform mutual authentication (Wechselseitige Authentifizierung ausführen) aus.

   iv. Klicken Sie auf OK, um die Änderungen anzuwenden.

f. Klicken Sie im Dialogfeld Mit Ziel verbinden auf OK.

4. Wenn Sie den richtigen geheimen Schlüssel angegeben haben, wird für das Ziel der Status Connected (Verbunden) angezeigt.

Auf einem Red Hat Linux-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:

In dieser Anleitung konfigurieren Sie CHAP im Linux-iSCSI-Initiator. Hierzu verwenden Sie dieselben Schlüssel, die Sie auch verwendet haben, als Sie in der Storage-Gateway-Konsole CHAP für das Volume konfiguriert haben.

1. Vergewissern Sie sich, dass der ISCSI-Daemon ausgeführt wird und dass bereits eine Verbindung zu einem Ziel besteht. Falls Sie diese beiden Aufgaben nicht abgeschlossen haben, finden Sie weitere Informationen unter Herstellen einer Verbindung mit einem Linux-Client.

2. Trennen Sie die Verbindung zu dem Ziel, für das Sie CHAP konfigurieren möchten, und entfernen Sie alle bereits vorhandenen Konfigurationen.

a. Listen Sie mithilfe des folgenden Befehls die gespeicherten Konfigurationen auf, um den Zielnamen zu ermitteln und sich zu vergewissern, dass es sich um eine definierte Konfiguration handelt:

```
sudo /sbin/iscsiadm --mode node
```

b. Trennen Sie die Verbindung mit dem Ziel.

Der folgende Befehl trennt die Verbindung mit dem Ziel **myvolume**, das im qualifizierten Amazon-iSCSI-Namen (IQN) definiert ist. Passen Sie den Zielnamen und den IQN entsprechend Ihrer konkreten Umgebung an.

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
 iqn.1997-05.com.amazon:myvolume
```

c. Entfernen Sie die Konfiguration des Ziels.

Der folgende Befehl entfernt die Konfiguration für das Ziel **myvolume**.

```
sudo /sbin/iscsiadm --mode node --op delete --targetname
 iqn.1997-05.com.amazon:myvolume
```

3. Bearbeiten Sie die iSCSI-Konfigurationsdatei, um CHAP zu aktivieren.

a. Rufen Sie den Namen des Initiators ab (also den des Clients, den Sie verwenden).

Der folgende Befehl ruft den Namen des Initiators aus der Datei `/etc/iscsi/initiatorname.iscsi` ab:

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

Die Ausgabe dieses Befehls sieht in etwa wie folgt aus:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. Öffnen Sie die `/etc/iscsi/iscsid.conf` Datei.

c. Kommentieren Sie die folgenden Zeilen in der Datei aus und geben Sie die richtigen Werte für*username*, *passwordusername_in*, und *password_in* an.

```
node.session.auth.authmethod = CHAP
```

```
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

Einen Überblick über die anzugebenden Werte finden Sie in der nachfolgenden Tabelle.

Konfigurationseinstellung	Wert
username	Gibt den Initiatornamen an, den Sie im vorherigen Schritt der Anleitung abgerufen haben. Der Wert beginnt mit iqn. **iqn.1994-05.com.redhat:8e89b27b5b8** Ist beispielsweise ein gültiger *username* Wert.
password	Gibt den geheimen Schlüssel an, der zur Authentifizierung des Initiators (also des verwendeten Clients) verwendet wird, wenn dieser mit dem Volume kommuniziert.
username_in	Gibt den IQN des Ziel-Volumes an. Der Wert beginnt mit iqn und endet mit dem Namen des Ziels. **iqn.1997-05.com.amazon:myvolume** Ist beispielsweise ein gültiger *username_in* Wert.
password_in	Gibt den geheimen Schlüssel an, der zur Authentifizierung des Ziels (also des Volumes) verwendet wird, wenn dieses mit dem Initiator kommuniziert.

d. Speichern Sie die Änderungen in der Konfigurationsdatei und schließen Sie die Datei.

4. Führen Sie eine Erkennung des Ziels durch und melden Sie sich beim Ziel an. Folgen Sie dazu den Schritten unter Herstellen einer Verbindung mit einem Linux-Client.

Verwendung AWS Direct Connect mit Storage Gateway

AWS Direct Connect verbindet Ihr internes Netzwerk mit der Amazon Web Services Cloud. Durch die Verwendung AWS Direct Connect mit Storage Gateway können Sie eine Verbindung für Workload-

Anforderungen mit hohem Durchsatz herstellen und so eine dedizierte Netzwerkverbindung zwischen Ihrem lokalen Gateway und bereitstellen. AWS

Storage Gateway verwendet öffentliche Endpunkte. Wenn eine AWS Direct Connect Verbindung besteht, können Sie eine öffentliche virtuelle Schnittstelle erstellen, über die der Datenverkehr an die Storage Gateway Gateway-Endpunkte weitergeleitet werden kann. Die öffentliche virtuelle Schnittstelle umgeht Internetdienstanbieter in Ihrem Netzwerkpfad. Der öffentliche Endpunkt des Storage Gateway Gateway-Dienstes kann sich in derselben AWS Region wie der AWS Direct Connect Standort oder in einer anderen AWS Region befinden.

Die folgende Abbildung zeigt ein Beispiel für die AWS Direct Connect Funktionsweise mit Storage Gateway.
Netzwerkarchitektur, die zeigt, dass Storage Gateway über AWS Direct Connect mit der Cloud verbunden ist.

In der folgenden Vorgehensweise wird davon ausgegangen, dass Sie bereits ein funktionsfähiges Gateway erstellt haben.

Zur Verwendung AWS Direct Connect mit Storage Gateway

1. Erstellen und stellen Sie eine AWS Direct Connect Verbindung zwischen Ihrem lokalen Rechenzentrum und Ihrem Storage Gateway Gateway-Endpunkt her. Weitere Informationen zum Erstellen einer Verbindung finden Sie unter Erste Schritte mit AWS Direct Connect im Benutzerhandbuch zu AWS Direct Connect .
2. Connect Sie Ihre lokale Storage Gateway 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-Endpoints mit dem erstellt werden. HAProxy Weitere Informationen finden Sie unter Erstellen einer virtuellen Schnittstelle im Benutzerhandbuch zu AWS Direct Connect .

Einzelheiten dazu finden Sie AWS Direct Connect unter Was ist? AWS Direct Connect im AWS Direct Connect Benutzerhandbuch.

Abrufen der IP-Adresse für Ihre Gateway-Appliance

Nachdem Sie einen Host ausgewählt und eine Gateway-VM bereitgestellt haben, verbinden und aktivieren Sie das Gateway. Hierzu benötigen Sie die IP-Adresse der Gateway-VM. Rufen Sie die IP-

Adresse von der lokalen Konsole des Gateways ab. Sie melden sich bei der lokalen Konsole an und rufen die IP-Adresse im oberen Bereich der Konsole ab.

Für lokal bereitgestellte Gateways können Sie auch die IP-Adresse vom Hypervisor abrufen. Für EC2 Amazon-Gateways können Sie die IP-Adresse Ihrer EC2 Amazon-Instance auch von der Amazon EC2 Management Console abrufen. Informationen zum Abrufen der IP-Adresse des Gateways finden unter:

- VMware Host: Zugreifen auf die lokale Gateway-Konsole mit VMware ESXi
- Hyper-V-Host: Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V
- Linux kernelbasierte virtuelle Maschine (KVM)-Host: Zugreifen auf die lokale Konsole des Gateways mit Linux KVM
- EC2 Gastgeber: Eine IP-Adresse von einem EC2 Amazon-Host abrufen

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.

Eine IP-Adresse von einem EC2 Amazon-Host abrufen

Um die IP-Adresse der EC2 Amazon-Instance abzurufen, auf der Ihr Gateway bereitgestellt wird, melden Sie sich bei der lokalen Konsole der EC2 Instance an. Rufen Sie dann die IP-Adresse am oberen Rand der Konsolenseite ab. Detaillierte Anweisungen finden Sie unter Melden Sie sich bei Ihrer lokalen Amazon EC2 Gateway-Konsole an.

Sie können die IP-Adresse auch von der Amazon EC2 Management Console 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 EC2 Amazon-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 wird.
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 EC2 Amazon-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 wird.
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 über die elastische IP-Adresse der EC2 Instance verbunden.

Grundlegendes zu Storage Gateway Gateway-Ressourcen und -Ressourcen IDs

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 (ARNs) zugeordnet, wie in der folgenden Tabelle dargestellt.

Ressourcentyp	ARN-Format
Gateway-ARN	`arn:aws:storagegateway:` *region*`:`*account-id* `:gateway/` *gateway-id*
Band-ARN	`arn:aws:storagegateway:` *region*`:`*account-id* `:tape/`*tapebarcode*
Ziel-ARN (iSCSI-Ziel)	`arn:aws:storagegateway:` *region*`:`*account-id* `:gateway/` *gateway-id* `/target/`*iSCSItarget*
VTL-Geräte-ARN	`arn:aws:storagegateway:` *region*`:`*account-id* `:gateway/` *gateway-id* `/device/`*vtldevice*

Storage Gateway unterstützt auch die Verwendung von EC2 Instances und EBS-Volumes und -Snapshots. Bei diesen Ressourcen handelt es sich EC2 um Amazon-Ressourcen, die in Storage Gateway verwendet werden.

Mit Ressourcen arbeiten IDs

Wenn Sie eine Ressource erstellen, weist Storage Gateway der Ressource eine eindeutige Ressourcen-ID zu. Diese Ressourcen-ID ist Teil des Ressourcen-ARN. Eine Ressourcen-ID besteht aus einer Ressourcenkennung, gefolgt von einem Bindestrich und einer eindeutigen Kombination aus acht Buchstaben und Zahlen. Eine Gateway-ID beispielsweise hat die Form `sgw-12A3456B`, wobei `sgw` die Ressourcenkennung für Gateways ist. 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.

Die Storage Gateway Gateway-Ressourcen IDs werden in Großbuchstaben geschrieben. Wenn Sie diese Ressourcen jedoch IDs mit der EC2 Amazon-API verwenden, EC2 erwartet Amazon die Ressource 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 in ändern. `vol-1122aabb` 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 Verwendung in AWS 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 Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich die Ressource, die Sie kennzeichnen möchten.

   Wenn Sie z. B. ein Gateway mit Tags versehen möchten, wählen Sie Gateways und wählen Sie dann das Gateway, das Sie kennzeichnen möchten, aus der Liste der Gateways aus.
3. Wählen Sie Tagsund dann Add/edit tags (Tags hinzufügen/bearbeiten).
4. Wählen Sie im Dialogfeld Add/edit tags (Tags hinzufügen/bearbeiten) die Option Create tag (Tag erstellen).
5. Geben Sie einen Schlüssel für Key (Schlüssel) und einen Wert für Value (Wert) ein. Beispielsweise können Sie **`Department`** für den Schlüssel und **`Accounting`** für den Wert eingeben.

   > **Note**
   >
   > Sie können das Feld Value (Wert) auch leer lassen.
6. Wählen Sie Create Tag (Tag erstellen), um weitere Tags hinzuzufügen. Sie können einer Ressource mehrere Tags hinzufügen.
7. Wenn Sie alle Tags hinzugefügt haben, wählen Sie Save (Speichern).

So bearbeiten Sie ein Tag

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie die Ressource aus, deren Tag Sie bearbeiten möchten.
3. Wählen Sie Tags, um das Dialogfeld Add/edit tags (Tags hinzufügen/bearbeiten) zu öffnen.
4. Wählen Sie das Bleistiftsymbol neben dem Tag aus, das Sie bearbeiten möchten, und bearbeiten Sie dann das Tag.
5. Wenn Sie das Tag bearbeitet haben, wählen Sie Save (Speichern).

So löschen Sie ein Tag

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie die Ressource aus, deren Tag Sie löschen möchten.
3. Wählen Sie Tags und dann Add/edit tags (Tags hinzufügen/bearbeiten), um das Dialogfeld Add/edit tags (Tags hinzufügen/bearbeiten) zu öffnen.
4. Wählen Sie das Symbol X neben dem Tag, das Sie löschen möchten, und wählen Sie dann Save (Speichern).

Arbeiten mit Open-Source-Komponenten für 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 bereitgestellt werden VMware ESXi, 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 kernelbasierten virtuellen Maschine unter Linux (KVM) bereitgestellt werden, sources_KVM.tar herunter.

Dieses Produkt enthält Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL-Toolkit (http://www.openssl.org/) entwickelt wurde. Die entsprechenden Lizenzen für alle abhängigen Drittanbieter-Tools finden Sie unter Lizenzen von Drittanbietern.

AWS Storage Gateway Kontingente

In diesem Thema finden Sie Informationen zu den für Storage Gateway geltenden Kontingenten für Dateifreigaben, Volumes und Bänder sowie zu den Konfigurations- und Leistungslimits des Service.

Themen

- Kontingente für Bänder

- Empfohlene Kapazität für die lokalen Datenträger des Gateways

Kontingente für Bänder

In der folgenden Tabelle sind die Kontingente für Bänder aufgeführt.

Beschreibung	Tape Gateway
Mindestgröße eines virtuellen Bands	100 GiB
Maximale Größe eines virtuellen Bands	15 TiB
Maximale Anzahl virtueller Bänder, die einem Gateway zugewiesen sind	1.500
Gesamtgröße aller pro Gateway zugewiesener Bänder	1 PiB
Maximale Anzahl von virtuellen Bändern pro Archiv	Kein Limit
Gesamtgröße aller Bänder im Archiv	Kein Limit

Empfohlene Kapazität für die lokalen Datenträger des Gateways

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

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

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

Storage-Gateway-API-Referenz

Zusätzlich zur Verwendung der Konsole können Sie die AWS Storage Gateway API verwenden, um Ihre Gateways programmgesteuert zu konfigurieren und zu verwalten. In diesem Abschnitt werden die AWS Storage Gateway Vorgänge, das Signieren von Anfragen zur Authentifizierung und die Fehlerbehandlung beschrieben. Weitere Informationen zu den für Storage Gateway verfügbaren Endpunkte finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

> **Note**
>
> Sie können den auch AWS SDKs 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 und vereinfachen so Ihre Programmieraufgaben. 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 ActivateGatewayOperation verwendet werden.

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

Die folgenden Kopfzeilen müssen mit in den POST-Abfragen an Storage Gateway enthalten sein. Die unten gezeigten Header, die mit „x-amz“ beginnen, sind -spezifische Header. AWS Alle anderen aufgeführten Header sind allgemeine Header für HTTP-Transaktionen.

Header	Beschreibung
`Authorization`	Der Autorisierungs-Header enthält mehrere Informationen über die Abfrage, mit denen Storage Gateway bestimmt, ob die Abfrage eine gültige Aktion für den Auftraggeber ist. Das Format dieses Headers lautet wie folgt (Zeilenumbrüche dienen besserer Lesbarkeit): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` In der vorherigen Syntax geben Sie das Jahr YourAccessKey, den Monat und den Tag (yyyymmdd), die Region und die an. CalculatedSignature Das Format des Autorisierungsheaders wird durch die Anforderungen des V4-Signaturprozesses bestimmt. AWS Detaillierte Informationen zum Signieren finden Sie unter dem Thema Signieren von Anforderungen.
`Content-Type`	Verwenden Sie `application/x-amz-json-1.1` als Inhaltstyp für alle Abfragen an Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Header	Beschreibung
`Host`	Verwenden Sie den Host-Header, um den Storage-Gateway-Endpunkt anzugeben, an den Sie die Abfrage senden. `storagegateway.us-east-2.amazonaws.com` steht beispielsweise für den Endpunkt der Region USA Ost (Ohio). Weitere Informationen zu den für Storage Gateway verfügbaren Endpunkte finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der Allgemeine AWS-Referenz. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Sie müssen den Zeitstempel entweder im `Date` HTTP-Header oder im AWS `x-amz-date` Header angeben. (Einige HTTP-Client-Biblio theken lassen den Header `Date` nicht zu.) Ist der Header `x-amz-dat e` vorhanden, ignoriert das Storage Gateway System bei der Abfrageau thentifizierung alle Header des Typs `Date`. Das `x-amz-date` Format muss ISO86 01 Basic im Format YYYYMMDD'T'HHMMSS'Z' sein. Wenn sowohl der `Date` `x-amz-date` Header als auch verwendet werden, muss das Format des Date-Headers nicht 01 sein. ISO86 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	In diesem Header werden die Version der API und die angefragte Operation angegeben. Die Werte des Ziel-Headers werden durch Verknüpfung der API-Version mit dem API-Namen gebildet und haben folgendes Format. `x-amz-target: StorageGateway_ APIversion .operationName` Der OperationName-Wert (z. B. "ActivateGateway„) kann in der API-Liste gefunden werden. Storage-Gateway-API-Referenz

Signieren von Anforderungen

Storage Gateway erfordert, dass Sie jede gesendete Anforderung durch eine Signatur authentifizieren. Zum Signieren einer Anforderung berechnen Sie eine digitale Signatur mit einer kryptografischen Hash-Funktion. Ein kryptografischer Hash ist eine Funktion, die auf Grundlage der Eingabe einen einzigartigen Hash-Wert zurückgibt. Die Eingabe in die Hash-Funktion besteht aus dem Text Ihrer Anforderung und Ihrem geheimen Zugriffsschlüssel. Die Hash-Funktion gibt einen Hash-Wert zurück, den Sie in die Anforderung als Ihre Signatur einfügen. Die Signatur ist Teil des Headers `Authorization` in der Anforderung.

Nach dem Erhalt Ihrer Anforderung berechnet Storage Gateway die Signatur mit derselben Hash-Funktion und den von Ihnen zum Signieren der Anforderung eingegebenen Daten neu. Wenn die so berechnete Signatur mit der Signatur in der Anforderung übereinstimmt, verarbeitet Storage Gateway die Anforderung. Andernfalls wird die Anforderung abgelehnt.

Storage Gateway unterstützt die Authentifizierung mittels AWS Signature Version 4. Der Prozess zum Berechnen einer Signatur lässt sich in drei Aufgaben untergliedern:

- Aufgabe 1: Erstellen einer kanonischen Anforderung

  Ordnen Sie Ihre HTTP-Anforderung in einem kanonischen Format neu an. Die Verwendung eines kanonischen Formats ist erforderlich, weil Storage Gateway das gleiche kanonische Format verwendet, wenn eine Signatur erneut berechnet wird, um sie mit der von Ihnen gesendeten Signatur zu vergleichen.
- Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge

  Erstellen Sie eine Zeichenfolge, die Sie als einen der Eingabewerte für die kryptografische Hash-Funktion nutzen. Die als zu signierende Zeichenfolge bezeichnete Zeichenfolge ist eine Kombination aus dem Namen des Hash-Algorithmus, dem Anforderungsdatum, einer Zeichenfolge mit dem Umfang der Anmeldeinformationen und der kanonischen Anforderung aus der vorherigen Aufgabe. Die Zeichenfolge mit dem Umfang der Anmeldeinformationen selbst ist eine Kombination aus Datum, Region und Serviceinformationen.
- Aufgabe 3: Erstellen einer Signatur

  Erstellen Sie eine Signatur für Ihre Anforderung. Verwenden Sie dazu eine kryptografische Hash-Funktion, die zwei Eingabezeichenfolgen akzeptiert: die zu signierende Zeichenfolge und einen abgeleiteten Schlüssel. Der abgeleitete Schlüssel wird berechnet, indem Sie mit Ihrem

geheimen Zugriffsschlüssel beginnen und anhand der Zeichenfolge für den Gültigkeitsbereich der Anmeldeinformationen eine Reihe von Hash-basierten Nachrichtenauthentifizierungscodes () erstellen. HMACs

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. Dies liegt daran, dass es für diese API (oder ein Storage Gateway APIs) keine Abfrageparameter gibt.

Die zu signierende Zeichenfolge für Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge ist:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

Die erste Zeile der zu signierenden Zeichenfolge ist der Algorithmus, die zweite Zeile der Zeitstempel, die dritte Zeile der Umfang der Anmeldeinformationen und die letzte Zeile ein Hash der kanonischen Anforderung aus Aufgabe 1.

Für Aufgabe 3: Erstellen einer Signatur kann der abgeleitete Schlüssel wie folgt dargestellt werden:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Wenn der geheime Zugriffsschlüssel, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, verwendet wird, dann lautet die berechnete Signatur:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Der letzte Schritt besteht im Erstellen des `Authorization`-Headers. Für die Demonstration: Zugangsschlüssel AKIAIOSFODNN7EXAMPLE, der Header (mit zur besseren Lesbarkeit hinzugefügten Zeilenumbrüchen) lautet:

```
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 Fehlercode für den Vorgang `ActivationKeyInvalid` wird jedoch nur für die ActivateGatewayAPI zurückgegeben.

Abhängig von der Art des Fehlers kann Storage Gateway nur eine Ausnahme oder eine Ausnahme und einen Fehlercode für die Operation zurückgegeben. Beispiele für Fehlermeldungen finden Sie unter Fehlermeldungen.

Ausnahmen

In der folgenden Tabelle sind AWS Storage Gateway API-Ausnahmen aufgeführt. Wenn ein AWS Storage Gateway Vorgang eine Fehlerantwort zurückgibt, enthält der Antworttext eine dieser Ausnahmen. Die Codes `InternalServerError` und `InvalidGatewayRequestException` geben eine Operationsfehlercodes-Nachricht zurück, in der der entsprechende Operationsfehlercode angegeben ist.

Exception	Fehlermeldung	HTTP-Statuscode
`IncompleteSignatureException`	Die angegebene Signatur ist unvollständig.	400 Bad Request (400 Ungültige Anfrage)
`InternalFailure`	Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.	500 Internal Server Error

Exception	Fehlermeldung	HTTP-Statuscode
`InternalServerError`	Eine der Operationsfehlercode-Nachrichten Operationsfehlercodes.	500 Internal Server Error
`InvalidAction`	Die angeforderte Aktion oder Operation ist ungültig.	400 Bad Request (400 Ungültige Anfrage)
`InvalidClientTokenId`	Das angegebene X.509-Zertifikat oder die angegebene AWS Zugriffsschlüssel-ID ist in unseren Aufzeichnungen nicht vorhanden.	403 Forbidden
`InvalidGatewayRequestException`	Eine der Operationsfehlercode-Nachrichten in Operationsfehlercodes.	400 Bad Request (400 Ungültige Anfrage)
`InvalidSignatureException`	Die berechnete Anforderungssignatur entspricht nicht der angegebenen Signatur. Überprüfen Sie Ihren AWS Zugriffsschlüssel und Ihre Signaturmethode.	400 Bad Request (400 Ungültige Anfrage)
`MissingAction`	In der Anforderung fehlt ein Aktions- oder Operationsparameter.	400 Bad Request (400 Ungültige Anfrage)
`MissingAuthenticationToken`	Die Anfrage muss entweder eine gültige (registrierte) AWS Zugriffsschlüssel-ID oder ein X.509-Zertifikat enthalten.	403 Forbidden

Exception	Fehlermeldung	HTTP-Statuscode
`RequestExpired`	Die Anforderung liegt nach dem Ablaufdatum oder dem Anforderungsdatum (jeweils in 15-Minuten-Schritten) oder das Anforderungsdatum liegt mehr als 15 Minuten in der Zukunft.	400 Bad Request (400 Ungültige Anfrage)
`SerializationException`	Fehler bei der Serialisierung. Stellen Sie sicher, dass Ihre JSON-Nutzdaten wohlgeformt sind.	400 Bad Request (400 Ungültige Anfrage)
`ServiceUnavailable`	Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.	503 Service Unavailable (503 Service nicht verfügbar)
`SubscriptionRequiredException`	Die AWS Access Key ID benötigt ein Abonnement für den Dienst.	400 Bad Request (400 Ungültige Anfrage)
`ThrottlingException`	Rate überschritten.	400 Bad Request (400 Ungültige Anfrage)
`TooManyRequests`	Zu viele Anfragen	429 Zu viele Anfragen
`UnknownOperationException`	Eine unbekannte Operation wurde angegeben. Gültige Operationen werden in Operationen im Storage Gateway aufgeführt.	400 Bad Request (400 Ungültige Anfrage)
`UnrecognizedClientException`	Das Sicherheits-Token der Anfrage ist nicht gültig.	400 Bad Request (400 Ungültige Anfrage)

Exception	Fehlermeldung	HTTP-Statuscode
`ValidationException`	Der Wert des Parameters ist ungültig oder außerhalb des Bereichs.	400 Bad Request (400 Ungültige Anfrage)

Operationsfehlercodes

Die folgende Tabelle zeigt die Zuordnung zwischen AWS Storage Gateway Operationsfehlercodes und Fehlercodes APIs , die die Codes zurückgeben können. Alle Operationsfehlercodes werden mit einer von zwei allgemeinen Ausnahmen – `InternalServerError` und `InvalidGatewayRequestException` – zurückgegeben, die in Ausnahmen beschrieben werden.

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`ActivationKeyExpired`	Der angegebene Aktivierungsschlüssel ist abgelaufen.	ActivateGateway
`ActivationKeyInvalid`	Der angegebene Aktivierungsschlüssel ist 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

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`InitiatorNotFound`	Der angegebene Initiator wurde nicht gefunden.	DeleteChapCredentials
`DiskAlreadyAllocated`	Der angegebene Datenträger ist bereits zugeordnet.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	Der angegebene Datenträger ist nicht vorhanden.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskSizeNotGigAligned`	Der angegebene Datenträger ist nicht für Gigabyte ausgerichtet.	CreateStorediSCSIVolume
`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
`MaximumVolumeCountExceeded`	Die maximale Volume-Anzahl wurde überschritten.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	Die Gateway-Netzwerkkonfiguration wurde geändert.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`NotSupported`	Die angegebene Operation wird nicht unterstützt.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	Das angegebene Gateway ist nicht mehr auf dem neuesten Stand.	ActivateGateway
`SnapshotInProgressException`	Der angegeben e Snapshot wird bearbeitet.	DeleteVolume
`SnapshotIdInvalid`	Der angegebene Snapshot ist nicht gültig.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`StagingAreaFull`	Der Staging-Bereich ist voll.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetAlreadyExists`	Das angegebene Ziel ist bereits vorhanden.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	Das angegebene Ziel ist nicht gültig.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	Das angegebene Ziel wurde nicht gefunden.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`UnsupportedOperationForGatewayType`	Die angegebene Operation ist für den Typ des Gateways nicht gültig.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Das angegebene Volume ist bereits vorhanden.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	Das angegebene Volume ist nicht gültig.	DeleteVolume
`VolumeInUse`	Das angegebene Volume wird bereits verwendet.	DeleteVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`VolumeNotFound`	Das angegebene Volume wurde nicht gefunden.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	Das angegeben e Volume ist nicht einsatzbereit.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Fehlermeldungen

Bei einem Fehler enthalten die Informationen im Antwort-Header:

- Inhaltstyp: Anwendung/ -1.1 x-amz-json
- Einen passenden `4xx`- oder `5xx`-HTTP-Statuscode

Der Textkörper einer Fehlermeldung enthält Informationen zu dem aufgetretenen Fehler. Das folgende Beispiel zeigt eine Fehlerantwort mit der Ausgabesyntax von Antwortelementen für alle Fehlermeldungen.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

In der folgenden Tabellen werden die Felder der JSON-Fehlerantwort in dieser Syntax erläutert.

__type

Eine der Ausnahmen aus Ausnahmen.

Typ: Zeichenfolge

error

Enthält API-spezifische Fehlerdetails. Unter den allgemeinen Fehler (z. B. nicht spezifische Fehler für eine API) werden diese Fehlerinformationen nicht angezeigt.

Typ: Sammlung

errorCode

Einer der Operationsfehlercodes .

Typ: Zeichenfolge

errorDetails

Dieses Feld wird nicht in der aktuellen Version der API verwendet.

Typ: Zeichenfolge

message

Eine der Operationsfehlercode-Nachrichten .

Typ: Zeichenfolge

Beispielantwort auf einen Fehler

Der folgende JSON-Hauptteil wird zurückgegeben, wenn Sie die DescribeStoredi SCSIVolumes API verwenden und eine Gateway-ARN-Anforderungseingabe angeben, die nicht existiert.

```
{
  "__type": "InvalidGatewayRequestException",
```

```
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
}
```

Der folgende JSON-Text wird zurückgegeben, wenn ein Storage Gateway eine Signatur berechnet, die nicht der mit einer Anforderung gesendeten Signatur entspricht.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Operationen im Storage Gateway

Eine vollständige Liste der Storage-Gateway-Operationen finden Sie unter Aktionen in der AWS Storage Gateway -API-Referenz.

Dokumentenverlauf für das Tape Gateway Benutzerhandbuch

- API-Version: 2013-06-30
- Letzte Aktualisierung der Dokumentation: 24. November 2020

In der folgenden Tabelle sind wichtige Änderungen der einzelnen Versionen des AWS Storage Gateway Benutzerhandbuchs nach April 2018 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Hinweis zur Änderung der Verfügbarkeit von FSx File Gateway	Amazon FSx File Gateway ist für Neukunden nicht mehr verfügbar. Bestandskunden von FSx File Gateway können den Service weiterhin normal nutzen. Informationen zu Funktionen, die FSx File Gateway ähneln, finden Sie in diesem Blogbeitrag.	28. Oktober 2024
Mitteilung über die Änderung der Verfügbarkeit für FSx File Gateway	AWS Storage Gateway FSx File Gateway wird ab dem 28.10.24 nicht mehr für Neukunden verfügbar sein. Um den Service nutzen zu können, müssen Sie sich vor diesem Datum anmelden. Bestandskunden von FSx File Gateway können den Service weiterhin normal nutzen. Informationen zu Funktionen, die FSx File Gateway ähneln,	26. September 2024

	finden Sie in diesem Blogbeitrag.	
Option zum Ein- oder Ausschalten von Wartungsupdates hinzugefügt	Storage Gateway erhält regelmäßige Wartungsupdates, die Betriebssystem- und Software-Upgrades, Korrekturen zur Verbesserung der Stabilität, Leistung und Sicherheit sowie den Zugriff auf neue Funktionen beinhalten können. Sie können jetzt eine Einstellung konfigurieren, um diese Updates für jedes einzelne Gateway in Ihrer Bereitstellung ein- oder auszuschalten. Weitere Informationen finden Sie unter Gateway-Updates mit der AWS Storage Gateway Konsole verwalten.	6. Juni 2024
Veraltete Unterstützung für Tape Gateway auf Snowball Edge	Es ist nicht mehr möglich, Tape Gateway auf Snowball Edge-Geräten zu hosten.	14. März 2024

Aktualisierte Anweisungen zum Testen Ihrer Gateway-Einrichtung mit Anwendungen von Drittanbietern	Die Anweisungen zum Testen Ihrer Gateway-Einrichtung mithilfe von Drittanbieteranwendungen beschreiben jetzt das erwartete Verhalten, wenn Ihr Gateway während einer laufenden Backup-Aufgabe neu gestartet wird. Weitere Informationen finden Sie unter Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung.	24. Oktober 2023
Die empfohlenen CloudWatch Alarme wurden aktualisiert	Der CloudWatch `HealthNotifications` Alarm gilt jetzt für alle Gateway-Typen und Host-Plattformen und wird für diese empfohlen. Die empfohlenen Konfigurationseinstellungen wurden auch für `HealthNotifications` und `AvailabilityNotifications` aktualisiert. Weitere Informationen finden Sie unter Grundlegendes zu CloudWatch Alarmen Grundlegendes .	2. Oktober 2023

Erhöhung der maximalen Bandgröße auf 15 TiB für Tape Gateways	Außerdem wurde für Tape Gateways die maximale Größe virtueller Bänder jetzt von 5 TiB auf 15 TiB erhöht. Weitere Informationen finden Sie unter Kontingente für Bänder im Storage Gateway-B enutzerhandbuch.	4. Oktober 2022
Separate Benutzerhandbücher für Tape und Volume Gateway	Das Storage Gateway-B enutzerhandbuch, 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-B enutzerhandbuch aufgeteil t, die jeweils nur Informati onen zu einem Gateway-Typ enthalten. Weitere Informati onen finden Sie im Tape Gateway-Benutzerhandbuch und im Volume Gateway-B enutzerhandbuch.	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 mit der 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
Support für Quest NetVault Backup 13 für Tape Gateway	Tape Gateways unterstützen jetzt Quest NetVault Backup 13, das auf Microsoft Windows Server 2012 R2 oder Microsoft Windows Server 2016 ausgeführt wird. Weitere Informationen finden Sie unter Testen Ihres Setups 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

Support für Bandrückhaltesperre 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
CloudWatch Amazon-Alarme in der Storage Gateway Gateway-Konsole anzeigen	Sie können jetzt CloudWatch Alarme in der Storage Gateway Gateway-Konsole anzeigen. Weitere Informationen finden Sie unter Grundlegendes zu CloudWatch Alarmen Grundlegendes .	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 bietet jetzt Unterstützung für Hochverfügbarkeit, VMware um Storage-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen zu schützen. Weitere Informationen finden Sie unter Verwenden von VMware vSphere High Availability mit Storage Gateway im Storage Gateway Gateway-Benutzerhandbuch. Diese Version enthält auch Leistungsverbesserungen. Weitere Informationen finden Sie unter Leistung im Storage Gateway-Benutzerhandbuch.	20. November 2019

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

Support für Amazon CloudWatch Logs	Sie können jetzt File Gateways mit Amazon CloudWatch Log Groups konfigurieren, um über Fehler und den Zustand Ihres Gateways und seiner Ressourcen benachrichtigt zu werden. Weitere Informationen finden Sie unter Benachrichtigungen über Gateway-Integrität und Fehler bei Amazon CloudWatch Log Groups im Storage Gateway Gateway-Benutzerhandbuch.	4. September 2019
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 für SMB-Dateifreigaben für Microsoft Windows ACLs	Für File Gateways können Sie jetzt Microsoft Windows-Zugriffskontrolllisten (ACLs) verwenden, um den Zugriff auf SMB-Dateifreigaben (Server Message Block) zu steuern. Weitere Informationen finden Sie unter Steuern des Zugriffs auf eine SMB-Dateifreigabe mithilfe von Microsoft Windows ACLs .	8. Mai 2019

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 lokale Geschäftsanwendungen sichern AWS Backup , die Storage Gateway 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 Veritas NetBackup, Veritas Backup Exec und Quest Backup. NetVault Sie können nun diese Sicherungsanwendungen 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 Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung.	13. November 2018

Unterstützung für Storage Gateway-Hardware-Appliance	Die Storage Gateway-Hardware-Applicance enthält auf einem Drittanbieterserver vorinstallierte Storage Gateway-Software. Sie können die Appliance in der AWS Management Console verwalten. Die Appliance kann Datei-, Band- und Volume Gateways hosten. Weitere Informationen finden Sie unter Verwenden der Storage Gateway-Hardware-Appliance.	18. September 2018
Kompatibilität mit dem Microsoft System Center 2016 DPM Data Protection Manager (DPM)	Tape Gateways sind jetzt mit dem Microsoft System Center 2016 DPM Data Protection Manager (DPM) kompatibel. Sie können nun Microsoft DPM verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Einrichtung mithilfe von Microsoft System Center Data Protection Manager.	18. Juli 2018

Support für Server Message Block (SMB)-Protokolle	File Gateways bieten jetzt Unterstützung für Server Message Block (SMB)-Pro tokolle bei Dateifreigaben. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	20. Juni 2018
Unterstützung für Dateifrei gaben, 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 zwischeng espeichertes Volume oder ein virtuelles Band geschrieb en wurden. Derzeit können Sie dies mit der AWS Storage Gateway -API durchführen. Weitere Informationen finden Sie unter Datenverschlüsselu ng mit AWS KMS.	12. Juni 2018
Support für NovaStor DataCenter /Network	Tape Gateways unterstützen jetzt NovaStor DataCenter/ Network. You can now use NovaStor DataCenter/Network Version 6.4 oder 7.1, um Ihre Daten auf Amazon S3 zu sichern und direkt im Offline-Speicher zu archivieren (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive). Weitere Informationen finden Sie unter Testen Ihres Setups mithilfe NovaStor DataCenter von /Network.	24. Mai 2018

Frühere Aktualisierungen

In der folgenden Tabelle werden wichtige Änderungen in den einzelnen Versionen des AWS Storage Gateway -Benutzerhandbuchs beschrieben, die vor Mai 2018 veröffentlicht wurden.

Änderung	Beschreibung	Änderungsdatum
Support für S3 One Zone_IA-S peicherklasse	Für File Gateways können Sie jetzt die S3 One Zone_IA als Standard-Speicherklasse für Ihre 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 die Storage Gateway unterstützen.	3. April 2018
Support für Cache-Aktualisieru ngsbenach richtigungen, Zahlungen durch den Anforderer und Vormerkun gen ACLs für Amazon S3 S3-Buckets.	Mit File Gateways können Sie nun eine Benachric htigung erhalten, wenn ein Gateway die Aktualisierung des Caches für Ihren Amazon S3-Bucket abgeschlo ssen hat. Weitere Informationen finden Sie unter RefreshCache.html in der Storage Gateway API-Refer enz. Mithilfe von File Gateways kann nun der Anforderer oder Abrufende anstelle des Bucket-Eigentümers für den Zugriff zahlen. Mithilfe von File Gateways können Sie nun dem Eigentümer des S3-Buckets, der der NFS-Datei freigabe zugeordnet ist, die volle Kontrolle gewähren. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	1. März 2018

Änderung	Beschreibung	Änderungsdatum
Support für Dell EMC NetWorker V9.x	Tape Gateways unterstützen jetzt Dell EMC V9.x. NetWorker Sie können jetzt Dell EMC NetWorker V9.x verwenden, um Ihre Daten auf Amazon S3 zu sichern und direkt im Offline-Speicher zu archivier en (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive). Weitere Informationen finden Sie unter Testen Ihres Setups mithilfe von 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 die Storage Gateway unterstüt zen.	18. Dezember 2017
Unterstützung für Datei-Upload-Benachrichtigu ng und zur Bestimmung des MIME-Typs	Mit File Gateways können Sie jetzt Benachric htigungen erhalten, sobald alle Dateien, die auf Ihre NFS-Dateifreigabe geschrieben werden, zu Amazon S3 hochgeladen wurden. Weitere Informationen finden Sie NotifyWhenUploadedin der Storage Gateway API-Referenz. Mit File Gateways können Sie jetzt den MIME-Typ für hochgeladene Objekte basierend auf Dateierwe iterungen bestimmen. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe.	21. November 2017
Support für VMware ESXi Hypervisor Version 6.5	AWS Storage Gateway unterstützt jetzt VMware ESXi Hypervisor Version 6.5. Diese Version wird zusätzlic h zu den Versionen 4.1, 5.0, 5.1, 5.5 und 6.0 unterstüt zt. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	13. September 2017

Änderung	Beschreibung	Änderungsdatum
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
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 die Storage Gateway unterstützen.	02. Mai 2017

Änderung	Beschreibung	Änderungsdatum
Updates bei den Einstellungen für Dateifreigaben Unterstützung für die Cache-Aktualisierung in Dateifreigaben	Die Einstellungen für Dateifreigaben in der File Gateway-Konfiguration wurden um Mounting-Optionen erweitert. Nun stehen für Dateifreigaben eine Squash-Option und eine schreibgeschützte Option zur Verfügung. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe. In der File-Gateway-Konfiguration lassen sich nun alle Objekte im Amazon-S3-Bucket finden, die hinzugefügt oder entfernt wurden, seit das Gateway letztmals die Inhalte des Buckets aufgelistet und die Ergebnisse zwischengespeichert hat. Weitere Informationen finden Sie RefreshCachein der API-Referenz.	28. März 2017
Unterstützung für das Klonen von Volumes	Unterstützt AWS Storage Gateway jetzt für zwischengespeicherte Volume Gateways die Möglichkeit, ein Volume von einem vorhandenen Volume zu klonen. Weitere Informationen finden Sie unter Klonen eines Volumes.	16. März 2017
Support für File Gateways bei Amazon EC2	AWS Storage Gateway bietet jetzt die Möglichkeit, ein File Gateway in Amazon bereitzustellen EC2. Sie können ein File Gateway in Amazon EC2 mit dem Storage Gateway Amazon Machine Image (AMI) starten, das jetzt als Community-AMI verfügbar ist. Informationen darüber, wie Sie ein File Gateway erstellen und auf einer EC2 Instance bereitstellen, finden Sie unter Amazon S3 File Gateway erstellen und aktivieren oder Amazon FSx File Gateway erstellen und aktivieren. Informationen zum Starten eines File Gateway-AMI finden Sie unter Bereitstellen eines S3 File Gateways auf einem EC2 Amazon-Host oder Bereitstellen von FSx File Gateway auf einem EC2 Amazon-Host.	08. Februar 2017

Änderung	Beschreibung	Änderungsdatum
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 Ihres Einrichtung mithilfe von Arcserve Backup r17.0.	17. Januar 2017
Neue -Region	Storage Gateway ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionen die Storage Gateway unterstützen.	13. Dezember 2016
Neue -Region	Storage Gateway ist jetzt in der Region Kanada (Zentral) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionen die Storage Gateway unterstützen.	08. Dezember 2016
Unterstützung für File Gateway	Zusätzlich zu Volume Gateways und Tape Gateway bietet Storage Gateway jetzt File Gateway. File Gateway kombiniert einen Service und eine virtuelle Software-Appliance. So können Sie Objekte in Amazon S3 mit Dateiprotokollen nach Branchenstandard wie beispielsweise NFS (Network File System) speichern und abrufen. Das Gateway stellt Objekte in Amazon S3 als Dateien auf einem NFS-Mounting-Punkt bereit.	29. November 2016
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 Ihres Einrichtung mithilfe von Veritas Backup Exec.	7. November 2016

Änderung	Beschreibung	Änderungsdatum
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 die Storage Gateway unterstützen.	17. Oktober 2016
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 Diensten wie CloudWatch Amazon EBS. Weitere Informati onen finden Sie unter Melde dich an für AWS Storage Gateway.	30. August 2016
Kompatibilität mit Veeam Backup & Re on V9 Update 2 und höher	Tape-Gateway ist nun kompatibel mit Veeam Backup & Replication V9 Update 2 und höher (d. h. mit Version 9.0.0.1715 und höheren Versionen). Sie können nun Veeam Backup Replication V9 Update 2verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivier en. Weitere Informationen finden Sie unter Testen der Einrichtung mithilfe von Veeam Backup & Replication.	15. August 2016

Änderung	Beschreibung	Änderungsdatum
Längeres Volumen und Snapshot IDs	Storage Gateway führt längere Versionen IDs für Volumes und Snapshots ein. Sie können das längere ID-Format für Ihre Volumes, Snapshots und andere unterstützte AWS Ressourcen aktivieren. Weitere Informationen finden Sie unter Grundlegendes zu Storage Gateway Gateway-Ressourcen und -Ressourcen IDs.	25. April 2016
Neue -Region Unterstützung für Stored Volumes mit bis zu 512 TiB Speicherkapazität Sonstige Gateway-Updates und -Verbesserungen in der lokalen Storage-Gateway-Konsole	Tape Gateway ist nun in der Region Asien-Pazifik (Seoul) verfügbar. Weitere Informationen finden Sie unter AWS-Regionen die Storage Gateway unterstützen. Stored Volumes unterstützen jetzt bis zu 32 Speicher-Volumes mit je bis zu 16 TiB und damit eine maximale Speicherkapazität von 512 TiB. Weitere Informationen finden Sie unter Architektur mit Stored Volumes und AWS Storage Gateway Kontingente. Die zulässige Gesamtgröße aller Bänder in einer virtuellen Bandbibliothek wurde auf 1 PiB erhöht. Weitere Informationen finden Sie unter AWS Storage Gateway Kontingente. Das Passwort der lokalen VM-Konsole kann jetzt in der Storage-Gateway-Konsole festgelegt werden. Weitere Informationen finden Sie unter Festlegen des Passworts der lokalen Konsole auf der Storage-Gateway-Konsole.	21. März 2016

Änderung	Beschreibung	Änderungsdatum
Kompatibilität mit für Dell EMC 8.x NetWorker	Tape Gateway ist jetzt mit Dell EMC NetWorker 8.x kompatibel. Sie können jetzt Dell EMC verwenden NetWorker , um Ihre Daten auf Amazon S3 zu sichern und direkt im Offline-Speicher zu archivieren (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive). Weitere Informationen finden Sie unter Testen Ihres Setups mithilfe von Dell EMC NetWorker.	29. Februar 2016
Support für VMware ESXi Hypervisor Version 6.0 und Red Hat Enterprise Linux 7 iSCSI-Initiator	AWS Storage Gateway unterstützt jetzt den VMware ESXi Hypervisor Version 6.0 und den Red Hat Enterprise Linux 7 iSCSI-Initiator. Weitere Informationen erhalten Sie unter Unterstützte Hypervisoren und Host-Anforderungen und Unterstützte iSCSI-Initiatoren.	20. Oktober 2015
Inhaltsumstrukturierung	Diese Version umfasst die folgende Verbesserung: Die Dokumentation wurde um einen Abschnitt zur Verwaltung aktivierter Gateways ergänzt. Dort finden Sie eine Übersicht über Verwaltungsaufgaben, die für alle Gateway-Lösungen gleich sind. Zudem finden Sie Anweisungen zur Verwaltung von Gateways nach der Bereitstellung und Aktivierung. Weitere Informationen finden Sie unter Verwaltung Ihres Tape Gateways.	

Änderung	Beschreibung	Änderungsdatum
Unterstützung für zwischengespeicherte Volumes mit bis zu 1 024 TiB Speicherkapazität Support für den Netzwerkadaptertyp VMXNET3 (10 GbE) im VMware ESXi Hypervisor Leistungsverbesserungen Verschiedene Verbesserungen und Aktualisierungen in der lokalen Storage Gateway-Konsole	Cached Volumes unterstützen jetzt bis zu 32 Speicher-Volumes mit je bis zu 32 TiB und damit eine maximale Speicherkapazität von 1 024 TiB. Weitere Informationen finden Sie unter Architektur mit zwischengespeicherten Volumes und AWS Storage Gateway Kontingente. Wenn Ihr Gateway auf einem VMware ESXi Hypervisor gehostet wird, können Sie das Gateway so umkonfigurieren, dass es den Adaptertyp verwendet . VMXNET3 Weitere Informationen finden Sie unter Netzwerkadapter für Ihr Gateway konfigurieren. Die maximale Upload-Rate für Storage Gateway wurde auf 120 MB pro Sekunde erhöht, die maximale Download-Rate auf 20 MB pro Sekunde. Die lokale Storage-Gateway-Konsole wurde aktualisiert und um zusätzliche Funktionen erweitert, die Sie bei Verwaltungsaufgaben unterstützen. Weitere Informationen finden Sie unter Konfigurieren Ihres Gateway-Netzwerks.	16. September 2015
Support für Markierungen	Storage Gateway unterstützt nun das Markieren von Ressourcen. Gateways, Volumes und virtuellen Bändern lassen sich zur einfacheren Verwaltung nun Tags hinzufügen. Weitere Informationen finden Sie unter Kennzeichnen der Storage Gateway-Ressourcen .	2. September 2015

Änderung	Beschreibung	Änderungsdatum
Kompatibilität mit Quest (ehemals Dell) NetVault Backup 10.0	Tape Gateway ist jetzt mit Quest NetVault Backup 10.0 kompatibel. Sie können jetzt Quest NetVault Backup 10.0 verwenden, um Ihre Daten auf Amazon S3 zu sichern und direkt im Offline-Speicher zu archivieren (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive). Weitere Informationen finden Sie unter Testen Ihres Setups 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 für die Einrichtung von Tape Gateway.	
	Diese Version umfasst die folgenden Verbesserungen und Aktualisierungen für Storage Gateway: • In der Storage-Gateway-Konsole können Sie jetzt das Datum und die Uhrzeit des letzten erfolgreichen Software-Updates auf Ihrem Gateway sehen. Weitere Informationen finden Sie unter Verwaltung von Gateway-Updates. • 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 ListVolumeInitiatorsin 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 Hyperviso rs Microsoft Hyper-V war bereits zuvor implementiert. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	30. April 2015
Kompatibilität mit Symantec Backup E:	Tape Gateway ist nun mit Symantec Backup Exec 15 kompatibel. Sie können nun Symantec Backup Exec 15 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec.	6. April 2015
Unterstützung für die CHAP-Auth entifizierung für Speicher-Volumes	Storage Gateway unterstützt jetzt die Konfiguration von CHAP-Authentifizierung für Speicher-Volumes. Weitere Informationen finden Sie unter Konfigurieren der CHAP-Authentifizierung für Ihre Volumes.	2. April 2015
Support für VMware ESXi Hypervisor Version 5.1 und 5.5	Storage Gateway unterstützt jetzt die VMware ESXi Hypervisor-Versionen 5.1 und 5.5. Dies gilt zusätzlic h zur Unterstützung der VMware ESXi Hypervisor-Versionen 4.1 und 5.0. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anfo rderungen.	30. März 2015

Änderung	Beschreibung	Änderungsdatum
Unterstützung für das Windows-Dienstprogramm CHKDSK	Storage Gateway unterstützt jetzt das Windows-Dienstprogramm CHKDSK. Mithilfe dieses Dienstprogramms können Sie die Integrität Ihrer Volumes überprüfen und Volume-Fehler beheben. Weitere Informationen finden Sie unter Fehlerbehebung bei Volume-Problemen.	04. März 2015
Integration mit AWS CloudTrail zur Erfassung von API-Aufrufen	Storage Gateway ist jetzt in integriert AWS CloudTrail. AWS CloudTrail erfasst API-Aufrufe, die von oder im Namen von Storage Gateway in Ihrem Amazon Web Services Services-Konto getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Weitere Informationen finden Sie unter Einloggen und Überwachen AWS Storage Gateway. Diese Version umfasst die folgenden Verbesserungen und Aktualisierungen für Storage Gateway: • Virtuelle Bänder, in deren Cache-Speicher ungültige Daten abgelegt sind (d. h. in denen nicht in AWS hochgeladene Inhalte abgelegt sind), werden jetzt wiederhergestellt, wenn das zwischengespeicherte Laufwerk eines Gateways geändert wird. Weitere Informationen finden Sie unter Wiederherstellen eines virtuellen Bandes von einem nicht wiederherstellbaren Gateway.	16. Dezember 2014

Änderung	Beschreibung	Änderungsdatum
Kompatibilität mit weiterer Sicherungssoftware und einem weiteren Medienwechsler	Tape-Gateway ist nun kompatibel mit der folgenden Sicherungssoftware: • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 Sie können jetzt diese vier Sicherungssoftware-Produkte mit der virtuellen Bandbibliothek (Virtual Tape Library, VTL) von Storage Gateway verwenden , um Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Verwenden Ihrer Sicherungssoftware zum Testen Ihrer Gateway-Einrichtung. Storage Gateway bietet nun einen zusätzlichen Medienwechsler, der mit der neuen Sicherungssoftware kompatibel ist. Diese Version enthält verschiedene AWS Storage Gateway Verbesserungen und Updates.	3. November 2014
Region Europa (Frankfurt)	Storage Gateway ist jetzt in der Region Europa (Frankfurt) verfügbar. Weitere Informationen hierzu finden Sie unter AWS-Regionen die Storage Gateway unterstützen.	23. Oktober 2014

Änderung	Beschreibung	Änderungsdatum
Inhaltsumstrukturierung	Wir haben einen gemeinsamen Erste-Schritte-Abschnitt für sämtliche Gateway-Lösungen verfasst. Dort finden Sie Links zu Anweisungen für den Download, die Bereitstellung und die Aktivierung von Gateways. Sobald Sie ein Gateway bereitgestellt und aktiviert haben, können Sie anhand weiterer Anleitungen Stored Volume-, Cached Volume- und Tape Gateway-Konfigurationen einrichten. Weitere Informationen finden Sie unter Erstellen eines Tape Gateways.	19. Mai 2014
Kompatibilität mit Symantec Backup E:	Tape Gateway ist nun mit Symantec Backup Exec 2012 kompatibel. Sie können nun Symantec Backup Exec 2012 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec.	28. April 2014

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Windows Server Failover Clustering Support für VMware ESX-Initiator Unterstützung für die Durchführung von Konfigurationsaufgaben in der lokalen Storage Gateway-Konsole	• Storage Gateway unterstützt jetzt Verbindungen zwischen mehreren Hosts und ein und demselben Volume, wenn die Hosts den Zugriff über Windows Server Failover Clustering (WSFC) koordinieren. Nicht über WSFC koordinierte Verbindungen zwischen mehreren Hosts und ein und demselben Volume werden jedoch nicht unterstützt. • Storage Gateway unterstützt jetzt die Verwaltung der Speicheranbindung direkt über den ESX-Host. Dies bietet eine Alternative zur Verwendung von Initiatoren, die sich im Gastbetriebssystem Ihres VMs befinden. • 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 . Informationen zum Ausführen von Konfigurationsaufgaben auf Gateways, die auf einer EC2 Instanz bereitgestellt werden, finden Sie unter Aufgaben auf der Amazon EC2 Local Console ausführen oder. Aufgaben auf der Amazon EC2 Local Console ausführen	31. Januar 2014

Änderung	Beschreibung	Änderungsdatum
Unterstützung für virtuelle Bandbibliotheken und Einführung der API-Version 2013-06-30	Storage Gateway verbindet eine lokale Software-Appliance mit cloudbasiertem Speicher, um Ihre lokale IT-Umgebung in die AWS Speicherinfrastruktur zu integrieren. Neben der Option Volume Gateway (zwischengespeicherte und gespeicherte Volumes) unterstützt Storage Gateway jetzt auch Gateways des Typs Virtual Tape Library (VTL). Ein Tape Gateway lässt sich mit bis zu 10 virtuellen Bandlaufwerken konfigurieren. Jedes virtuelle Bandlaufwerk reagiert auf den SCSI-Befehlssatz, sodass Ihre vorhandenen lokalen Sicherungsanwendungen ohne Anpassungen funktionieren. Weitere Informationen finden Sie in folgenden Themen im AWS Storage Gateway - Benutzerhandbuch: • Einen Überblick über die Architektur finden Sie unter So funktioniert Tape Gateway (Architektur). • Informationen zu den ersten Schritten mit Tape Gateway finden Sie unter Erstellen eines Tape Gateways.	5. November 2013
Unterstützung für Microsoft Hyper-V	Storage Gateway unterstützt jetzt die Bereitstellung eines On-Premises-Gateways auf der Virtualisierungsplattform Microsoft Hyper-V. Auf Microsoft Hyper-V bereitgestellte Gateways verfügen über denselben Funktionsumfang wie das vorhandene On-premises-Storage Gateway. Erste Schritte für die Bereitstellung eines Gateways mit Microsoft Hyper-V finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	10. April 2013

Änderung	Beschreibung	Änderungsdatum
Support für die Bereitstellung eines Gateways bei Amazon EC2	Storage Gateway bietet jetzt 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 unter verfügbar ist AWS Marketplace. Informationen zu den ersten Schritten für die Bereitstellung eines Gateways mithilfe des Storage Gateway-AMI finden Sie unter Stellen Sie eine maßgeschneiderte EC2 Amazon-Instance für Tape Gateway bereit.	15. Januar 2013

Änderung	Beschreibung	Änderungsdatum
Unterstützung für Cached Volumes und Einführung der API-Version 2012-06-30	Ab dieser Version unterstützt Storage Gateway Cached Volumes. Cached Volumes reduzieren die Notwendigkeit für Skalierungen Ihrer lokalen Speicherinfrastruktur auf ein Minimum und gewährleisten dabei gleichzeitig, dass Ihre Anwendungen mit niedriger Latenz auf ihre aktiven Daten zugreifen können. Sie können Speicher-Volumes mit bis zu 32 TiB erstellen und sie über Ihre lokalen Anwendungsserver als iSCSI-Geräte mounten. Auf zwischengespeicherten Volumes geschriebene Daten werden in Amazon Simple Storage Service (Amazon S3) gespeichert. Auf der On-Premises-Speicherhardware wird nur ein Cache mit den vor kurzem geschriebenen und gelesenen Daten lokal gespeichert. Dank Cached Volumes können Sie Daten, bei deren Abruf höhere Latenzen akzeptabel sind, in Amazon S3 speichern, beispielsweise ältere Daten, auf die selten zugegriffen wird. Daten, auf die Zugriff mit niedriger Latenz möglich sein muss, bleiben On-Premises gespeichert. In dieser Version von Storage Gateway wird zudem eine neue API-Version eingeführt, die neben den aktuell bereits verfügbaren Operationen neue Operationen für Cached Volumes bereitstellt. Weitere Informationen zu den beiden Storage Gateway-Lösungen finden Sie unter So funktioniert Tape Gateway. Sie können auch eine Testkonfiguration einrichten. Anweisungen finden Sie unter Erstellen eines Tape Gateways.	29. Oktober 2012

Änderung	Beschreibung	Änderungsdatum
API- und IAM-Unterstützung	In dieser Version führt Storage Gateway API-Unterstützung sowie Unterstützung für AWS Identity and Access Management(IAM) ein. • API-Unterstützung – Storage Gateway-Ressourcen lassen sich jetzt programmgesteuert konfigurieren und verwalten. Weitere Informationen zur API finden Sie unter Storage-Gateway-API-Referenz im AWS Storage Gateway -Benutzerhandbuch. • IAM-Unterstützung: Mithilfe von AWS Identity and Access Management (IAM) können Sie Benutzer erstellen und den Benutzerzugriff auf Ihre Storage Gateway-Ressourcen mithilfe von IAM-Richtlinien verwalten. Beispiele für IAM-Richtlinien finden Sie unter Identity and Access Management für AWS Storage Gateway. Weitere Informationen zu IAM finden Sie auf der Detailseite zu AWS Identity and Access Management (IAM).	9. Mai 2012
Unterstützung für statische IPs	Sie können nun eine statische IP für Ihr lokales Gateway festlegen. Weitere Informationen finden Sie unter Konfigurieren Ihres Gateway-Netzwerks.	5. März 2012
Neues Handbuch	Dies ist die erste Version des AWS Storage Gateway -Benutzerhandbuchs.	24. Januar 2012

Versionshinweise für die Tape Gateway-Appliance-Software

In diesen Versionshinweisen werden die neuen und aktualisierten Funktionen, Verbesserungen und Korrekturen beschrieben, die in jeder Version der Tape Gateway enthalten sind. Jede Softwareversion wird durch ihr Veröffentlichungsdatum und eine eindeutige Versionsnummer identifiziert.

Sie können die Softwareversionsnummer eines Gateways ermitteln, indem Sie die Seite „Details“ in der Storage Gateway Gateway-Konsole überprüfen oder die DescribeGatewayInformationAPI-Aktion mit einem AWS CLI Befehl aufrufen, der dem folgenden ähnelt:

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

Die Versionsnummer wird im `SoftwareVersion` Feld der API-Antwort zurückgegeben.

> **Note**
>
> Unter den folgenden Umständen meldet ein Gateway keine Informationen zur Softwareversion:
>
> - Das Gateway ist offline.
> - Auf dem Gateway wird ältere Software ausgeführt, die keine Versionsberichterstattung unterstützt.
> - Der Gateway-Typ ist FSx File Gateway.

Weitere Informationen zu Tape , einschließlich der Änderung des standardmäßigen automatischen Wartungs- und Aktualisierungszeitplans für ein Gateway, finden Sie unter Gateway-Updates mit der AWS Storage Gateway Console verwalten.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-07-01	2.12,11	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		neuer und vorhandener Gateways
2025-06-02	2.12,10	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-05-01	2.12,9	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-05-01	2.12,8	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-04-01	2.12,7	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-03-04	2.12,6	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-02-04	2,1,5	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways • Es wurde ein Problem behoben, bei dem Gateways nach einem Softwareupdate im heruntergefahrenen Zustand hängen bleiben konnten
2025-01-07	2.12.3	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2024-12-06	2.12.2	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-11-06	2.12,1	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2024-10-03	2.12.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2024-08-30	2.11.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
29.07.2024-07	2.10.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways • Verschiedene Fehlerkor rekturen und Verbesser ungen

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-06-17	2.9.2	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2024-05-28	2.9.0	• Verkürzte Gateway-N eustartzeit bei Softwareu pdates • Die zur Schätzung der Netzwerkbandbreite übertragene Datenmenge wurde reduziert
2024-05-08	2,8.3	• Das Problem mit der Cloud-Konnektivität bei der Verwendung eines SOCKS5 Proxys wurde behoben • Das Problem mit Leistungs einbußen beim Upload unter bestimmten Bedingung en (z. B. bei einer hohen Anzahl von Bandlösch vorgängen) wurde behoben

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-04-10	2.8.1	• Ein in 2.8.0 eingeführtes Problem mit der Speichern utzung wurde behoben • Sicherheitspatch-Updates • Verbesserter Software-Aktualisierungsprozess • Die fehlende NTP-Kompo nente (Network Time Protocol) für neue Gateways wurde behoben
2024-03-06	2.8.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer Gateways • Sicherheitspatch-Updates • Verbesserte Leistung für gleichzeitige Backup- und Wiederherstellungs-Workloads
2023-12-19	2.7.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer Gateways
2023-12-14	2,6.6	• Es wurde ein Problem mit der relativen Positionierung auf Bändern mit mehr als 5 TiB behoben

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2023-10-19	2,6.5	• Es wurden Schutzmaß nahmen gegen das Überschreiben von Bändern durch Clients nach einem Gateway-Neustart hinzugefü gt

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.