Benutzerhandbuch für Volume Gateway

AWS Storage Gateway

API-Version 2013-06-30

AWS Storage Gateway: Benutzerhandbuch für Volume Gateway

Table of Contents

Was ist Volume Gateway? 1
So funktioniert Volume Gateway 2
Volume Gateways 2
Erste Schritte mit AWS Storage Gateway 8
Melde dich an für AWS Storage Gateway 8
Einen IAM-Benutzer mit Administratorrechten erstellen 9
Zugreifen AWS Storage Gateway 11
AWS-Regionen die Storage Gateway unterstützen 11
Anforderungen an die Einrichtung von Volume Gateway 13
Hardware- und Speicheranforderungen 13
Hardwareanforderungen für VMs 13
Anforderungen für Amazon-EC2-Instance-Typen 14
Speicheranforderungen 14
Netzwerk- und Firewall-Anforderungen 15
Port-Anforderungen 16
Netzwerk- und Firewall-Anforderungen für die Hardware-Appliance 29
Gewähren von Gateway-Zugriff über Firewalls und Router 32
Konfigurieren einer Sicherheitsgruppe 35
Unterstützte Hypervisoren und Host-Anforderungen 36
Unterstützte iSCSI-Initiatoren 37
Verwenden der Hardware-Appliance 39
Einrichten Ihrer Hardware-Appliance 40
Physische Installation Ihrer Hardware-Appliance 42
Zugreifen auf die Hardware-Appliance-Konsole 44
Netzwerkparameter der Hardware-Appliance konfigurieren 45
Aktivieren Ihrer Hardware-Appliance 47
Erstellen eines Gateways auf Ihrer Hardware-Appliance 48
Konfiguration einer Gateway-IP-Adresse auf der Hardware-Appliance 49
Gateway-Software von Ihrer Hardware-Appliance entfernen 52
Löschen Ihrer Hardware-Appliance 53
Erstellen Sie Ihr Gateway 55
Überblick – Gateway-Aktivierung 55
Einrichten eines Gateways 55
Verbinden mit AWS 56

Überprüfen und aktivieren ... 56
Überblick – Gateway-Konfiguration ... 56
Überblick – Speicherressourcen ... 56
Erstellen eines Volume Gateways ... 57
Einrichten eines Volume Gateways ... 57
Connect Ihr Volume Gateway mit AWS ... 58
Überprüfen von Einstellungen und Aktivieren Ihres Volume Gateways ... 60
Konfigurieren Ihres Volume Gateways ... 61
Erstellen eines Volumes ... 63
Konfigurieren der CHAP-Authentifizierung für Ihre Volumes ... 66
Verbinden Sie Ihre Volumes mit Ihrem Client ... 66
Verbindung zu einem Microsoft Windows-Client herstellen ... 67
Verbindung zu einem Red Hat Enterprise Linux Client herstellen ... 67
Volume initialisieren und formatieren ... 69
Initialisierung und Formatierung unter Windows ... 69
Initialisierung und Formatierung auf RHEL ... 71
Testen Sie Ihr Gateway ... 72
Sicherung Ihrer Volumes ... 74
Verwenden von Storage Gateway zum Sichern Ihrer Volumes ... 74
Wird AWS Backup zur Sicherung Ihrer Volumes verwendet ... 74
Wie geht es weiter? ... 77
Bestimmen der Größe des Volume-Gateway-Speichers für reale Workloads ... 78
Aktivieren eines Gateways in einer Virtual Private Cloud ... 80
Erstellen eines VPC-Endpunkts für Storage Gateway ... 81
Verwalten Ihres Volume Gateways ... 83
Bearbeiten von Gateway-Informationen ... 85
Volumen hinzufügen und erweitern ... 86
Ein Volume klonen ... 87
Volumenverbrauch anzeigen ... 89
Löschen von Speichervolumes ... 89
Verschieben Ihrer Volumes zu einem anderen Gateway ... 90
Einen Wiederherstellungs-Snapshot erstellen ... 93
Einen Snapshot-Zeitplan bearbeiten ... 94
Löschen von Snapshots ... 95
Verwenden des AWS SDK for Java ... 95
Das AWS SDK for .NET verwenden ... 99

Mit dem AWS Tools for Windows PowerShell ... 106
Grundlagen zu Status und Übergängen bei Volumes ... 108
Grundlagen zum Volume Status ... 108
Grundlagen zum Volume Status ... 115
Grundlagen zu Statusübergängen bei zwischengespeicherten Volumes ... 115
Grundlagen zu Statusübergängen bei gespeicherten Volumes ... 117
Verschieben Ihrer Daten auf eine neue Gateway-Instanz ... 121
Verschieben gespeicherter Volumes auf ein neues gespeichertes Volume Gateway ... 121
Verschieben zwischengespeicherter Volumes auf eine neue virtuelle Gateway-Maschine ... 124
Überwachen von Storage Gateway ... 130
Grundlagen zu Gateway-Metriken ... 131
Dimensionen für Storage-Gateway-Metriken ... 138
Überwachen des Upload-Puffers ... 138
Überwachen des Cache-Speichers ... 141
CloudWatch Alarme verstehen ... 143
Empfohlene CloudWatch Alarme erstellen ... 145
Einen benutzerdefinierten CloudWatch Alarm erstellen ... 146
Überwachung Ihres Volume Gateways ... 148
Volume Gateway-Zustandsprotokolle abrufen ... 149
Amazon CloudWatch Metrics verwenden ... 151
Messung der Leistung zwischen Ihrer Anwendung und dem Gateway ... 152
Messung der Leistung zwischen Ihrem Gateway und AWS ... 154
Volumenmetriken verstehen ... 158
Warten eines Gateways ... 167
Verwalten von lokalen Festplatten ... 167
Bestimmen der Größe des lokalen Festplattenspeichers ... 168
Hinzufügen von Upload-Puffer oder Cache-Speicher ... 172
Verwalten der Bandbreite ... 173
Ändern der Bandbreitendrosselung mithilfe der Storage-Gateway-Konsole ... 174
Planung der Bandbreitendrosselung ... 174
Mit dem AWS SDK für Java ... 176
Mit dem AWS SDK für .NET ... 178
Mit dem AWS Tools for Windows PowerShell ... 180
Verwaltung von Gateway-Updates ... 182
Aktualisierungshäufigkeit und erwartetes Verhalten ... 182
Wartungsupdates ein- oder ausschalten ... 183

Ändern Sie den Zeitplan für das Gateway-Wartungsfenster ... 184
Manuelles Anwenden eines Updates ... 185
Herunterfahren der Gateway-VM ... 187
Starten und Anhalten eines Volume Gateways ... 187
Löschen Sie Ihr Gateway und entfernen Sie Ressourcen ... 188
Löschen eines Gateways mithilfe der Storage-Gateway-Konsole ... 189
Entfernen von Ressourcen von einem lokal bereitgestellten Gateway ... 190
Entfernen von Ressourcen von einem auf einer Amazon-EC2-Instance bereitgestellten Gateway ... 191
Durchführung von Wartungsaufgaben über die lokale Konsole ... 192
Zugreifen auf die lokale Konsole des Gateways ... 192
Zugreifen auf die lokale Konsole des Gateways mit Linux KVM ... 193
Zugreifen auf die lokale Gateway-Konsole mit VMware ESXi ... 193
Zugreifen auf die lokale Gateway-Konsole mit Microsoft Hyper-V ... 194
Ausführen von Aufgaben in der lokalen VM-Konsole von ... 195
An der lokalen Konsole von Volume Gateway anmelden ... 196
Konfiguration eines SOCKS5 Proxys für Ihr lokales Gateway ... 198
Konfigurieren Ihres Gateway-Netzwerks ... 199
Testen Sie Ihre Gateway-Konnektivität zum Internet ... 206
Storage-Gateway-Befehle in der lokalen Konsole für ein lokales Gateway ausführen ... 207
Anzeigen des Gateway-Systemressourcen-Status ... 210
Ausführen von Aufgaben in der lokalen EC2-Konsole ... 212
Anmelden bei der lokalen EC2-Konsole des Gateways ... 212
Konfigurieren eines HTTP-Proxys ... 213
Testen der Gateway-Netzwerkkonnektivität ... 214
Anzeigen des Gateway-Systemressourcen-Status ... 215
Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole ... 216
Leistung und Optimierung für Volume Gateway ... 219
Optimierung der Gateway-Leistung ... 219
Empfohlene Konfiguration ... 219
Hinzufügen von Ressourcen zu Ihrem Gateway ... 220
Optimieren von iSCSI-Einstellungen ... 223
Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung ... 224
Sicherheit ... 225
Datenschutz ... 226
Datenverschlüsselung ... 227

Konfigurieren der CHAP-Authentifizierung ... 229
Identitäts- und Zugriffsverwaltung ... 230
Zielgruppe ... 231
Authentifizierung mit Identitäten ... 231
Verwalten des Zugriffs mit Richtlinien ... 233
So funktioniert AWS Storage Gateway mit IAM ... 234
Beispiele für identitätsbasierte Richtlinien ... 240
Fehlerbehebung ... 243
Compliance-Validierung ... 245
Ausfallsicherheit ... 246
Infrastruktursicherheit ... 247
AWS Bewährte Methoden im Bereich Sicherheit ... 248
Protokollieren und Überwachen ... 248
Storage Gateway Gateway-Informationen in CloudTrail ... 249
Informationen zu Storage-Gateway-Protokolldateieinträgen ... 250
Fehlerbehebung bei Gateway-Problemen ... 253
Fehlerbehebung: Gateway-Offline-Probleme ... 254
Überprüfen Sie die zugehörige Firewall oder den zugehörigen Proxy ... 254
Suchen Sie nach einer laufenden SSL- oder Deep-Packet-Inspektion des Datenverkehrs Ihres Gateways ... 254
Suchen Sie nach einem Strom- oder Hardwarefehler auf dem Hypervisor-Host ... 254
Suchen Sie nach Problemen mit einer zugehörigen Cache-Festplatte ... 255
Fehlerbehebung: Probleme mit der Gateway-Aktivierung ... 255
Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt ... 256
Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen Amazon VPC-Endpunkt ... 259
Beheben Sie Fehler, wenn Sie Ihr Gateway über einen öffentlichen Endpunkt aktivieren und es in derselben VPC einen Storage Gateway Gateway-VPC-Endpunkt gibt ... 264
Fehlerbehebung bei lokalen Gateway-Problemen ... 264
Aktivierung Support zur Unterstützung bei der Fehlerbehebung Ihres Gateways ... 269
Fehlerbehebung bei Problemen mit der Einrichtung von Microsoft Hyper-V ... 271
Fehlerbehebung bei Problemen mit Amazon-EC2-Gateway ... 275
Die Aktivierung des Gateways ist nach einigen Momenten nicht erfolgt. ... 276
EC2-Gateway-Instance in der Instance-Liste nicht gefunden ... 276
Ein Amazon-EBS-Volume kann nicht an die EC2-Gateway-Instance angefügt werden ... 277
Sie können keinen Initiator an ein Volume-Ziel auf dem EC2-Gateway anfügen ... 277

Beim Hinzufügen von Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind ... 277
So entfernen Sie einen als Upload-Pufferspeicher zugewiesenen Datenträger, um die Größe des Upload-Pufferspeichers zu reduzieren ... 277
Durchsatz zum oder vom EC2-Gateway sinkt auf Null ... 278
Aktivierung Support zur Unterstützung der Fehlerbehebung am Gateway ... 278
Verbindung mit Ihrem Amazon-EC2-Gateway über die serielle Konsole ... 280
Fehlerbehebung bei Hardware-Appliance-Problemen ... 280
So ermitteln Sie die Service-IP-Adresse ... 281
So führen Sie eine Zurücksetzung auf die Werkseinstellungen durch ... 281
So führen Sie einen Remote-Neustart durch ... 281
So erhalten Sie Support für Dell iDRAC ... 281
So finden Sie die Seriennummer der Hardware-Appliance ... 281
So erhalten Sie Hardware-Appliance-Support ... 282
Fehlerbehebung bei Volume-Problemen ... 282
Die Konsole behauptet, dass Ihre Volume nicht konfiguriert ist ... 283
Die Konsole gibt an, dass Ihre Volume verloren ist ... 283
Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen ... 284
Die Konsole gibt an, das Ihre Volume PASS THROUGH Status hat ... 284
Sie möchten Volume-Integrität überprüfen und möglicher Fehler beheben ... 285
Ihre Volume-iSCSI-Target erscheint nicht in Windows Disk Management Konsole ... 286
Sie möchten den iSCSI-Volumen-Zielnamen ändern ... 286
Ihr geplanter Volume Snapshot taucht nicht auf ... 286
Sie müssen eine Festplatte entfernen oder ersetzen, die ausgefallen ist ... 286
Durchsatz von Ihrer Anwendung zu einem Volume ist auf Null abgefallen ... 287
In einem Cache-Datenträger in Ihrem Gateway tritt ein Fehler auf ... 287
Ein Volume Snapshot hat einen PENDING Status länger als erwartet ... 288
High Availability-Zustandsbenachrichtigungen ... 289
Beheben von Problemen mit Hochverfügbarkeit ... 289
Zustandsbenachrichtigungen ... 289
Kennzahlen ... 291
Best Practices ... 292
Bewährte Methoden: Wiederherstellung Ihrer Daten ... 292
Wiederherstellung nach dem unerwarteten Herunterfahren einer VM ... 293
Wiederherstellen von Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM ... 293
Wiederherstellung von Daten von einem nicht wiederherstellbaren Volume ... 294

Wiederherstellen von Daten von einem fehlerhaften Cache-Datenträger 295
Wiederherstellen von Daten von einem beschädigten Datensystem 295
Wiederherstellen von Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann 296
Säuberung unnötiger Ressourcen 297
Reduzierung der Menge des fakturierten Speichers auf einem Volume 298
Weitere Ressourcen 299
Host-Setup 300
Stellen Sie einen Amazon EC2 EC2-Standardhost für Volume Gateway bereit 301
Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume Gateway bereit . 304
Metadatenoptionen Amazon EC2 EC2-Instances ändern 308
Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Hostzeit 308
Synchronisieren Sie die VM-Zeit mit der VMware Host-Zeit 309
Konfigurieren Sie paravirtualisierte Festplattencontroller 311
Netzwerkadapter für Ihr Gateway konfigurieren 312
VMware Hochverfügbarkeit mit Storage Gateway verwenden 317
Arbeiten mit Volume Gateway-Speicherressourcen 323
Entfernen von Datenträgern aus dem Gateway 323
EBS-Volumes für EC2-Gateways 325
Den Aktivierungsschlüssel erhalten 326
Linux (curl) 327
Linux (bash/zsh) 329
Microsoft Windows PowerShell 329
Verwenden der lokalen Konsole 330
Verbinden von iSCSI-Initiatoren 332
Von einem Windows-Client aus eine Verbindung zu Ihren Volumes herstellen 333
Volumes einem Linux-Client verbinden 336
Anpassen von iSCSI-Einstellungen 338
Konfigurieren der CHAP-Authentifizierung 345
Verwendung Direct Connect mit Storage Gateway 351
Die Gateway-IP-Adresse abrufen 352
Abrufen einer IP-Adresse von einem Amazon-EC2-Host 353
IPv6 Unterstützung 354
Ressourcen und Ressourcen verstehen IDs 354
Mit Resource arbeiten IDs 355
Markieren Ihrer Ressourcen 355

Arbeiten mit Tags ... 356
Open-Source-Komponenten ... 358
Kontingente ... 358
Kontingente für Volumes ... 358
Empfohlene Kapazität für die lokalen Datenträger des Gateways ... 359
API-Referenz ... 361
Erforderliche Abfrage-Header ... 361
Signieren von Anforderungen ... 364
Signatur-Berechnungsbeispiel ... 365
Fehlermeldungen ... 367
Ausnahmen ... 367
Operationsfehlercodes ... 370
Fehlermeldungen ... 389
Operationen ... 391
Dokumentverlauf ... 392
Frühere Aktualisierungen ... 411
Migration von AL2 nach AL2023 ... 431
Schnelllinks und Ressourcen ... 432
Referenz zur Migration von Gateway-Versionen ... 432
Zeitplan für die Migration ... 432
Pre-migration Checkliste ... 432
Leitfäden zur Migration ... 433
Support und Überwachung ... 433
Häufig gestellte Fragen ... 434
Versionshinweise ... 435
... cdxlvii

Was ist Volume 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 Volume Gateway.

Volume Gateway bietet Cloud-gestützte Speichervolumes, die Sie als Internet Small Computer System Interface (iSCSI) -Geräte von Ihren lokalen Anwendungsservern aus bereitstellen können.

Volume Gateway unterstützt die folgenden Volume-Konfigurationen:

- Zwischengespeicherte Volumes – Sie speichern Ihre Daten in Amazon Simple Storage Service (Amazon S3) und halten lokal eine Kopie von Datenteilmengen vor, auf die häufig zugegriffen wird. Zwischengespeicherte Volumes bieten substanzielle Kosteneinsparungen bei primärem Speicher und minimieren den Anpassungsbedarf für lokalen Speicher. Sie behalten auch einen schnellen Zugriff auf Daten, auf die häufig zugegriffen wird.
- Gespeicherte Volumes – Wenn Sie schnellen Zugriff auf Ihren ganzen Datensatz benötigen, können Sie Ihr lokales Gateway zunächst so konfigurieren, dass alle Ihre Daten lokal gespeichert werden. Sichern Sie dann asynchron point-in-time Schnappschüsse dieser Daten auf Amazon S3. Diese Konfiguration bietet langlebige und kostengünstige externe Backups, die Sie in Ihrem lokalen Rechenzentrum oder in Amazon Elastic Compute Cloud (Amazon EC2) wiederherstellen können.

Wenn Sie beispielsweise Ersatzkapazität für die Notfallwiederherstellung benötigen, können Sie die Backups auf Amazon wiederherstellen EC2.

Eine Übersicht über die Architektur finden Sie unter So funktioniert Volume 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 Volume Gateway und Abschnitte, in denen beschrieben wird, wie Sie Ihr bereitstellen, aktivieren, konfigurieren und verwalten.

Die Verfahren in diesem Benutzerhandbuch konzentrieren sich hauptsächlich auf die Durchführung von Gateway-Vorgängen mithilfe von AWS-Managementkonsole. Informationen zum programmgesteuerten Ausführen dieser Operationen finden Sie in der AWS Storage Gateway -API-Referenz.

So funktioniert Volume Gateway

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

Volume Gateways

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

Themen

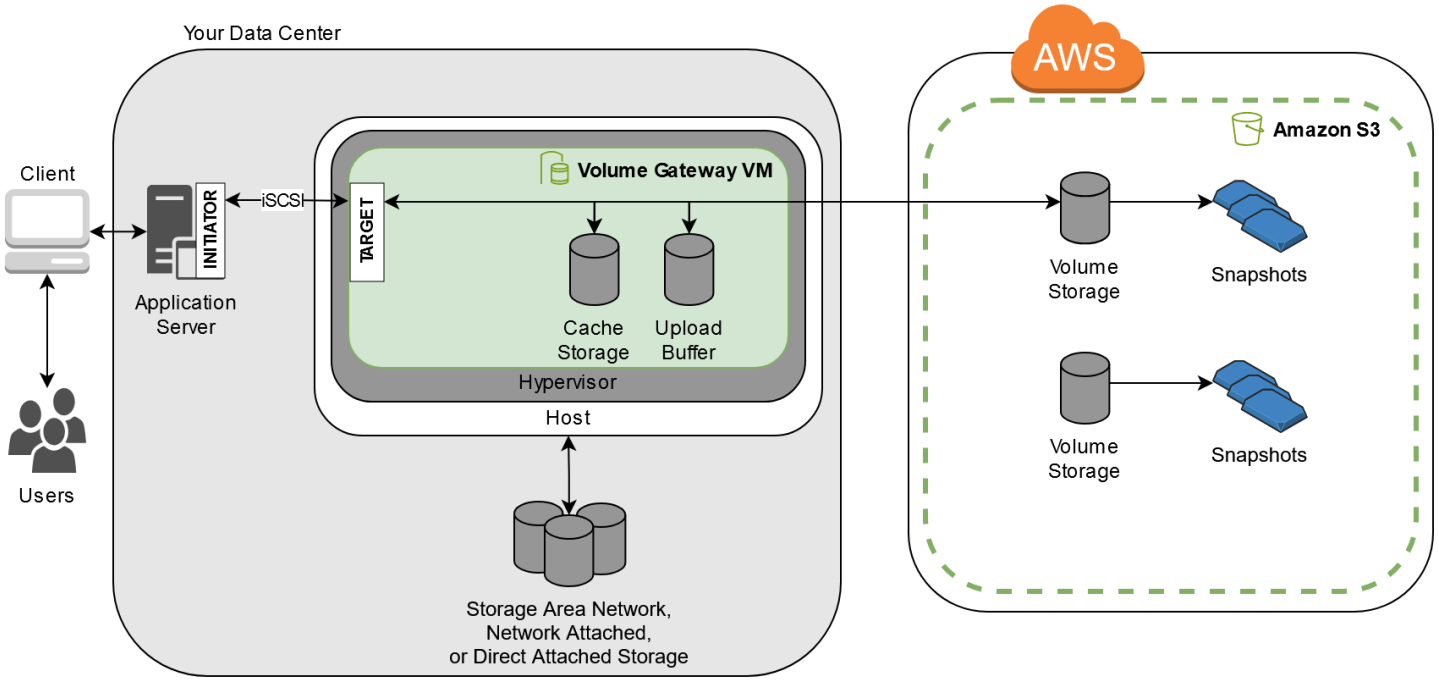
- Architektur mit zwischengespeicherten Volumes
- Architektur mit Stored Volumes

Architektur mit zwischengespeicherten Volumes

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

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

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



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

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

- Festplatten zur Verwendung durch das Gateway als Cache-Speicher — Wenn Ihre Anwendungen Daten auf die Speichervolumes schreiben AWS, speichert das Gateway die Daten zunächst auf den lokalen Festplatten, die für den Cache-Speicher verwendet werden. Danach werden die Daten vom Gateway in Amazon S3 hochgeladen. Der Cache-Speicher fungiert wie der dauerhafte On-

Premises-Speicher für Daten, die vom Upload-Puffer aus in Amazon S3 hochgeladen werden sollen.

Dank der Cache-Speicherung kann das Gateway auch die Daten, auf die die Anwendung zuletzt zugegriffen hat, lokal speichern, sodass ein schneller Zugriff möglich ist. Wenn die Anwendung Daten anfordert, überprüft das Gateway zunächst den Cache-Speicher auf Daten, bevor Amazon S3 überprüft wird.

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

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

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

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

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

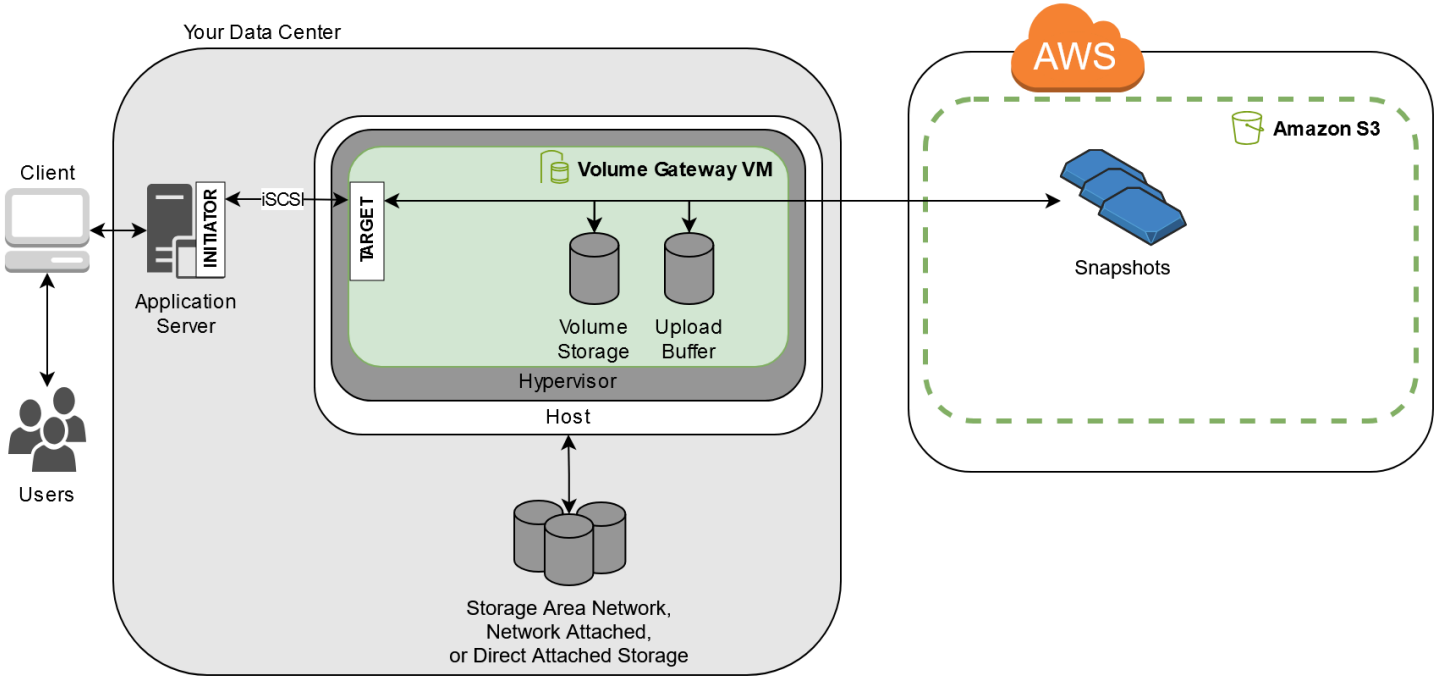
Architektur mit Stored Volumes

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

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

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

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



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

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

Sie können inkrementelle Sicherungen, sogenannte Snapshots, der Speicher-Volumes durchführen. Das Gateway speichert diese Snapshots in Amazon S3 als Amazon-EBS-Snapshots. Für jeden neuen Snapshot werden nur die Daten gespeichert, die seit dem letzten Snapshot geändert wurden. Wenn der Snapshot erstellt wurde, lädt das Gateway die Änderungen bis zum Snapshot-Punkt hoch und erstellt dann den neuen Snapshot mithilfe von Amazon EBS. Sie können Snapshots nach einem Zeitplan oder zu einem bestimmten Zeitpunkt starten. Ein einzelnes Volume unterstützt das schnelle

Aneinanderreihen mehrerer Snapshots in einer Warteschlange, aber jeder Snapshot muss fertig erstellt sein, bevor der nächste erstellt werden kann. Wenn Sie einen Snapshot löschen, werden nur die Daten entfernt, die nicht für einen anderen Snapshot benötigt werden.

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

Erste Schritte mit AWS Storage Gateway

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

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

Topics

- Melde dich an für AWS Storage Gateway- Erfahre, wie du dich registrierst AWS und ein AWS Konto erstellst.
- Einen IAM-Benutzer mit Administratorrechten erstellen- 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.

Einen IAM-Benutzer mit Administratorrechten erstellen

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 Anleitungen unter IAM-Benutzer für den Notfallzugriff erstellen im IAM-Benutzerhandbuch.	Sie konfigurieren den programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch.

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

Zugreifen AWS Storage Gateway

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

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

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

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

AWS-Regionen die Storage Gateway unterstützen

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

jeweils über redundante Stromversorgung, Netzwerke und Konnektivität verfügen und in separaten Einrichtungen untergebracht sind. Das bedeutet, AWS-Region dass jede Region physisch isoliert und unabhängig von den anderen Regionen ist. Regionen bieten Fehlertoleranz, Stabilität und Ausfallsicherheit und können auch die Latenz verkürzen. Die Ressourcen, die Sie in einer Region erstellen, sind in keiner anderen Region vorhanden, es sei denn, Sie verwenden ausdrücklich eine von einem AWS Dienst angebotene Replikationsfunktion. 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

Anforderungen für die Einrichtung von Volume 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

Hardware- und Speicheranforderungen

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

Hardwareanforderungen für VMs

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

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

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

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

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

Für Volume Gateway sollte Ihre Amazon EC2 EC2-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.

Volumes empfohlen

- General-purpose Instance-Familie — Instance-Typ m5 oder m6.
- Compute-optimized Instance-Familie — Instance-Typen c5, c6 oder c7. Wählen Sie die Instance-Größe 2xlarge oder höher aus, um die erforderlichen RAM-Anforderungen zu erfüllen.
- Memory-optimized Instance-Familie — Instance-Typen r5, r6 oder r7.
- Storage-optimized 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
Gateway für zwischengespeicherte Volumes	150 GiB	64 TiB	150 GiB	2 TiB	—
Gateway für gespeicherte Volumes	—	—	150 GiB	2 TiB	1 oder mehr für gespeicherte Volumes oder Volumes

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

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

Netzwerk- und Firewall-Anforderungen

Das Gateway muss unter anderem auf das Internet, lokale Netzwerke, DNS (Domain Name Service)-Server, Firewalls und Router zugreifen können. Nachfolgend finden Sie Informationen zu den erforderlichen Ports sowie eine Anleitung zur Gewährung von Zugriff über Firewalls und Router.

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

Themen

- Port-Anforderungen
- Netzwerk- und Firewall-Anforderungen für das Storage-Gateway-Hardwaregerät
- Zulassen AWS Storage Gateway Zugriff über Firewalls und Router
- Konfigurieren von Sicherheitsgruppen für eine Amazon-EC2-Gateway-Instance

Port-Anforderungen

Volume 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.

Portanforderungen für

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

Netzwerkelement	Aus	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								VM ist es nicht erforderlich, dass Port 80 öffentlich zugänglich ist. Die erforderliche Ebene des Zugangs auf Port 80 hängt von der Netzwerkkonfiguration ab. Wenn Sie Ihr Gateway von der Storage Gateway Management Console aus

Netzwerkelement	Aus	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
								aktivieren, muss der Host, von dem aus Sie eine 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	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
DNS	Storage-Gateway-VM	Domain Name Service (DNS)-Server	TCP- und UDP-DNS	53	✓	✓	✓	Wird für die Kommunikation zwischen einer Storage Gateway Gateway-VM und dem DNS-Server für die IP-Namensauflösung verwendet.

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

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

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

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

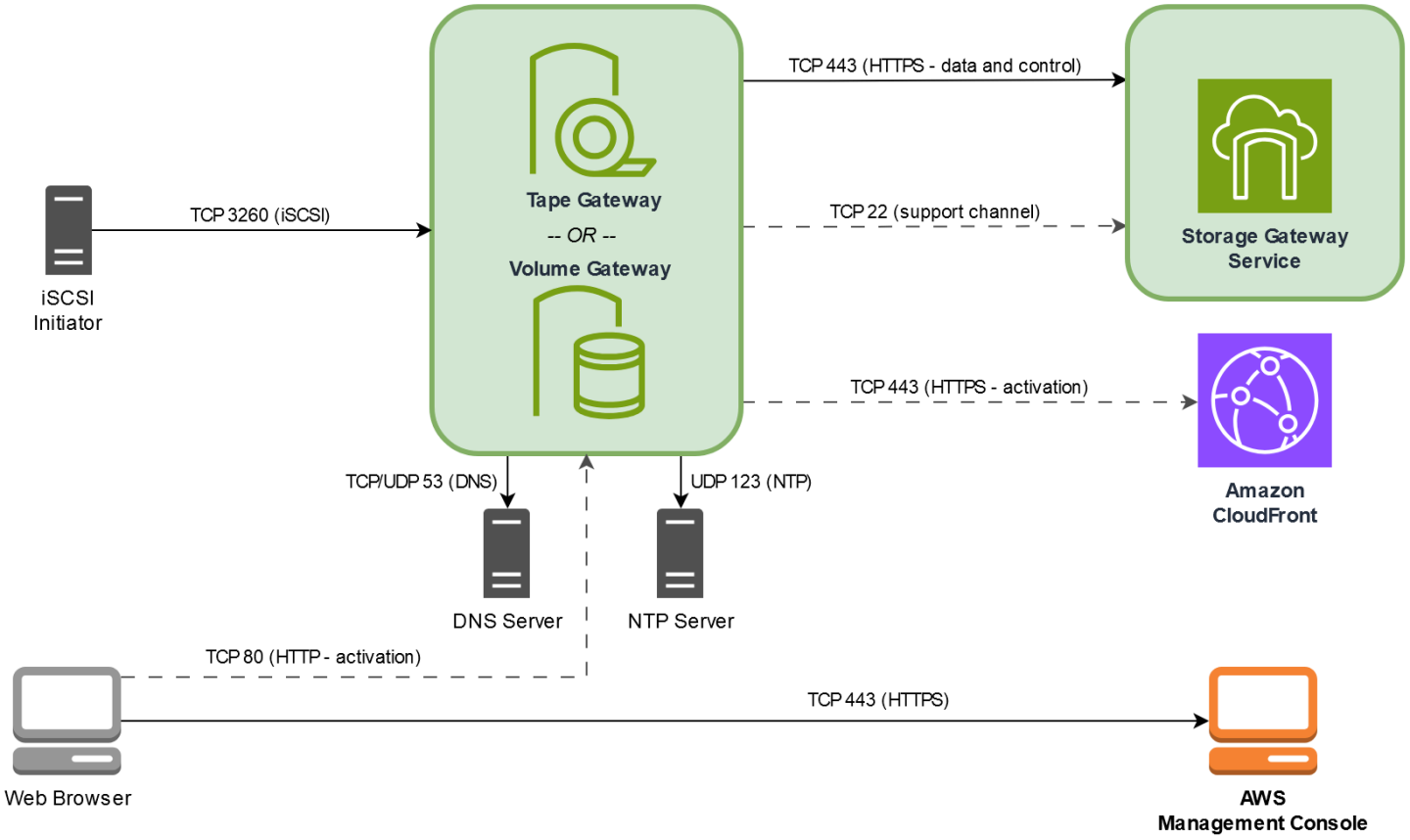
Netzwerkelement	Aus	Bis	Protocol (Protokoll)	Port	Eingehend	Ausgehend	Erforderlich	Hinweise
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	443	✓	✓	✓*	Managementkontrolle *Nur erforderlich, wenn VPC-Endpoints verwendet werden
VPC	Storage-Gateway-VM	AWS	TCP HTTPS	1026		✓	✓*	Endpunkt der Kontrollebene *Nur erforderlich,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

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

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

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



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

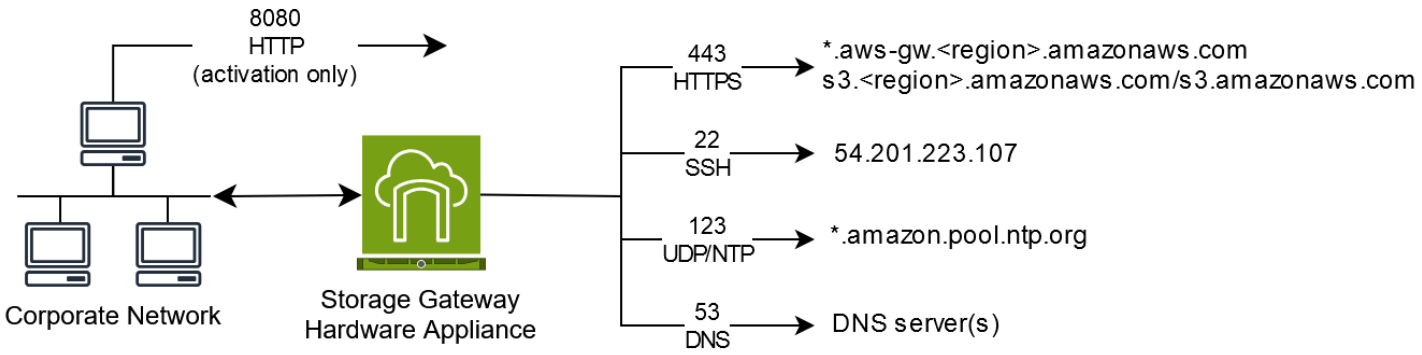
Jedes Storage-Gateway-Hardwaregerät benötigt die folgenden Netzwerkdienste:

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

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

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

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



Eine Hardware-Appliance benötigt die folgenden Ports.

Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	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

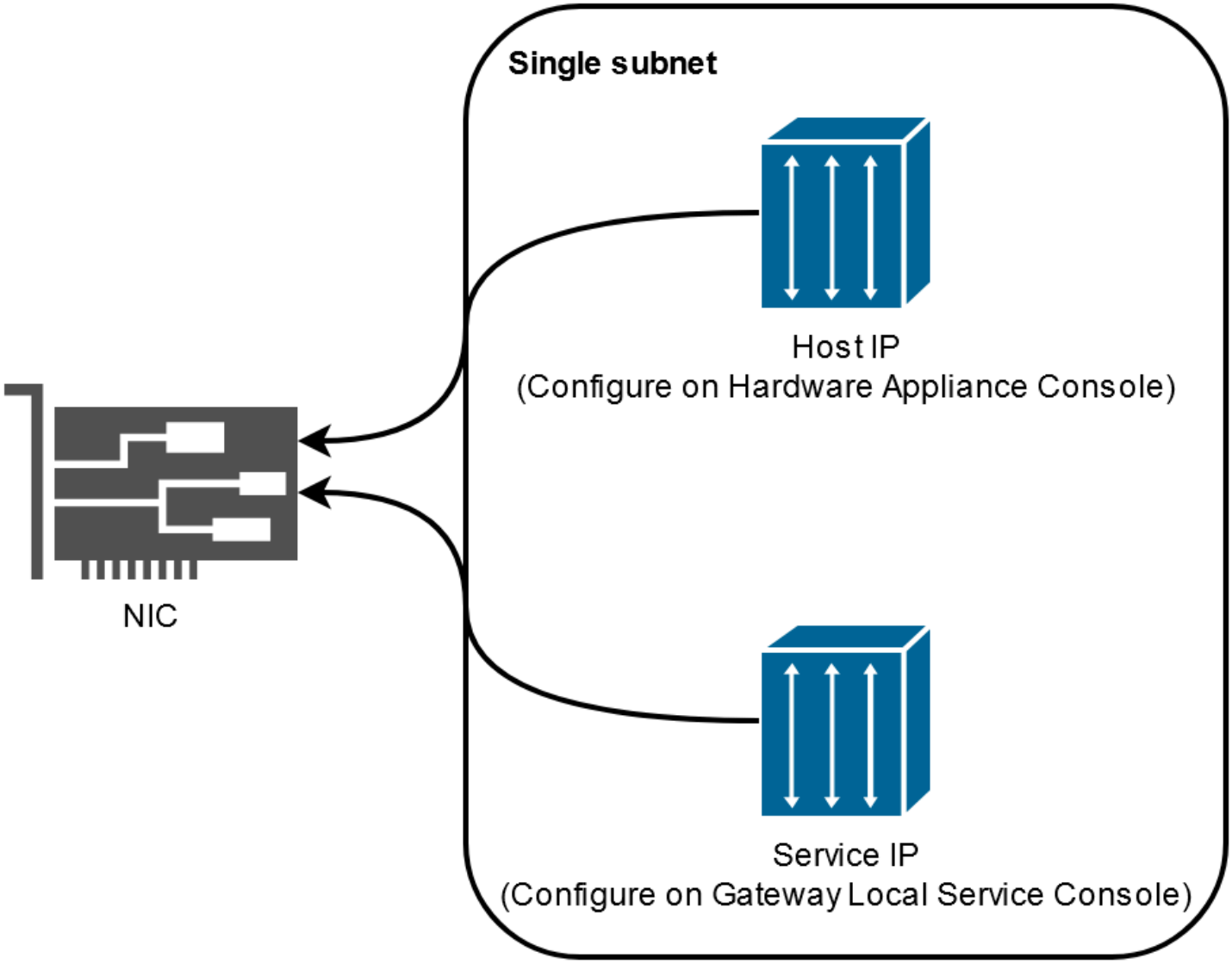
Protocol (Protokoll)	Port	Richtung	Quelle	Ziel	Verwendung
HTTP	8080	Eingehend	AWS	Hardware-Appliance	Aktivierung (nur kurz)

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.

Zulassen AWS Storage Gateway Zugriff über Firewalls und Router

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

> **Note**
>
> Wenn Sie private VPC-Endpunkte für Ihr Storage Gateway konfigurieren, die für die Verbindung und Datenübertragung von und zu verwendet werden 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.

Endpunkttypen

Standard-Endpunkte

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

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

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

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

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

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

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

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

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

Dual-stack Endpunkte

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

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

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

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

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

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

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

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

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

NTP-Server

Eine Storage Gateway Gateway-VM benötigt Netzwerkzugriff auf die folgenden NTP-Server.

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

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

Eine vollständige Liste der unterstützten Endpunkte AWS-Regionen und Service-Endpunkte finden Sie unter Storage Gateway in der Allgemeine AWS-Referenz.

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

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

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

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

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

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

Unterstützte Hypervisoren und Host-Anforderungen

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

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

> **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 außerdem einen VMware vSphere-Client, um eine Verbindung zum Host herzustellen.
- Microsoft Hyper-V Hypervisor (Version 2019, 2022 oder 2025) — Für dieses Setup benötigen Sie einen Microsoft Hyper-V Manager auf einem Microsoft Windows-Client-Computer, um eine Verbindung zum Host herzustellen.
- Linux Kernel-based Virtual Machine (KVM) — Eine kostenlose Open-Source-Virtualisierungstechnologie. KVM ist in allen Versionen von Linux Version 2.6.20 und neuer enthalten. Storage Gateway wurde für die Distributionen CentOS/RHEL 7.7, Ubuntu 16.04 LTS und Ubuntu 18.04 LTS getestet und unterstützt. Jede andere moderne Linux-Verteilung kann funktionieren, aber weder Funktion noch Leistung werden garantiert. Wir empfehlen diese Option, wenn Sie bereits über eine KVM-Umgebung verfügen und bereits mit der Funktionsweise von KVM vertraut sind. In der mitgelieferten Datei aws-storage-gateway.xml finden Sie empfohlene Startkonfigurationen. Der UEFI-Startmodus mit deaktiviertem Secure Boot (loader_secure=no) ist für File Gateway 2.x, Volume Gateway 3.x und Tape Gateway 3.x erforderlich.

- Nutanix AHV (Acropolis Hypervisor) ab Version 10.0.1.1 — Eine Virtualisierungsplattform, die in die Nutanix Hyper-Converged Infrastructure (HCI) -Lösung integriert ist. KVM-based
- Amazon-EC2-Instance: Storage Gateway stellt ein Amazon Machine Image (AMI) mit dem Abbild der Gateway-VM bereit. In Amazon EC2 können ausschließlich Gateways vom Typ File Gateway, Gateway für zwischengespeicherte Volumes oder Tape Gateway bereitgestellt werden. Weitere Informationen zur Bereitstellung von Gateways in Amazon EC2 finden Sie unter Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume 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**
>
> Die Wiederherstellung eines Gateways von einer VM, die aus einem Snapshot oder Klon einer anderen Gateway-VM oder aus Ihrem Amazon-EC2-Computerabbild (AMI) erstellt wurde, wird von Storage Gateway nicht unterstützt. Wenn Ihre Gateway-VM nicht funktioniert, aktivieren Sie ein neues Gateway und stellen Sie Ihre Daten zu diesem Gateway wieder her. Weitere Informationen finden Sie unter Wiederherstellung nach dem unerwarteten Herunterfahren einer virtuellen Maschine.
>
> Dynamischer Speicher und virtuelle Speicherballonierung werden von Storage Gateway nicht unterstützt.

Unterstützte iSCSI-Initiatoren

Wenn Sie ein Volume Gateway für zwischengespeicherte oder gespeicherte Volumes bereitstellen, können Sie iSCSI-Speicher-Volumes auf Ihrem Gateway erstellen.

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

- Microsoft Windows Server 2022
- RedHat Enterprise Linux 8
- RedHat Enterprise Linux 9
- VNware ESX-Initiator (als Alternative zu den Initiatoren in den Gastbetriebssystemen Ihrer VMs)

Important

Storage Gateway unterstützt Microsoft Multipath I/O (MPIO) von Windows-Clients nicht. 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 können Sie jedoch nicht mehrere Hosts mit demselben Volume verbinden (z. B. wenn Sie ein NTFS/ext4 Dateisystem gemeinsam nutzen, das nicht gruppiert ist).

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 Erstellen eines Volume Gateways.

   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).

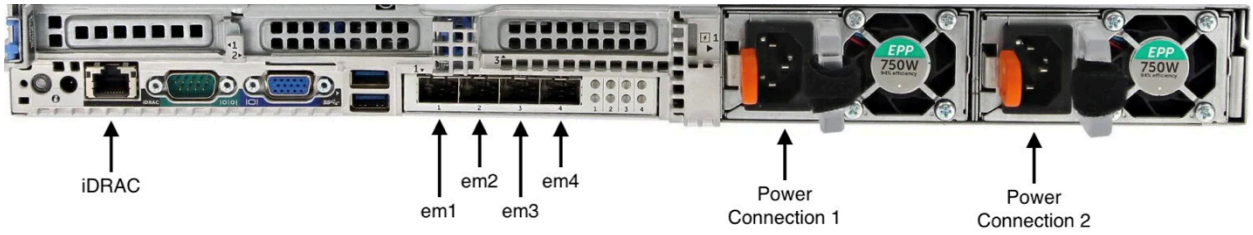
> **Note**
>
> Stellen Sie vor Ausführung der folgenden Schritte sicher, dass Sie alle Anforderungen für die Storage-Gateway-Hardware-Appliance erfüllen wie in Netzwerk- und Firewall-Anforderungen für das Storage-Gateway-Hardwaregerät beschrieben.

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.



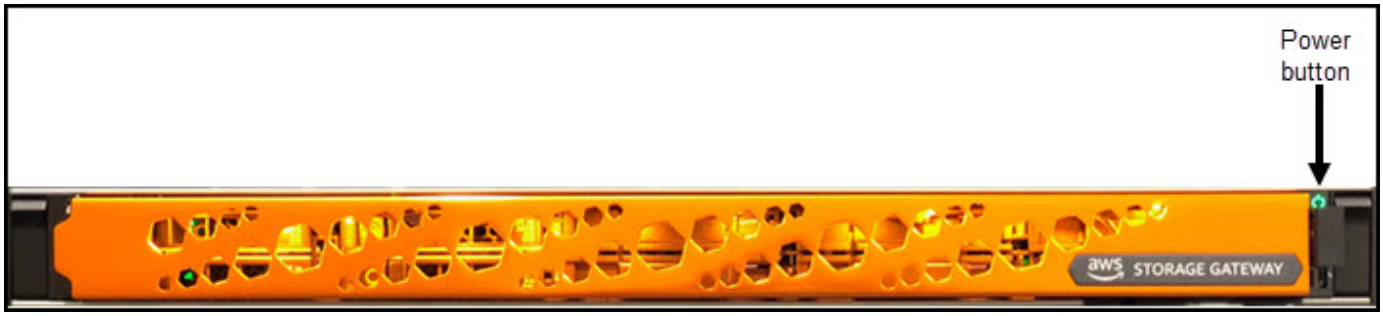
Hardware-Gerät auf einer Rückseite mit Netzwerk- und Stromanschlussetiketten.

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

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

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

Nächster Schritt

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

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

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

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

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

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

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

   > **Note**
   >
   > Wir empfehlen, das Standardpasswort zu ändern, indem Sie im Hauptmenü AWS Geräteaktivierung – Konfiguration die entsprechende Zahl für die Gateway-Konsole eingeben und dann den Befehl `passwd` ausführen. Weitere Informationen zum Ausführen des Befehls finden Sie unter 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 Einstellen des Kennworts für die lokale Konsole von der Storage Gateway Gateway-Konsole aus.

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

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

- Informationen zur Lizenz
- Eingabeaufforderung

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

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

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

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

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

So verlassen Sie die lokale Konsole des Gateways

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

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

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

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 gehosteten Gateway zu beheben.

So löschen Sie Ihre Hardware-Appliance

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

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

Erstellen Sie Ihr Gateway

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

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

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

Überblick – Gateway-Aktivierung

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 Amazon EC2 EC2-Instance in Ihrer AWS Cloud-Umgebung. Wenn Sie die Gateway-Appliance bereitstellen, weisen Sie lokalen physischen Festplattenspeicher auf dem Virtualisierungshost zu.

Verbinden mit AWS

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

Überprüfen und aktivieren

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

Überblick – Gateway-Konfiguration

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

Überblick – Speicherressourcen

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

Erstellen eines Volume Gateways

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

Themen

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

Einrichten eines Volume Gateways

Einrichten eines neuen Volume Gateways

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

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

    b. Wählen Sie Gateway-Zeitzone die lokale Zeitzone für den Teil der Welt aus, in dem Sie Ihr Gateway einsetzen möchten.
4. Wählen Sie im Abschnitt Gateway-Optionen für Gateway-Typ die Option Volume Gateway und dann den Volume-Typ aus, den Ihr Gateway verwenden soll. Sie können aus den folgenden Optionen wählen:

    - Zwischengespeicherte Volumes – Speichert Ihre Primärdaten in Amazon S3 und behält häufig aufgerufene Daten lokal im Cache für einen schnelleren Zugriff.
    - Gespeicherte Volumes – Speichert alle Ihre Daten lokal und sichert sie gleichzeitig asynchron auf Amazon S3. Gateways, die diesen Volume-Typ verwenden, können nicht auf Amazon EC2 bereitgestellt werden.
5. Gehen Sie im Abschnitt Plattform-Optionen wie folgt vor:

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

   - VMware ESXi- Laden Sie die virtuelle Gateway-Maschine herunter, stellen Sie sie bereit und konfigurieren Sie sie mithilfe von VMware ESXi.
   - Microsoft Hyper-V – Laden Sie die virtuelle Gateway-Maschine mit Microsoft Hyper-V herunter, stellen Sie sie bereit und konfigurieren Sie sie.
   - Linux KVM – Laden Sie die virtuelle Gateway-Maschine mit Linux KVM herunter, stellen Sie sie bereit und konfigurieren Sie sie. In der mitgelieferten aws-storage-gateway .xml-Datei finden Sie empfohlene Startkonfigurationen. Der UEFI-Startmodus mit deaktiviertem Secure Boot (loader_secure=no) ist für File Gateway 2.x, Volume Gateway 3.x und Tape Gateway 3.x erforderlich.
   - Amazon EC2 – Konfigurieren und starten Sie eine Amazon-EC2-Instance zum Hosten Ihres Gateways. Diese Option ist für Gateways für gespeicherte Volumes nicht verfügbar.
   - Hardware-Appliance — Bestellen Sie eine dedizierte physische Hardware-Appliance, die Ihr Gateway hostet. AWS

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

6. Wählen Sie Weiter aus, um fortzufahren.

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

Connect Ihr Volume Gateway mit AWS

Um ein neues Volume Gateway zu verbinden AWS

1. Führen Sie das unter Einrichten eines Volume-Gateways beschriebene Verfahren aus, falls Sie dies noch nicht getan haben. Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Verbinden mit AWS in der Storage-Gateway-Konsole zu öffnen.

2. Wählen Sie im Abschnitt Endpunktoptionen für Service-Endpunkt den Endpunkttyp aus, mit dem Ihr Gateway kommunizieren soll AWS. Sie können aus den folgenden Optionen wählen:

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

3. Wählen Sie im Abschnitt Gateway-Verbindungsoptionen unter Verbindungsoptionen aus, wie Sie Ihr Gateway gegenüber AWS identifizieren möchten. Sie können aus den folgenden Optionen wählen:

   - IP-Adresse – Geben Sie die IP-Adresse Ihres Gateways in das entsprechende Feld ein. Diese IP-Adresse muss öffentlich sein oder von Ihrem aktuellen Netzwerk aus zugänglich sein, und Sie müssen in der Lage sein, über Ihren Webbrowser eine Verbindung zu ihr herzustellen.

     Sie können die Gateway-IP-Adresse abrufen, indem Sie sich von Ihrem Hypervisor-Client aus bei der lokalen Konsole des Gateways anmelden oder sie von Ihrer Amazon-EC2-Instance-Detailseite kopieren.

   - Aktivierungsschlüssel – Geben Sie den Aktivierungsschlüssel für Ihr Gateway in das entsprechende Feld ein. Sie können einen Aktivierungsschlüssel mithilfe der lokalen Konsole des Gateways generieren. 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 Volume Gateways.

Überprüfen von Einstellungen und Aktivieren Ihres Volume Gateways

So aktivieren Sie ein neues Volume Gateway

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

   - Einrichten eines Volume Gateways
   - Connect Ihr Volume 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 erstellt wurde.

4. Wählen Sie Gateway aktivieren, um fortzufahren.

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

Konfigurieren Ihres Volume Gateways

So führen Sie die Erstkonfiguration auf einem neuen Volume Gateway durch

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

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

   Wenn Sie fertig sind, wählen Sie Weiter, um die Seite Gateway konfigurieren in der Storage-Gateway-Konsole zu öffnen.
2. Verwenden Sie im Abschnitt Speicher konfigurieren die Dropdownmenüs, um mindestens eine Festplatte mit mindestens 165 GiB Kapazität für CACHE STORAGE und mindestens eine Festplatte mit mindestens 150 GiB Kapazität für UPLOAD BUFFER zuzuweisen. Die in diesem Abschnitt aufgeführten lokalen Festplatten entsprechen dem physischen Speicher, den Sie auf Ihrer Hostplattform bereitgestellt haben.
3. Wählen Sie im Abschnitt CloudWatch Protokollgruppe aus, wie Amazon CloudWatch Logs eingerichtet werden soll, um den Zustand Ihres Gateways zu überwachen. Sie können aus den folgenden Optionen wählen:

   - Eine neue Protokollgruppe erstellen – Richten Sie eine neue Protokollgruppe ein, um Ihr Gateway zu überwachen.
   - Eine bestehende Protokollgruppe verwenden – Wählen Sie eine bestehende Protokollgruppe aus 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 wählen:

   - Empfohlene Alarme für 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 ein Volume erstellen, damit es verwendet werden kann. Detaillierte Anweisungen finden Sie unter Erstellen eines Volumes.

Ein Speichervolume erstellen

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

> **Note**
>
> Sie können AWS Key Management Service (AWS KMS) verwenden, um Daten zu verschlüsseln, die auf ein zwischengespeichertes Volume geschrieben wurden, das in Amazon S3 gespeichert ist. Derzeit können Sie dies mithilfe der AWS Storage Gateway - API-Referenz durchführen. Für weitere Informationen siehe CreateCachediSCSIVolume oder create-cached-iscsi-volume.

So erstellen Sie ein Volume

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

   Wählen Sie für gespeicherte Volumes einen Wert für Disk ID (Datenträger-ID) aus der Liste aus.
5. Welche Optionen für Volume-Inhalt verfügbar sind, hängt vom Typ des Gateways ab, für den Sie das Volume erstellen.

   Für zwischengespeicherte Volumes haben Sie die folgenden Optionen:

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

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

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

   Für gespeicherte Volumes haben Sie die folgenden Optionen:

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

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

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

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

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

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

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

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

   Anschließend wird das Dialogfeld CHAP-Authentifizierung konfigurieren geöffnet. Sie können an dieser Stelle das Challenge-Handshake Authentication Protocol (CHAP) für Ihr Volume konfigurieren oder Abbrechen auswählen und CHAP später konfigurieren. Weitere Informationen

zur CHAP-Einrichtung finden Sie unter Konfigurieren der CHAP-Authentifizierung für Ihre Volumes.

Wenn Sie CHAP nicht konfigurieren möchten, beginnen Sie mit der Verwendung Ihres Volumes. Weitere Informationen finden Sie unter Verbinden Sie Ihre Volumes mit Ihrem Client.

Konfigurieren der CHAP-Authentifizierung für Ihre Volumes

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

So konfigurieren Sie CHAP

1. Wählen Sie das Volume aus, für das Sie CHAP konfigurieren möchten.
2. Klicken Sie im Menü Aktionen auf CHAP-Authentifizierung konfigurieren.
3. Geben Sie unter Initiatorname den Namen Ihres Initiators ein.
4. Geben Sie unter Initiatorgeheimnis den geheimen Begriff ein, den Sie zum Authentifizieren Ihres iSCSI-Initiators verwendet haben.
5. Geben Sie unter Zielgeheimnis den geheimen Begriff ein, den Sie zum Authentifizieren Ihres Ziels für die gegenseitige CHAP-Authentifizierung verwendet haben.
6. Wählen Sie Speichern aus, um Ihre Einträge zu speichern.

   Weitere Informationen zum Einrichten der CHAP-Authentifizierung finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.

Nächster Schritt

Verbinden Sie Ihre Volumes mit Ihrem Client

Verbinden Sie Ihre Volumes mit Ihrem Client

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

> **Important**
>
> Mit Storage Gateway können mehrere Hosts mit demselben Volume verbunden werden, wenn die Hosts den Zugriff über Windows Server Failover Clustering (WSFC) koordinieren. Ohne WSFC ist es nicht möglich, mehrere Hosts mit dem gleichen Volume zu verbinden (z. B. durch Freigabe eines nicht geclusterten NTFS/ext4-Dateisystems).

Themen

- Verbindung zu einem Microsoft Windows-Client herstellen
- Verbindung zu einem Red Hat Enterprise Linux Client herstellen

Verbindung zu einem Microsoft Windows-Client herstellen

Das folgende Verfahren zeigt eine Zusammenfassung der Schritte, die Sie zum Verbinden mit einem Windows-Client ausführen. Weitere Informationen finden Sie unter Verbinden von iSCSI-Initiatoren.

So stellen Sie eine Verbindung mit einem Windows-Client her

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

Verbindung zu einem Red Hat Enterprise Linux Client herstellen

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

So verbinden Sie einen Linux-Client mit iSCSI-Zielen

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

   Verwenden Sie den folgenden Befehl zum Installieren des Pakets.

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

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

   Verwenden Sie unter RHEL 5 oder 6 den folgenden Befehl.

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

   Verwenden Sie für RHEL 7, 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 sollte der folgenden Beispielausgabe gleichen.

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

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

4. Stellen Sie eine Verbindung mit einem Ziel her.

   Stellen Sie sicher, dass Sie im Verbindungsbefehl 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
```

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

Volume initialisieren und formatieren

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

Themen

- Initialisieren und Formatieren Ihres Volumes unter Microsoft Windows
- Initialisierung und Formatierung Ihres Volumes auf Red Hat Enterprise Linux

Initialisieren und Formatieren Ihres Volumes unter Microsoft Windows

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

So initialisieren und formatieren Sie Ihr Speicher-Volume

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

Partitionsstil	Unter folgenden Bedingungen verwenden
MBR (Master Boot Record, Master-Bootdatensatz)	• Wenn Ihr Gateway ein gespeichertes Volume ist und das Speicher-Volume auf eine Größe von 1 TiB begrenzt ist. • Wenn Ihr Gateway ein zwischengespeichertes Volume ist und das Speicher-Volume eine Größe von weniger als 2 TiB aufweist.
GPT (GUID Partition Table, GUID-Partitionstabelle)	Wenn das Speicher-Volume des Gateways eine Größe von 2 TiB oder mehr aufweist.

3. Erstellen Sie ein einfaches Volumes:

   a. Schalten Sie das Volume online, um es zu initialisieren. Alle verfügbaren Volumes werden in der Disk Management-Konsole angezeigt.

   b. Öffnen Sie das Kontextmenü (Rechtsklick) für den Datenträger und wählen Sie dann New Simple Volume (Neues einfaches Volume) aus.

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

   c. Geben Sie die maximale Festplattengröße an.

   d. Weisen Sie dem Volume einen Laufwerksbuchstaben oder -pfad zu und formatieren Sie das Volume durch Auswählen von Perform a quick format (Schnellformatierung ausführen).

   > **Important**
   >
   > Es wird nachdrücklich empfohlen, für zwischengespeicherte Volumes Perform a quick format (Schnellformatierung ausführen) auszuwählen. Dies führt zu weniger E/A-Initialisierung, einer kleineren anfänglichen Snapshot-Größe und der

schnellstmöglichen Herstellung eines betriebsfähigen Volumes. Gleichzeitig wird eine Cached-Volume-Nutzung für die vollständige Formatierung verhindert.

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

Initialisierung und Formatierung Ihres Volumes auf Red Hat Enterprise Linux

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

So initialisieren und formatieren Sie Ihr Speicher-Volume

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

   ```
   $ lsblk
   ```

   Ein Fehler wegen nicht erkannter Volume-Bezeichnung für das neue unpartitionierte Volume wird angezeigt.
4. Initialisieren Sie das neue Volume. Wenn Sie den Partitionsstil auswählen, sollten Sie den Typ und die Größe des Volumes berücksichtigen, mit dem Sie eine Verbindung herstellen – Cached oder Stored. Dies wird in der folgenden Tabelle gezeigt.

Partitionsstil	Unter folgenden Bedingungen verwenden
MBR (Master Boot Record, Master-Bootdatensatz)	• Wenn Ihr Gateway ein gespeichertes Volume ist und das Speicher-Volume auf eine Größe von 1 TiB begrenzt ist.

Partitionsstil	Unter folgenden Bedingungen verwenden
	• Wenn Ihr Gateway ein zwischengespeichertes Volume ist und das Speicher-Volume eine Größe von weniger als 2 TiB aufweist.
GPT (GUID Partition Table, GUID-Partitionstabelle)	Wenn das Speicher-Volume des Gateways eine Größe von 2 TiB oder mehr aufweist.

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

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

5. Erstellen Sie mit dem folgenden Befehl eine Partition.

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

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

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

7. Mounten Sie das Dateisystem mit dem folgenden Befehl.

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

Testen Sie Ihr Gateway

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

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

Sie überprüfen das Setup für ein Gateway, indem Sie ein Snapshot-Backup Ihres Volumes erstellen und den Snapshot darin speichern AWS. Sie stellen dann den Snapshot auf einem neuen Volume

wieder her. Ihr Gateway kopiert die Daten aus dem angegebenen Snapshot AWS auf das neue Volume.

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

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

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

   Die kopierte Datenmenge ist unerheblich, für diese Demonstration. Eine kleine Datei ist ausreichend für die Demonstration des Wiederherstellungsprozesses.
2. Wählen Sie im Navigationsbereich der Storage-Gateway-Konsole Sie Option Volumes aus.
3. Wählen Sie den Speicher-Volume aus, den Sie für das Gateway erstellt haben.

   Dieses Gateway sollte nur ein Speicher-Volume enthalten. Wenn Sie das Volume auswählen, werden die zugehörigen Eigenschaften angezeigt.
4. Wählen Sie unter Actions (Aktionen) die Option Create EBS Snapshot (EBS-Snapshot erstellen) aus, um einen Snapshot des Volumes zu erstellen.

   Abhängig von der Menge der Daten auf dem Datenträger und die Upload-Bandbreite, kann es einige Sekunden dauern bis der Snapshot erstellt ist. Beachten Sie die Volume-ID für das Volume, von dem Sie einen Snapshot erstellen. Sie verwenden die Snapshot-ID, um den Snapshot zu finden.
5. Geben Sie im Dialogfeld Create EBS Snapshot (EBS-Snapshot erstellen) eine Beschreibung für Ihren Snapshot ein.
6. (Optional) Geben Sie unter Tags einen Schlüssel und Wert ein, um Tags zum Snapshot hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar mit Unterscheidung von Groß- und Kleinschreibung, das Ihnen das Verwalten, Filtern und Suchen Ihrer Snapshots erleichtert.
7. Wählen Sie Create Snapshot (Snapshot erstellen) aus. Ihre Snapshot ist als Amazon EBS-Snapshot gespeichert. Notieren Sie sich Ihre Snapshot-ID. Die Anzahl der Snapshots, die für Ihr Volume erstellt wurde, wird in der Snapshot-Spalte anzeigt.

8. Wählen Sie in der Spalte EBS-Snapshots den Link für das Volume aus, für das Sie den Snapshot erstellt haben, um Ihren EBS-Snapshot auf der Amazon-Konsole zu sehen. EC2

So stellen Sie einen Snapshot auf einem anderen Volume wieder her

Siehe Ein Speichervolume erstellen.

Sicherung Ihrer Volumes

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

Themen

- Verwenden von Storage Gateway zum Sichern Ihrer Volumes
- Wird AWS Backup zur Sicherung Ihrer Volumes verwendet

Verwenden von Storage Gateway zum Sichern Ihrer Volumes

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

- Testen Sie Ihr Gateway
- Einen Wiederherstellungs-Snapshot erstellen
- Klonen eines zwischengespeicherten Volumes von einem Recovery Point

Wird AWS Backup zur Sicherung Ihrer Volumes verwendet

AWS Backup ist ein zentralisierter Backup-Service, der es Ihnen einfach und kostengünstig macht, Ihre Anwendungsdaten AWS dienstübergreifend sowohl in der Amazon Web Services Cloud als

auch vor Ort zu sichern. Auf diese Weise können Sie Ihre geschäftlichen und behördlichen Backup-Compliance-Anforderungen erfüllen. AWS Backup macht den Schutz Ihrer AWS Speichervolumes, Datenbanken und Dateisysteme einfach, indem ein zentraler Ort bereitgestellt wird, an dem Sie Folgendes tun können:

- Konfigurieren und prüfen Sie die AWS Ressourcen, die Sie sichern möchten.
- Automatisieren geplanter Sicherungen
- Festlegen von Aufbewahrungsrichtlinien
- Überwachen der letzten Sicherungs- und Wiederherstellungsaktivitäten

Da Storage Gateway integriert ist AWS Backup, können Kunden damit lokale Geschäftsanwendungen sichern, die Storage Gateway Gateway-Volumes für Cloud-gestützten Speicher verwenden. AWS Backup AWS Backup unterstützt die Sicherung und Wiederherstellung von zwischengespeicherten und gespeicherten Volumes. Informationen zu AWS Backup finden Sie in der AWS Backup Dokumentation. Weitere Informationen zu AWS Backup finden Sie unter Was ist AWS Backup? im AWS Backup Benutzerhandbuch.

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

Storage Gateway Gateway-Volume-Backups, von AWS Backup denen sie stammen, werden in Amazon S3 als Amazon EBS-Snapshots gespeichert. Sie können die Storage Gateway Gateway-Volume-Backups von der AWS Backup Konsole oder der Amazon EBS-Konsole aus sehen.

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

Vorteile der Verwendung AWS Backup zur Sicherung von Storage Gateway Gateway-Volumes

Die Vorteile der Sicherung von Storage Gateway Gateway-Volumes bestehen darin, dass Sie Compliance-Anforderungen erfüllen, betriebliche Belastungen vermeiden und das Backup-Management zentralisieren können. AWS Backup AWS Backup ermöglicht Ihnen Folgendes:

- Festlegen anpassbarer geplanter Sicherungsrichtlinien, die Ihre Sicherungsanforderungen erfüllen
- Legen Sie Regeln für die Aufbewahrung und den Ablauf von Backups fest, sodass Sie keine benutzerdefinierten Skripts mehr entwickeln oder die point-in-time Backups Ihrer Volumes manuell verwalten müssen.
- Verwalten und überwachen Sie Backups über mehrere Gateways und andere AWS Ressourcen hinweg von einer zentralen Ansicht aus.

Wird verwendet, AWS Backup um Backups Ihrer Volumes zu erstellen

> **Note**
>
> AWS Backup erfordert, dass Sie eine AWS Identity and Access Management (IAM-) Rolle wählen, die AWS Backup verbraucht. Sie müssen diese Rolle erstellen, da sie AWS Backup nicht für Sie erstellt wird. Sie müssen auch eine Vertrauensbeziehung zwischen AWS Backup und dieser IAM-Rolle einrichten. Weitere Informationen dazu finden Sie im AWS Backup -Benutzerhandbuch. Weitere Informationen dazu finden Sie unter Erstellen eines Sicherungsplans im AWS Backup -Benutzerhandbuch.

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

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

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

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

Suchen und Wiederherstellen Ihrer Volumes von AWS Backup

Sie können Ihre Backup-Storage Gateway-Volumes von der AWS Backup Konsole aus suchen und wiederherstellen. Weitere Informationen finden Sie im AWS Backup -Benutzerhandbuch. Weitere Informationen finden Sie unter Wiederherstellungspunkte im AWS Backup -Benutzerhandbuch.

So finden Sie Ihre Volumes und stellen sie wieder her

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

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

Wie geht es weiter?

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

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

- Wenn Sie Ihr Gateway weiter nutzen möchten, sollten Sie die Informationen über die bessere Dimensionierung des Upload-Puffers für reale Workloads lesen. Weitere Informationen finden Sie unter Bestimmen der Größe des Volume-Gateway-Speichers für reale Workloads.

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

- Weitere Informationen zu Speicher-Volumes und deren Verwaltung finden Sie unter Verwalten Ihres Volume Gateways.
- Wenn Sie Ihr Gateway nicht weiter nutzen möchten, sollten Sie das Gateway löschen, um anfallende Gebühren zu vermeiden. Weitere Informationen finden Sie unter Säuberung unnötiger Ressourcen.
- Informationen zum Beheben von Gateway-Problemen finden Sie unter Fehlerbehebung bei Ihrem Gateway.
- Informationen zum Optimieren Ihres Gateways finden Sie unter Optimierung der Gateway-Leistung.
- Informationen zu Storage-Gateway-Metriken und dazu, wie Sie die Leistung Ihres Gateways überwachen können, finden Sie unter Überwachen von Storage Gateway.
- Weitere Informationen zum Konfigurieren der iSCSI-Ziele Ihres Gateways zum Speichern von Daten finden Sie unter Von einem Windows-Client aus eine Verbindung zu Ihren Volumes herstellen.

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

Bestimmen der Größe des Volume-Gateway-Speichers für reale Workloads

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

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

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

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

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

  Die Upload-Puffer-Formel berücksichtigt den Unterschied zwischen dem Durchsatz von Ihrer Anwendung zu Ihrem Gateway und dem Durchsatz von Ihrem Gateway zu AWS, multipliziert mit der Dauer, mit der Sie voraussichtlich Daten schreiben werden. Beispiel: Ihre Anwendungen schreiben Textdaten mit einer Rate von 40 MB pro Sekunde während 12 Stunden täglich an das Gateway und der Netzwerkdurchsatz beträgt 12 MB pro Sekunde. Bei einem Komprimierungsfaktor von 2:1 für die Textdaten gibt die Formel an, dass Sie etwa 675 GiB Upload-Puffer-Speicherplatz zuweisen müssen.

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

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

  Die Upload-Pufferformel berücksichtigt den Unterschied zwischen dem Durchsatz von Ihrer Anwendung zu Ihrem Gateway und dem Durchsatz von Ihrem Gateway zu AWS, multipliziert mit der Dauer, mit der Sie voraussichtlich Daten schreiben werden. Beispiel: Ihre Anwendungen schreiben Textdaten mit einer Rate von 40 MB pro Sekunde während 12 Stunden täglich an das Gateway und der Netzwerkdurchsatz beträgt 12 MB pro Sekunde. Bei einem Komprimierungsfaktor von 2:1 für die Textdaten gibt die Formel an, dass Sie etwa 675 GiB Upload-Puffer-Speicherplatz zuweisen müssen.

So überwachen Sie den Upload-Puffer

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

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

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 Ihrem Volume 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-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpoints (Endpunkte) und anschließend Create Endpoint (Endpunkt erstellen) aus.
3. Wählen Sie auf der Seite Endpunkt erstellen die Option AWS -Services in Servicekategorie aus.
4. Wählen Sie für Servicename `com.amazonaws.region.storagegateway` aus. Zum Beispiel `com.amazonaws.us-east-2.storagegateway`.
5. Wählen Sie in VPC (VPC) Ihre VPC aus und notieren Sie ihre Availability Zones und Subnetze.
6. Stellen Sie sicher, dass Enable Private DNS Name (Privaten DNS-Namen aktivieren) ausgewählt ist.
7. Wählen Sie in Security group (Sicherheitsgruppe) die Sicherheitsgruppe aus, die Sie für Ihre VPC verwenden möchten. Sie können die Standardsicherheitsgruppe akzeptieren. Stellen Sie sicher, dass alle der folgenden TCP-Ports in Ihrer Sicherheitsgruppe zulässig sind:
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028

- TCP 1031
- TCP 2222

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

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

Verwalten Ihres Volume Gateways

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

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

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

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

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

Im Folgenden finden Sie Informationen zur Verwaltung Ihrer Volume Gateway .

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.
- Volumen hinzufügen und erweitern- Erfahren Sie, wie Sie Ihrem Gateway weitere Volumes hinzufügen oder die Größe vorhandener Volumes erweitern können, wenn Ihre Anwendungsanforderungen steigen.
- Klonen eines zwischengespeicherten Volumes von einem Recovery Point- Erfahren Sie, wie Sie anhand des Wiederherstellungspunkts eines vorhandenen Volumes ein neues Volume erstellen. Dabei handelt es sich um einen gespeicherten Zeitpunkt, zu dem alle Daten auf dem Volume konsistent sind.
- Volumenverbrauch anzeigen- Erfahren Sie, wie Sie die auf einem Volume gespeicherte Datenmenge mithilfe der Storage Gateway Gateway-Konsole anzeigen können.
- Löschen von Speichervolumes- Erfahren Sie, wie Sie ein Volume löschen, wenn Ihre Anwendung geändert werden muss, z. B. wenn Sie eine Anwendung migrieren, um ein größeres Speichervolume zu verwenden.
- Verschieben Ihrer Volumes zu einem anderen Gateway- Erfahren Sie, wie Sie Volumes trennen und wieder anhängen. Dies ist nützlich, wenn Sie Ihre Volumes auf ein anderes Volume Gateway verschieben müssen, wenn sich Ihre Leistungsanforderungen ändern.
- Einen Wiederherstellungs-Snapshot erstellen- Erfahren Sie, wie Sie einen Wiederherstellungs-Snapshot von einem Volume-Wiederherstellungspunkt für ein Gateway erstellen und wo Sie diesen Snapshot in der Storage Gateway Gateway-Konsole finden, nachdem Sie ihn erstellt haben.
- Einen Snapshot-Zeitplan bearbeiten- Erfahren Sie, wie Sie einen Snapshot-Zeitplan anpassen können, indem Sie entweder die Uhrzeit ändern, zu der der Snapshot an jedem Tag erstellt wird, oder die Häufigkeit, mit der Snapshots erstellt werden.
- Löschen von Snapshots Ihrer Speichervolumes- Erfahren Sie, wie Sie unnötige Snapshots löschen, wenn Sie sie nicht mehr benötigen.
- Grundlagen zu Status und Übergängen bei Volumes- Erfahren Sie mehr über die verschiedenen Volume-Statuswerte, die Storage Gateway meldet, um festzustellen, ob ein Volume normal funktioniert oder ob ein Problem vorliegt, das möglicherweise Maßnahmen Ihrerseits erfordert.
- Verschieben Ihrer Daten auf eine neue Gateway-Instanz- 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.

Volumen hinzufügen und erweitern

Wenn Ihre Anwendungsanforderungen steigen, müssen Sie möglicherweise weitere Volumes zu Ihrem Gateway hinzufügen oder die Größe vorhandener Volumes erweitern. Wenn Sie Volumes hinzufügen oder erweitern, müssen Sie die Größe des Cache-Speichers und des Upload-Puffers berücksichtigen, den Sie dem Gateway zugewiesen haben. Das Gateway muss über genügend Puffer und Cache-Speicherplatz für neue Volumes verfügen. Weitere Informationen finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.

Sie können Volumes mithilfe der Storage-Gateway-Konsole oder der Storage-Gateway-API hinzufügen. Informationen zum Hinzufügen von Volumes mithilfe der Storage-Gateway-Konsole finden Sie unter Ein Speichervolume erstellen. Informationen zur Verwendung der Storage Gateway Gateway-API zum Hinzufügen von Volumes finden Sie unter CreateCachediSCSIVolume.

Sie können die Größe vorhandener Volumes mit einer der folgenden Methoden erweitern:

- Erstellen Sie einen Snapshot der Volume, die Sie erweitern möchten und verwenden Sie dann diesen Snapshot um eine größere Volume zu erstellen. Weitere Informationen, wie Sie einen Snapshot erstellen, finden Sie unter Einen Wiederherstellungs-Snapshot erstellen. Weitere Informationen, wie Sie einen Snapshot verwenden um eine neue Volume zu erstellen, finden Sie unter Ein Speichervolume erstellen.
- Verwenden Sie das zwischengespeicherte Volume die Sie erweitern möchten um eine neue, größere Volume zu klonen. Weitere Informationen, wie Sie eine Volume klonen können, finden Sie unter Klonen eines zwischengespeicherten Volumes von einem Recovery Point. Weitere Informationen, wie Sie eine Volume erstellen können, finden Sie unter Ein Speichervolume erstellen.

Klonen eines zwischengespeicherten Volumes von einem Recovery Point

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

Das Klonen eines Volumes ist schneller und kostengünstiger als das Erstellen eines Amazon EBS-Snapshots. Beim Klonen wird eine byte-to-byte Kopie Ihrer Daten vom Quell-Volume auf das neue Volume erstellt. Dabei wird der neueste Wiederherstellungspunkt des Quell-Volumes verwendet. Storage Gateway erstellt automatisch Wiederherstellungspunkte für Ihre zwischengespeicherten Volumes. Um zu sehen, wann der letzte Wiederherstellungspunkt erstellt wurde, überprüfen Sie die `TimeSinceLastRecoveryPoint` Metrik in Amazon CloudWatch.

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

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

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

Das Klonen und die Verwendung von einem unerreichbarem Gateway aus.

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie in der Storage-Gateway-Konsole Volume erstellen aus.

3. Wählen Sie im Dialogfeld Create volume (Volume erstellen) einen Gateway für Gateway (Gateway) aus.
4. Geben Sie unter Capacity (Kapazität) die Kapazität für das Volume ein. Die Kapazität muss mindestens dieselbe Größe wie die Quell-Volume sein.
5. Wählen Sie Clone from last recovery point (Klonen vom letzten Wiederherstellungspunkt) und wählen Sie eine Volume-ID für Source volume (Quell-Volume) aus. Das Quellvolume kann ein beliebiges zwischengespeichertes Volume in der ausgewählten AWS Region sein.
6. Geben Sie in iSCSI target name iSCSI-Zielname) einen Namen ein.

   Der Zielname kann Kleinbuchstaben, Zahlen, Punkte (.) und Bindestriche (-) enthalten. iSCSI target nodeDieser Zielname wird als der Name des iSCSI target node (iSCSI-Zielknoten) auf der Registerkarte Targets (Ziele) in der Benutzeroberfläche von iSCSI Microsoft Initiator angezeigt. Beispielsweise wird der Name `target1` als `iqn.1007-05.com.amazon:target1` angezeigt. Stellen Sie sicher, dass der Zielname global innerhalb Ihres Storage Area Network (SAN) eindeutig ist.
7. Überprüfen Sie, dass für die Einstellung zu Network interface (Netzwerkschnittstelle) die IP-Adresse des Gateways ausgewählt ist, oder wählen Sie eine IP-Adresse für Network interface (Netzwerkschnittstelle).

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

   Wenn die Gateway-VM für mehr als einen Netzwerkadapter konfiguriert ist, zeigt das Dialogfeld Create volume (Volume erstellen) eine Liste für Network interface (Netzwerkschnittstelle) an. In dieser Liste wird für jeden für die Gateway-VM konfigurierten Adapter eine IP-Adresse angezeigt. Wenn die Gateway-VM für nur einen Netzwerkadapter konfiguriert ist, wird keine Liste angezeigt, weil nur eine IP-Adresse existiert.
8. Wählen Sie Create Volume (Volume erstellen) aus. Anschließend wird das Dialogfeld CHAP-Authentifizierung konfigurieren geöffnet. Sie können Ihre CHAP später konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.

Der nächste Schritt ist Ihr Volume mit Ihrem Client zu verbinden. Weitere Informationen finden Sie unter Verbinden Sie Ihre Volumes mit Ihrem Client.

Volumenverbrauch anzeigen

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

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

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Volumes und wählen Sie das gewünschte Volume.
3. Wählen Sie die Registerkarte Details.

   Die folgenden Felder enthalten Informationen über das Volume:

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

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

Löschen von Speichervolumes

Möglicherweise müssen Sie ein Volume löschen, da an Ihrer Anwendung Änderungen vorgenommen werden müssen, z. B. wenn Sie Ihre Anwendung migrieren möchten, um ein größeres Storage Volume verwenden zu können. Bevor Sie diese Volume löschen, stellen Sie sicher, dass derzeit keine Anwendungen auf die Gateway-Volumes schreiben. Stellen Sie darüber hinaus sicher, dass sich keine Snapshots in Bearbeitung für das Volume befinden. Wenn ein Snapshot-Zeitplan für das Volume definiert ist, können Sie diesen auf der Registerkarte Snapshot-Zeitpläne der Storage-Gateway-Konsole überprüfen. Weitere Informationen finden Sie unter Einen Snapshot-Zeitplan bearbeiten.

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

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

So löschen Sie ein Volume

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

Verschieben Ihrer Volumes zu einem anderen Gateway

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

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

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

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

> **Note**
>
> Ein getrenntes Volume wird zum Standardsatz für Volumespeicher abgerechnet, bis Sie es löschen. Informationen dazu, wie Sie Kosten sparen können, finden Sie unter Reduzierung der Menge des fakturierten Speichers auf einem Volume.

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

Die folgenden Schritte zeigen, wie Sie ein Volume über die Storage-Gateway-Konsole trennen und anfügen. Weitere Informationen dazu, wie Sie dies mithilfe der API tun können, finden Sie unter DetachVolumeoder AttachVolumein der AWS Storage Gateway API-Referenz.

So trennen Sie ein Volume von einem Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Volumes und dann ein oder mehrere Volumes aus, die getrennt werden sollen.

3. Wählen Sie Actions (Aktionen) und Detach volume (Volume trennen) aus. Das Bestätigungsdialogfeld wird angezeigt.
4. Vergewissern Sie sich, dass Sie die angegebenen Volumes trennen möchten, geben Sie dann das Wort trennen in das Bestätigungsfeld ein und wählen Sie Trennen aus.

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

Sie können das Volume nun an ein anderes Gateway anfügen.

So fügen Sie ein Volume an ein Gateway an

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Volumes aus. Als Status der einzelnen Volumes, die getrennt wurden, wird Detached (Getrennt) angezeigt.
3. Wählen Sie aus der Liste der getrennten Volumes das Volume aus, das Sie anfügen möchten. Sie können nur jeweils ein Volume anfügen.
4. Wählen Sie unter Actions (Aktionen) die Option Attach volume (Volume anfügen) aus.
5. Wählen Sie im Dialogfeld Attach Volume (Volume anfügen) das Gateway aus, an das Sie das Volume anfügen möchten, und geben Sie dann das iSCSI-Ziel ein, mit dem das Volume verbunden werden soll.

   Geben Sie beim Anfügen eines gespeicherten Volumes die Datenträger-ID unter Disk ID (Datenträger-ID) ein.
6. Wählen Sie Attach volume (Volume anfügen) aus. Wenn ein Volume, das Sie anfügen möchten, viele Daten umfasst, geht es vom Status Detached (Getrennt) in den Status Attached (Angefügt) über, wenn die `AttachVolume`-Operation erfolgreich war.

7. Geben Sie im Assistenten zum Konfigurieren der CHAP-Authentifizierung in den Feldern Initiatorname, Initatorgeheimnis und Zielgeheimnis die entsprechenden Angaben ein und wählen Sie Speichern aus. Weitere Informationen zum Arbeiten mit der CHAP-Authentifizierung (Challenge-Handshake Authentication Protocol) finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.

Einen Wiederherstellungs-Snapshot erstellen

Das folgende Verfahren zeigt Ihnen, wie Sie einen Wiederherstellungs-Snapshot von einem Volume-Wiederherstellungspunkt für ein Gateway erstellen und wo Sie diesen Snapshot in der Storage Gateway Gateway-Konsole finden, nachdem Sie ihn erstellt haben. Sie können Wiederherstellungs-Snapshots einmalig oder ad hoc erstellen oder Sie können einen Snapshot-Zeitplan einrichten, um in regelmäßigen, von Ihnen festgelegten Intervallen wiederkehrende Snapshots des Volumes zu erstellen.

Um einen Wiederherstellungs-Snapshot eines Volumes von einem vorhandenen Gateway aus zu erstellen und zu verwenden

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich auf der linken Seite der Konsolenseite die Option Gateways aus.
3. Wählen Sie das Gateway aus, für das Sie einen Snapshot erstellen möchten, und klicken Sie dann auf die Registerkarte Details.

   Auf der Registerkarte Details wird eine Wiederherstellungs-Snapshot-Nachricht für das ausgewählte Gateway angezeigt.
4. Wählen Sie Create recovery snapshot (Wiederherstellungs-Snapshot erstellen), um das Dialogfeld Create recovery snapshot (Wiederherstellungs-Snapshot erstellen) zu öffnen.
5. Wählen Sie aus der angezeigten Liste der Volumes das Volume aus, das Sie wiederherstellen möchten, und klicken Sie dann auf Snapshots erstellen.

   Storage Gateway initiiert den Snapshot-Prozess für das angegebene Volume. Wenn der Snapshot-Vorgang abgeschlossen ist, finden Sie den Snapshot in der Spalte Snapshots, wenn Sie das Volume auf der Seite Volumes der Storage Gateway Gateway-Konsole aufrufen.

Einen Snapshot-Zeitplan bearbeiten

AWS Storage Gateway Erstellt für gespeicherte Volumes einen standardmäßigen Snapshot-Zeitplan, der einmal täglich lautet.

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

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

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

Bearbeitung eines Snapshot-Zeitplans für eine Volume

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

Löschen von Snapshots Ihrer Speichervolumes

Sie können einen Snapshot des Speichervolumes löschen. Dies kann beispielsweise sinnvoll sein, wenn Sie im Lauf der Zeit Snapshots eines Speichervolumes erstellt haben und die älteren Snapshots nicht mehr benötigen. Da es sich bei Snapshots um inkrementelle Sicherungen handelt, werden nur die Daten gelöscht, die nicht in anderen Snapshots benötigt werden, wenn Sie diese löschen.

Themen

- Löschen von Snapshots mithilfe des AWS SDK for Java
- Löschen von Snapshots mithilfe des AWS SDK for .NET
- Löschen von Snapshots mit dem AWS Tools for Windows PowerShell

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

Um mehrere Snapshots gleichzeitig zu löschen, können Sie einen davon verwenden AWS SDKs , der Storage Gateway Gateway-Operationen unterstützt. Beispiele finden Sie unter Löschen von Snapshots mithilfe des AWS SDK for Java, Löschen von Snapshots mithilfe des AWS SDK for .NET und Löschen von Snapshots mit dem AWS Tools for Windows PowerShell.

Löschen von Snapshots mithilfe des AWS SDK for Java

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

Example: Löschen von Snapshots mithilfe des AWS SDK for Java

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

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

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

public class ListDeleteVolumeSnapshotsExample {

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

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

    // The number of days back you want to save snapshots. Snapshots before this cutoff
 are deleted
```

```
   // if viewOnly = false.
   public static int daysBack = 10;

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

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

       // Create a Storage Gateway and amazon ec2 client
       sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

       sgClient.setEndpoint(serviceURLSG);

       ec2Client = new AmazonEC2Client(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
       ec2Client.setEndpoint(serviceURLEC2);

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

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

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

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

       return volumes;
```

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

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

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

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

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

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

    private static String OutputVolumeInfo(VolumeInfo vi) {
```

```
        String volumeInfo = String.format(
                "Volume Info:\n" +
                "  ARN: %s\n" +
                "  Type: %s\n",
                vi.getVolumeARN(),
                vi.getVolumeType());
        return volumeInfo;
     }

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

}
```

Löschen von Snapshots mithilfe des AWS SDK for .NET

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

Example: Löschen von Snapshots mithilfe des AWS SDK for .NET

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

Das folgende Codebeispiel verwendet das AWS SDK for .NET Version 2 und 3. Sie können ältere Versionen von .NET auf die neue Version migrieren. Weitere Informationen finden Sie unter Migrieren Ihres Projekts für das AWS SDK for .NET.

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

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

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

JSON

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

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

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

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

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

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

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

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

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

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

```
        static String SnapshotStatus = "completed";

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

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

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

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

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

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

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

```
            try
            {
                ListVolumesRequest request = new ListVolumesRequest();
                request.GatewayARN = GatewayARN;
                response = sgClient.ListVolumes(request);

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

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

                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

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

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

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

                DescribeSnapshotsResponse describeSnapshotsResponse =
                  ec2Client.DescribeSnapshots(describeSnapshotsRequest);

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

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

```
                foreach (Snapshot s in snapshots)
                {

                    DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
                    DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                    Console.WriteLine("Volume: " +
                              s.VolumeId +
                              " => Snapshot: " +
                              s.SnapshotId +
                              " Response: "
                              + response.HttpStatusCode.ToString());
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

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

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

```
    }
}
```

Löschen von Snapshots mit dem AWS Tools for Windows PowerShell

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

Example: Löschen von Schnappschüssen mit dem AWS Tools for Windows PowerShell

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

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

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

.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS Region stored in session using Initialize-AWSDefault.
    For more info see, https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html

.EXAMPLE
    powershell.exe .\SG_DeleteSnapshots.ps1
```

```
#>

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "*** provide gateway ARN ***"
$viewOnly = $true;

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

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

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

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

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

       $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
 $meetsCriteria
       if (!$viewOnly -AND $meetsCriteria)
       {
           $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
```

```
            #Can get RequestId from response for troubleshooting.
            $sb = $sb + ", deleted? yes"
        }
        else {
            $sb = $sb + ", deleted? no"
        }
        Write-Output($sb)
    }
}
```

Grundlagen zu Status und Übergängen bei Volumes

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

Themen

- Grundlagen zum Volume Status
- Grundlegendes zum Anfügestatus
- Grundlagen zu Statusübergängen bei zwischengespeicherten Volumes
- Grundlagen zu Statusübergängen bei gespeicherten Volumes

Grundlagen zum Volume Status

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

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

Status	Bedeutung
Verfügbar	Der Volume ist zur Verwendung verfügbar. Dieser Status ist der normalen Ausführungsstatus eines Volumes. Wenn eine Bootstrapping-Phase abgeschlossen ist, erhält das Volume wieder den Status Available (Verfügbar). Das bedeutet, dass das Gateway alle am Volume vorgenommenen Änderungen synchronisiert hat, seitdem es den Status Pass Through erhalten hat.
Bootstrapping	Das Gateway synchronisiert Daten lokal mit einer Kopie der in AWS gespeicherten Daten. In der Regel müssen Sie bei diesem Status keine Maßnahmen ergreifen, weil das Speichervolume den Status Available (Verfügbar) in den meisten Fällen automatisch erkennt. Die folgenden Szenarien gelten, wenn ein Volume den Status Bootstrap ping besitzt: • Ein Gateway ist unerwartet heruntergefahren. • Ein Gateway-Upload-Puffer wurde überschritten. In diesem Szenario tritt Bootstrapping auf, wenn Ihr Volume den Status Pass Through besitzt und die Menge des kostenlosen Upload-Puffers ausreiche nd erhöht wird. Sie können zusätzlichen Upload-Pufferspeicherplatz als eine Möglichkeit zur Erhöhung des Prozentsatzes der kostenlos en Upload-Pufferspeicher schaffen. In diesem Szenario ändert sich der Status des Speichervolumes von Pass Through in Bootstrap ping in Available. Sie können dieses Volume während des Bootstrap ping Zeitraums weiterhin verwenden. Sie können jedoch zu diesem Zeitpunkt keine Snapshots des Volumes erstellen. • Sie erstellen ein Volume Gateway für gespeicherte Volumes und behalten die vorhandenen lokalen Festplattendaten bei. In diesem Szenario beginnt Ihr Gateway mit dem Hochladen aller Daten auf. AWS Das Volume hat den Status Bootstrapping, bis alle Daten von der lokalen Festplatte auf das Laufwerk kopiert wurden. AWS Sie können dieses Volume während des Bootstrapping Zeitraums weiterhin

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

Status	Bedeutung
Pass Through	Lokal verwaltete Daten sind nicht mit den darauf gespeicherten Daten synchron. AWS Daten, die auf ein Volume geschrieben werden, während das Volume sich im Status Pass Through befindet, verbleiben im Cache, bis der Volume-Status Bootstrapping lautet. Der Upload dieser Daten beginnt zu dem AWS Zeitpunkt, zu dem der Bootstrapping-Status beginnt. Der Status Pass Through kann aus verschiedenen Gründen auftreten, darunter z. B.: • Der Status Pass Through tritt auf, wenn Ihr Gateway keinen Upload-Pufferspeicher mehr hat. Während die Volumes den Status Pass Through haben, können Ihre Anwendungen weiterhin Daten von Ihren Speichervolumes lesen und Daten auf Speichervolumes schreiben. Jedoch schreibt das Gateway keine Volume-Daten in den Upload-Puffer oder lädt diese Daten auch nicht in AWS hoch. Das Gateway lädt weiterhin alle Daten hoch, die auf das Volume geschrieben wurden, bevor das Volume den Status Pass Through angenommen hat. Alle ausstehenden oder geplanten Snapshots eines Speichervolumes schlagen fehl, während das Volume im Status Pass Through ist. Weitere Informationen darüber, welche Aktion durchzuführen ist, wenn das Speichervolume den Status Pass Through erreicht, weil der Upload-Puffer erschöpft ist, finden Sie unter Fehlerbehebung bei Volume-Problemen. Um zum Status ACTIVE (AKTIV) zurückzukehren, muss ein Volume im Status Pass Through die Bootstrapping-Phase beenden. Während des Bootstrappings stellt das Volume die interne Synchronisation wieder her AWS, sodass es die Aufzeichnung (das Protokoll) der Änderungen am Volume fortsetzen und die Funktionalität aktivieren kann. `CreateSnapshot` Beim Bootstrapping werden Schreibvorgänge auf das Volume im Upload-Puffer erfasst. •

Status	Bedeutung
	Der Status Pass Through tritt auf, wenn sich mehr als ein Speichervolume im Bootstrapping befindet. Es kann nur jeweils ein Gateway-Speichervolume zur gleichen Zeit Bootstrappen. Beispiel: Sie erstellen zwei Speichervolumes und wollen die vorhandenen Daten auf beiden beibehalten. In diesem Fall behält das zweite Speichervolume den Status Pass Through, bis das erste Speichervolume das Bootstrapping beendet hat. In diesem Szenario müssen Sie keine Maßnahmen ergreifen. Jedes Speichervolume wechselt automatisch in den Status Verfügbar, sobald seine Erstellung abgeschlossen ist. Sie können die Lese- und Schreibvorgänge zum Speichervolume fortsetzen, während es im Status Pass Through oder Bootstrapping ist. • In seltenen Fällen gibt der Status Pass Through an, dass eine Festplatte, die einem Upload-Puffer zugeordnet wurde, fehlgeschlagen ist. Weitere Informationen, welche Aktionen in diesem Fall auszuführen sind, finden Sie unter Fehlerbehebung bei Volume-Problemen. • Der Status Pass Through kann auftreten, wenn ein Volume den Zustand Active (Aktiv) oder Bootstrapping aufweist. In diesem Fall empfängt das Volume eine Schreiboperation, die Kapazität des Upload-Puffers reicht aber nicht mehr aus, um die Schreiboperation aufzuzeichnen (zu protokollieren). • Der Status Pass Through tritt bei beliebigem Status des Volumes auf, wenn das Gateway nicht ordnungsgemäß heruntergefahren wird. Zu einem nicht ordnungsgemäßen Herunterfahren kann es kommen, wenn die Software abstürzt oder die VM ausgeschaltet wird. In diesem Fall wird ein Volume, egal in welchem Zustand es sich befindet, in den Status Pass Through übergehen.

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

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

Grundlegendes zum Anfügestatus

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

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

Grundlagen zu Statusübergängen bei zwischengespeicherten Volumes

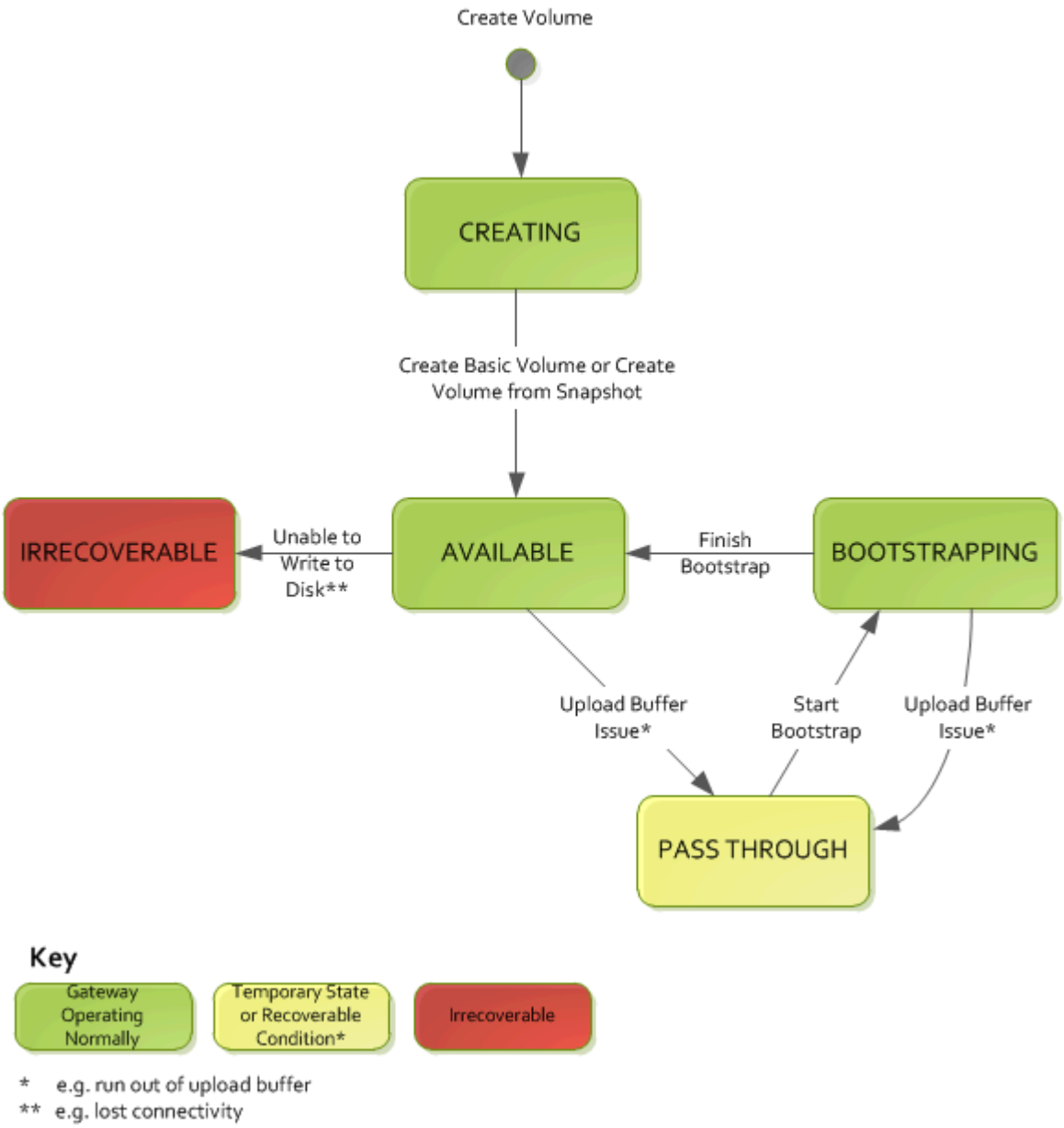
Das folgende Statusdiagramm beschreibt die gängigsten Statusübergänge für Volumes in Cached-Gateways. Sie müssen das Diagramm nicht im Detail verstehen, um Ihr Gateway effektiv zu verwenden. Die Abbildung bietet vielmehr detaillierte Informationen, wenn Sie mehr darüber erfahren möchten, wie Volume Gateways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

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

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

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

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



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

Grundlagen zu Statusübergängen bei gespeicherten Volumes

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

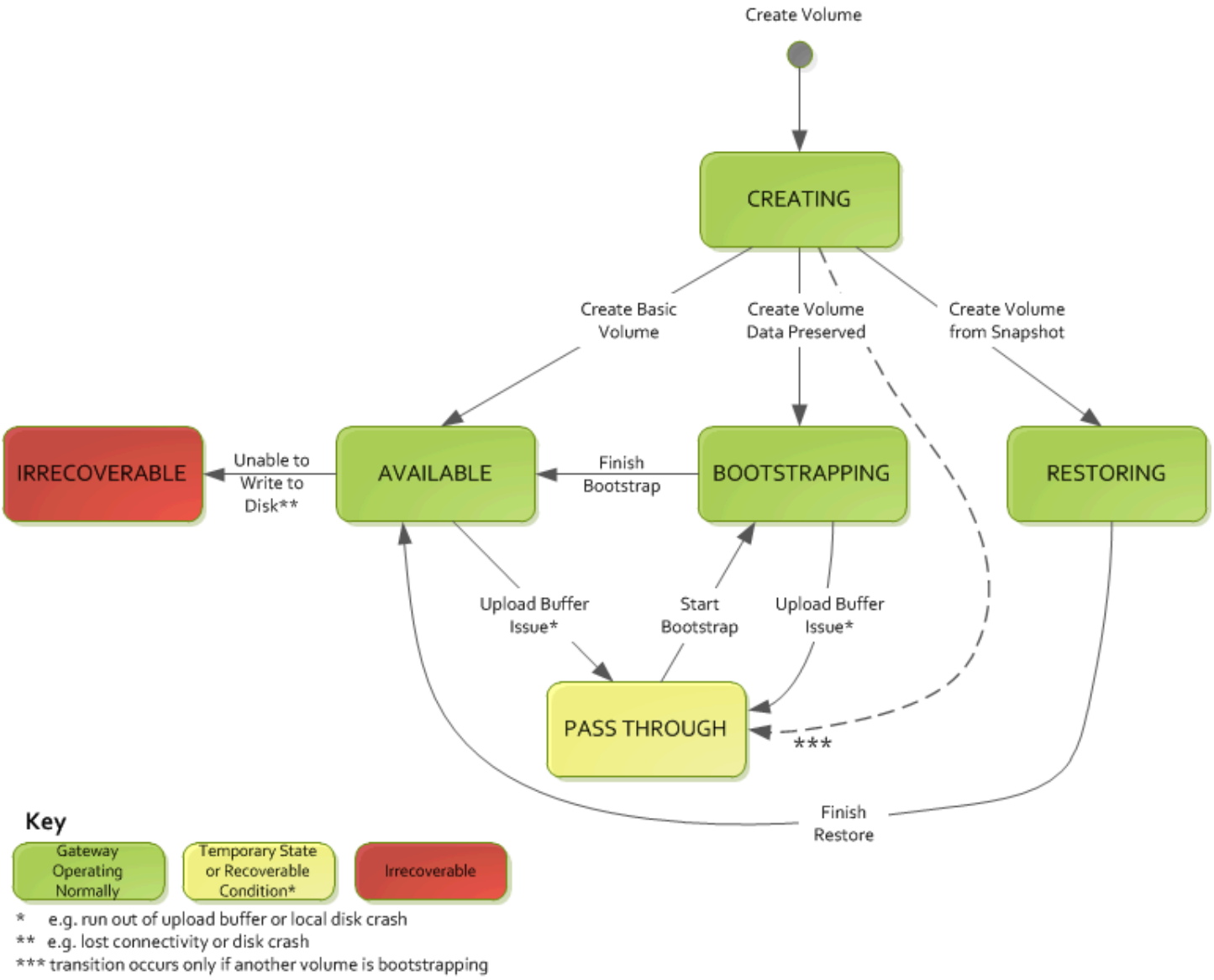
verwenden. Die Abbildung bietet vielmehr detaillierte Informationen, wenn Sie verstehen möchten, wie Volume Gateways funktionieren.

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

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

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

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



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

Verschieben Ihrer Daten auf eine neue Gateway-Instanz

> **Note**
>
> Wenn Sie eine Migration von Storage Gateway AL2 zu AL2023 durchführen, stellen Sie vor Beginn sicher, dass Sie alle Punkte der Pre-migration Checkliste in der abgeschlossen haben.

Sie können Daten zwischen Gateways verschieben, wenn Ihre Daten- und Leistungsanforderungen steigen oder wenn Sie eine Benachrichtigung zur Migration Ihres Gateways erhalten. AWS Nachfolgend sind einige Gründe für diesen Vorgang ausgeführt:

- Verschieben Sie Ihre Daten zu besseren Host-Plattformen oder neueren Amazon-EC2-Instances.
- Aktualisieren der zugrunde liegenden Hardware für Ihren Server

> **Important**
>
> Daten können nur zwischen den gleichen Gateway-Typen verschoben werden.
> Die folgenden Migrationsanweisungen können nur für Gateway-Geräte verwendet werden, auf denen Version 2.x ausgeführt wird. Sie können sie nicht zur Migration von Gateway-Appliances verwenden, auf denen niedrigere Versionen ausgeführt werden.

Der Migrationsprozess unterscheidet sich je nachdem, ob Sie gespeicherte Volumes oder zwischengespeicherte Volumes verwenden. Für diese beiden Gateway-Typen sind unterschiedliche Migrationsschritte erforderlich. Wählen Sie das Verfahren, das Ihrem Gateway-Typ entspricht:

Themen

- Verschieben gespeicherter Volumes auf ein neues gespeichertes Volume Gateway
- Verschieben zwischengespeicherter Volumes auf eine neue virtuelle Gateway-Maschine

Verschieben gespeicherter Volumes auf ein neues gespeichertes Volume Gateway

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

1. Beenden Sie alle Anwendungen, die auf das alte gespeicherte Volume Gateway schreiben.
2. Führen Sie die folgenden Schritte aus, um einen Snapshot für Ihr Volume zu erstellen, und warten Sie dann, bis der Snapshot abgeschlossen ist.

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

   b. Wählen Sie im Navigationsbereich zunächst Volumes und anschließend das Volume aus, von dem Sie den Snapshot erstellen möchten.

   c. Wählen Sie für Aktionen Snapshot erstellen aus.

   d. Geben Sie im Dialogfeld Snapshot erstellen die Beschreibung des Snapshots ein und wählen Sie anschließend Snapshot erstellen.

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

   a. Wählen Sie im Navigationsbereich Gateways und anschließend das alte gespeicherte Volume Gateway aus, das Sie beenden möchten. Der Status des Gateways lautet In Ausführung.

   b. Wählen Sie unter Aktionen die Option Gateway anhalten aus. Überprüfen Sie die ID des Gateways im Dialogfeld. Wählen Sie dann Gateway anhalten aus.

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

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

   Weitere Informationen zum Anhalten von Gateways finden Sie unter Starten und Anhalten eines Volume Gateways.

4. Trennen Sie die Speicherfestplatten, die Ihren gespeicherten Volumes zugeordnet sind, von der Gateway-VM. Die Stammfestplatte der VM wird hier ausgeschlossen.
5. Aktivieren Sie ein neues Stored Volume Gateway mit einem neuen Hypervisor-VM-Image, das über die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause verfügbar ist.
6. Fügen Sie die physischen Speicherfestplatten an, die Sie in Schritt 5 von der alten gespeicherten Volume Gateway-VM getrennt haben.
7. Gehen Sie wie folgt vor, um gespeicherte Volumes zu erstellen und die vorhandenen Daten auf der Festplatte beizubehalten.

   a. Wählen Sie in der Storage-Gateway-Konsole Volume erstellen aus.
   b. Wählen Sie im Dialogfeld Volume erstellen das gespeicherte Volume Gateway aus, das Sie in Schritt 5 erstellt haben.
   c. Wählen Sie einen Wert für Festplatten-ID aus der Liste aus.
   d. Für Volume-Inhalt wählen Sie die Option Vorhandene Daten auf der Festplatte beibehalten aus.

   Weitere Informationen zur Erstellung von Volumes finden Sie unter Ein Speichervolume erstellen.
8. (Optional) Geben Sie im Assistenten zum Konfigurieren der CHAP-Authentifizierung in den Feldern Initiatorname, Initiatorgeheimnis und Zielgeheimnis die entsprechenden Angaben ein und wählen Sie Speichern aus.

   Weitere Informationen zum Arbeiten mit der CHAP-Authentifizierung (Challenge-Handshake Authentication Protocol) finden Sie unter Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele.
9. Starten Sie die Anwendung, die auf Ihr gespeichertes Volume schreibt.
10. Wenn Sie sich vergewissert haben, dass Ihr neues gespeichertes Volume Gateway ordnungsgemäß funktioniert, können Sie das alte gespeicherte Volume Gateway löschen.

> **Important**
>
> Bevor Sie diesen Schritt ausführen, stellen Sie sicher, dass derzeit keine Anwendungen in die Volumes dieses Gateways schreiben. Wenn Sie ein Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten.

Gehen Sie wie folgt vor, um das alte gespeicherte Volume Gateway zu löschen:

> **Warning**
>
> Wenn ein Gateway gelöscht worden ist, gibt es keine Möglichkeit, es wiederherzustellen.

a. Wählen Sie im Navigationsbereich zunächst Gateways und anschließend das gespeicherte Volume Gateway aus, das Sie löschen möchten.

b. Wählen Sie für Aktionen die Option Gateway löschen aus.

c. Aktivieren Sie im Bestätigungsdialogfeld, das angezeigt wird, das Kontrollkästchen zum Bestätigen des Löschvorgangs. Stellen Sie sicher, dass die aufgelistete Gateway-ID das alte gespeicherte Volume Gateway angibt, das Sie löschen möchten, und wählen Sie dann Löschen aus.

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

Verschieben zwischengespeicherter Volumes auf eine neue virtuelle Gateway-Maschine

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

1. Beenden Sie alle Anwendungen, die auf das alte zwischengespeicherte Volume Gateway schreiben.
2. Gehen Sie wie folgt vor, um das Gateway auf die neueste Version zu aktualisieren

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

   b. Wählen Sie im Navigationsbereich Gateways und dann das alte zwischengespeicherte Volume Gateway aus, das Sie migrieren möchten.

   c. Klicken Sie auf Jetzt aktualisieren, falls verfügbar. Wenn nicht, ist Ihr Gateway bereits auf der neuesten Version.

3. Stellen Sie sicher, dass die `CachePercentDirty` Metrik auf der Registerkarte Überwachung für das vorhandene Cache-Gateway `0`
4. Trennen Sie die iSCSI-Volumes von allen Clients, die sie verwenden, oder heben Sie die Bereitstellung dieser Volumes auf. Dies trägt dazu bei, dass die Daten auf diesen Volumes konsistent bleiben, indem verhindert wird, dass Clients Daten auf diesen Volumes ändern oder hinzufügen.
5. Führen Sie die folgenden Schritte aus, um einen Snapshot für Ihr Volume zu erstellen, und warten Sie dann, bis der Snapshot abgeschlossen ist.

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

   b. Wählen Sie im Navigationsbereich zunächst Volumes und anschließend das Volume aus, von dem Sie den Snapshot erstellen möchten.

   c. Wählen Sie unter Aktionen die Option EBS-Snapshot erstellen aus.

   d. Geben Sie im Dialogfeld Snapshot erstellen die Beschreibung des Snapshots ein und wählen Sie anschließend Snapshot erstellen.

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

   Weitere Informationen zum Überprüfen des Volume-Status finden Sie unter Grundlagen zu Status und Übergängen bei Volumes. Informationen zum Status zwischengespeicherter Volumes finden Sie unter Grundlagen zu Statusübergängen bei zwischengespeicherten Volumes.
6. Führen Sie die folgenden Schritte aus, um das alte zwischengespeicherte Volume Gateway zu beenden:

   a. Wählen Sie im Navigationsbereich Gateways und anschließend das alte zwischengespeicherte Volume Gateway aus, das Sie beenden möchten.

   b. Wählen Sie unter Aktionen die Option Gateway anhalten aus. Überprüfen Sie die ID des Gateways im Dialogfeld und wählen Sie dann Gateway anhalten aus. Notieren Sie sich die Gateway-ID, da sie in einem späteren Schritt benötigt wird.

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

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

Weitere Informationen zum Beenden von Gateways finden Sie unter Starten und Anhalten eines Volume Gateways.

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

> **Note**
>
> Notieren Sie sich die Volume-ID der Stammfestplatte sowie die Gateway-ID, die dieser Stammfestplatte zugeordnet ist. Sie verwenden diese Festplatte in späteren Schritten.

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

8. Erstellen Sie eine neue Storage-Gateway-Hypervisor-VM-Instance, aktivieren Sie sie jedoch nicht als Gateway. Weitere Informationen zum Erstellen einer neuen Storage-Gateway-Hypervisor-VM finden Sie unterEinrichten eines Volume Gateways. Dieses neue Gateway nimmt die Identität des alten Gateways an.

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

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

   Wenn Sie eine statische IP-Adresse für Ihre neue VM manuell konfigurieren müssen, finden Sie weitere Informationen unter Konfigurieren Ihres Gateway-Netzwerks. Wenn Ihr Gateway einen Socket Secure Version 5 (SOCKS5) -Proxy verwenden muss, um eine Verbindung zum Internet herzustellen, finden Sie weitere Informationen unter. Konfiguration eines SOCKS5 Proxys für Ihr lokales Gateway

10. Starten Sie die neue VM.
11. Hängen Sie die Festplatten, die Sie in Schritt 7 von der alten zwischengespeicherten Volume Gateway-VM getrennt haben, an das neue zwischengespeicherte Volume Gateway an. Fügen Sie sie in derselben Reihenfolge an die neue Gateway-VM an, in der sie sich auf der alten Gateway-VM befinden.

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

12. Initiieren Sie den Gateway-Migrationsprozess, indem Sie entweder eine Verbindung zur lokalen Konsole der neuen Gateway-VM herstellen oder Webanfragen an die IP-Adresse der neuen Gateway-VM stellen (unten beschrieben).

    a. Um die lokale Konsole zu verwenden, wählen Sie die Option Migrate Gateway und geben Sie Ihre bestehende Gateway-ID ein, wenn Sie dazu aufgefordert werden. Sie werden aufgefordert, zuvor angewendete Einstellungen auf dem alten Gateway auf das neue Gateway zu kopieren. Sie können wählen, ob Sie sie anwenden oder später manuell konfigurieren möchten. Siehe Zugreifen auf die lokale Gateway-Konsole.

    b. Alternativ können Sie den Gateway-Migrationsprozess einleiten, indem Sie mit einer URL, die das folgende Format verwendet, eine Verbindung zur neuen VM herstellen.

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

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

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

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

Wenn der Gateway-Migrationsprozess erfolgreich abgeschlossen wurde, wird eine Meldung angezeigt, die die erfolgreiche Migration bestätigt.

13. Trennen Sie die Root-Festplatte des alten Gateways, deren Volume-ID Sie in Schritt 7 notiert haben.
14. Starten Sie das Gateway.

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

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

    b. Wählen Sie im Navigationsbereich Gateways und wählen Sie dann das zu startende Gateway. Der Status des Gateways ist Shutdown (Herunterfahren).

    c. Wählen Sie Details und dann Gateway starten aus.

    Weitere Informationen zum Starten von Gateways finden Sie unter Starten und Anhalten eines Volume Gateways.
15. Ihre Volumes sollten jetzt über die Netzwerkschnittstellen der neuen Gateway-VM für Ihre Anwendungen verfügbar sein. Die Erfolgsmeldung der Migration enthält Details zur aktualisierten Zuordnung zwischen den einzelnen Volumes und der Netzwerkschnittstelle des neuen Gateways. Weitere Informationen zu den IP-Adressen, die den einzelnen Netzwerkschnittstellen zugeordnet sind, finden Sie auf der Hauptseite der lokalen Konsole des Gateways. Siehe Zugreifen auf die lokale Gateway-Konsole.

16. Vergewissern Sie sich, dass Ihre Volumes verfügbar sind, und löschen Sie die alte Gateway-VM. Informationen zum Löschen einer VM finden Sie in der Dokumentation zu Ihrem Hypervisor.

Überwachen von Storage Gateway

In diesem Abschnitt wird beschrieben, wie Sie ein 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 Volume Gateways und der zugehörigen Ressourcen finden Sie unter Monitoring your Volume 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
- Überwachung Ihres Volume Gateways

Grundlagen zu Gateway-Metriken

Für die Diskussion in diesem Thema definieren wir Gateway-Metriken als Metriken, die sich auf das Gateway beziehen – das heißt, sie messen einen bestimmten Aspekt des Gateways. Da ein Gateway ein oder mehrere Volumes enthält, steht eine Gateway-spezifische Metrik stellvertretend für alle Volumes auf dem Gateway. Die `CloudBytesUploaded`-Metrik stellt beispielsweise die Gesamtanzahl der Bytes dar, die das Gateway im Berichtszeitraum an die Cloud gesendet hat. Diese Metrik enthält die Aktivitäten aller Volumes auf dem Gateway.

Bei der Verwendung von Gateway-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	Description
`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	Description	
	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	Description	
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	Description	
QueuedWrites	Normalerweise steht dieser Wert für die Anzahl der lokal gespeicherten Byte, die darauf warten, geschrieben en zu werden AWS, aber er spiegelt auch den Synchroni sationsprozess wider, der zwischen lokalen Daten und Cloud-Daten während des „Bootstrappings“ stattfindet, das bei jedem Neustart eines Gateways stattfindet. Einheit: Byte	
ReadBytes	Die Gesamtzahl der Byte, die in Ihren lokalen Anwendung en im Berichtszeitraum für alle Volumes im Gateway gelesen wurden. Verwenden Sie diese Metrik mit der Sum-Statistik, um den Durchsatz zu messen, und mit der Samples-Statistik, um die IOPS-Werte zu messen. Einheit: Byte	

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

Metrik	Description	
`WorkingStorageUsed`	Gesamtanzahl der im Gateway-Upload-Puffer verwendeten Byte. Die Stichprobe wird am Ende des Berichtszeitraums entnommen . Einheit: Byte	
`WriteBytes`	Die Gesamtzahl der Byte, die in Ihren lokalen Anwendung en im Berichtszeitraum für alle Volumes im Gateway geschrieben wurden. Verwenden Sie diese Metrik mit der `Sum`-Statistik, um den Durchsatz zu messen, und mit der `Samples`-Statistik, um die IOPS-Werte zu messen. Einheit: Byte	
`WriteTime`	Die Gesamtzahl der Milliseku nden, die für Schreibop erationen in Ihren lokalen Anwendungen im Berichtsz eitraum für alle Volumes im Gateway aufgewendet wurden. Verwenden Sie diese Metrik mit der `Average`-Statistik, um die Latenz zu messen. Einheit: Millisekunden	

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

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 Volume 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 Volume 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	Verwenden Sie die `CacheHitPercent` -Metrik mit der `Average`-Statistik.

Interessierendes Element	Methode zum Messen
bedienten Leseanfragen	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 Volume Gateway verwendet werden, finden Sie unter Grundlegendes zu Gateway-Metriken und Grundlegendes zu Volume-Metriken. Für jeden Alarm geben Sie Bedingungen an, unter denen der ALARM-Status ausgelöst wird. Die Alarmstatusanzeigen in der Storage-Gateway-Konsole leuchten rot, wenn der Status ALARM aktiv ist, sodass Sie den Status leichter proaktiv überwachen können. Sie können Alarme so konfigurieren, dass bei anhaltenden Zustandsänderungen automatisch Aktionen aufgerufen werden. Weitere Informationen zu CloudWatch Alarmen finden Sie unter Verwenden von 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 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 Fehlerinformatione

Status	Beschreibung
	n 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 Volume 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.

Überwachung Ihres Volume Gateways

In den Themen dieses Abschnitts wird beschrieben, wie Volume Gateway entweder in der Konfiguration eines zwischengespeicherten Volumes oder eines gespeicherten Volumes überwacht wird, einschließlich der Überwachung der mit dem Gateway verknüpften Volumes und der Überwachung des Upload-Puffers. Sie verwenden den AWS-Managementkonsole , um Metriken für Ihr Gateway einzusehen. Sie können beispielsweise die für Lese- und Schreiboperationen verwendete Anzahl von Bytes, die für Lese- und Schreiboperationen aufgewendete Zeit und die Zeit für das Abrufen von Daten aus der Amazon Web Services-Cloud anzeigen. Mit Metriken können Sie den Zustand des Gateways verfolgen und Alarme festlegen, sodass Sie benachrichtigt werden, falls für eine oder mehrere Metriken ein festgelegter Schwellenwert überschritten wird.

Storage Gateway stellt CloudWatch Metriken ohne zusätzliche Kosten bereit. Storage-Gateway-Metriken werden für einen Zeitraum von zwei Wochen aufgezeichnet. Mithilfe dieser Metriken können Sie auf historische Informationen zugreifen und einen besseren Überblick darüber erhalten, wie das Gateway und die Volumes arbeiten. Ausführliche Informationen dazu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Topics

- Volume Gateway-Zustandsprotokolle mit Amazon CloudWatch Logs abrufen- Erfahren Sie, wie Sie Amazon CloudWatch Logs verwenden, um Informationen über den Zustand Ihres Volume Gateways und verwandter Ressourcen zu erhalten.
- Amazon CloudWatch Metrics verwenden- Erfahren Sie, wie Sie mithilfe der API AWS-Managementkonsole oder der CloudWatch API Überwachungsdaten für Ihr Gateway abrufen können.
- Messung der Leistung zwischen Ihrer Anwendung und dem Gateway- Erfahren Sie, wie Sie Datendurchsatz, Datenlatenz und Vorgänge pro Sekunde messen, um die Leistung zwischen Ihren Anwendungen und Ihrem Gateway zu verstehen.
- Messung der Leistung zwischen Ihrem Gateway und AWS- Erfahren Sie, wie Sie Datendurchsatz, Datenlatenz und Vorgänge pro Sekunde messen, um die Leistung zwischen Ihrem Gateway und der AWS Cloud zu verstehen.
- Volumenmetriken verstehen- Erfahren Sie, wie Sie Metriken messen, die Daten über die mit einem Gateway verbundenen Volumen liefern.

Volume Gateway-Zustandsprotokolle mit Amazon CloudWatch Logs abrufen

Sie können Amazon CloudWatch Logs verwenden, um Informationen über den Zustand Ihres Volume Gateways und verwandter Ressourcen zu erhalten. Sie können diese Protokolle verwenden, um Ihr Gateway auf auftretende Fehler zu überwachen. Darüber hinaus können Sie 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 High Availability (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. Hinweise zur Konfiguration einer CloudWatch Protokollgruppe bei der Aktivierung eines Gateways finden Sie unterKonfigurieren Ihres Volume 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 Fehlerbehebung bei Volume-Problemen.

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

Um eine CloudWatch Protokollgruppe so zu konfigurieren, dass sie mit Ihrem Gateway funktioniert

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Storage Gateway Gateway-Konsole zu https://console.aws.amazon.com/storagegateway/Hause.
2. Wählen Sie im linken Navigationsbereich Gateways und dann das Gateway aus, für das Sie die CloudWatch Protokollgruppe konfigurieren möchten.
3. Wählen Sie für Aktionen die Option Gateway-Informationen bearbeiten aus, oder wählen Sie auf der Registerkarte Details unter Integritätsprotokolle und Nicht aktiviert die Option Protokollgruppe konfigurieren aus, um das *CustomerGatewayName* Dialogfeld 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 linken 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 Protokollgruppendetails wird in der CloudWatch Amazon-Konsole geöffnet.

Amazon CloudWatch Metrics verwenden

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

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

- Die zu verwendende Metrikdimension. Eine Dimension ist ein Name-Wert-Paar, mit dem Sie eine Metrik eindeutig identifizieren. Die Dimensionen für Storage Gateway sind `GatewayId`, `GatewayName` und `VolumeId`. In der CloudWatch Konsole können Sie mithilfe der `Volume Metrics` Ansichten `Gateway Metrics` und auf einfache Weise Gateway-spezifische und volumespezifische Dimensionen auswählen. 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 Typen von Storage-Gateway-Metrikdaten, die Sie verwenden können.

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

CloudWatch Namespace	Dimension	Beschreibung
	`VolumeId`	Diese Dimension filtert nach Metrikdaten, die für ein Volume spezifisch sind. Identifizieren Sie ein zu verwendendes Volume mithilfe seiner `VolumeId`-Dimension. Die Daten werden automatisch in 5-Minuten-Intervallen kostenlos zur Verfügung gestellt.

Das Arbeiten mit Gateway- und Volume-Metriken gleicht dem Arbeiten mit anderen Service-Metriken. Eine Erläuterung einiger der häufigsten Aufgaben mit Metriken finden Sie in der folgenden CloudWatch-Dokumentation:

- Anzeigen der verfügbaren Metriken
- Abrufen von Statistiken für eine Metrik
- Erstellen von CloudWatch-Alarmen

Messung der Leistung zwischen Ihrer Anwendung und dem Gateway

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

Eine Statistik ist eine Aggregation einer Metrik über einen bestimmten Zeitraum. Wenn Sie die Werte einer Metrik in anzeigen CloudWatch, verwenden Sie die `Average` Statistik für Datenlatenz (Millisekunden), verwenden Sie die `Sum` Statistik für den Datendurchsatz (Byte pro Sekunde) und verwenden Sie die `Samples` Statistik für input/output Operationen 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 Ihren Anwendungen und Gateways messen können.

Interessierendes Element	Methode zum Messen
Durchsatz	Verwenden Sie die Metriken `ReadBytes` und `WriteBytes` mit der Statistik `Sum` CloudWatch . Beispiel: Mit dem `Sum`-Wert der `ReadBytes` -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie den Durchsatz als Rate in Byte pro Sekunde.
Latenz	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.
E/A\Sek	Verwenden Sie die Metriken `ReadBytes` und `WriteBytes` mit der Statistik `Samples` CloudWatch . Beispiel: Mit dem `Samples`-Wert der `ReadBytes` -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie IOPS.

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

So messen Sie den Datendurchsatz von einer Anwendung zu einem Volume

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

Wenn der Lesedurchsatz beispielsweise 2.384.199680 Byte über einen Zeitraum von 300 Sekunden beträgt, beträgt die ungefähre Durchsatzrate für diesen Datenpunkt 7,9 Megabyte pro Sekunde.

Um die input/output Datenoperationen pro Sekunde von einer Anwendung bis zu einem Volume zu messen

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

Wenn die Anzahl der Schreibvorgänge beispielsweise 24.373 über einen Zeitraum von 300 Sekunden beträgt, beträgt die Anzahl der IOPS für diesen Datenpunkt 81 Schreibvorgänge pro Sekunde.

Messung der Leistung zwischen Ihrem Gateway und AWS

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

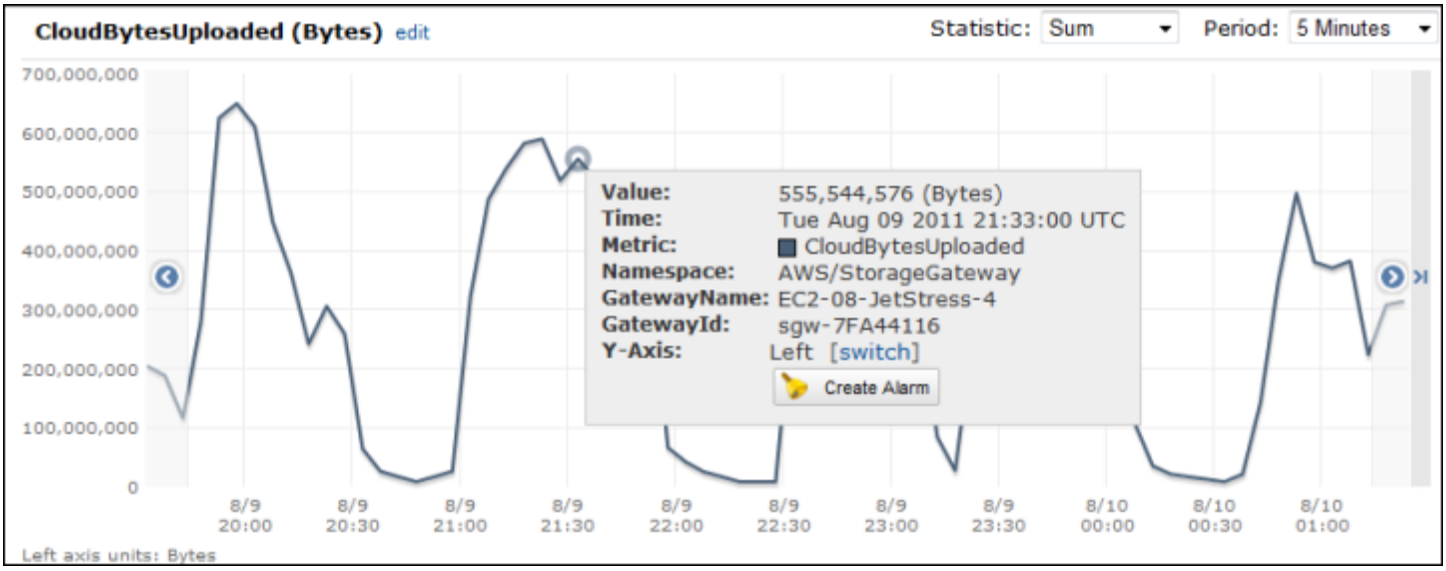
Interessierendes Element	Methode zum Messen
Durchsatz	Verwenden Sie die Metriken `ReadBytes` und `WriteBytes` mit der Statistik `Sum` CloudWatch . Beispiel: Mit dem `Sum`-Wert der `ReadBytes` -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie den Durchsatz als Rate in Byte pro Sekunde.
Latenz	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.
E/A\Sek	Verwenden Sie die Metriken `ReadBytes` und `WriteBytes` mit der Statistik `Samples` CloudWatch . Beispiel: Mit dem `Samples`-Wert der `ReadBytes` -Metrik über einen Stichprobenzeitraum von 5 Minuten dividiert durch 300 Sekunden erhalten Sie IOPS.
Durchsatz bis AWS	Verwenden Sie die `CloudBytesUploaded` Metriken `CloudBytesDownloaded` und zusammen mit der `Sum` CloudWatch Statistik. Beispiel: Der `Sum` Wert der `CloudBytesDownloaded` Metrik über einen Stichprobenzeitraum von 5 Minuten geteilt durch 300 Sekunden ergibt den Durchsatz vom Gateway AWS zum Gateway 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 Gateway zu AWS

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Gateway-Metriken aus und suchen Sie das Volume, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudBytesUploaded` aus.
5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die `Sum`-Statistik aus.

7. Wählen Sie für Zeitraum einen Wert von 5 Minuten oder mehr.
8. Dividieren Sie in der resultierenden zeitlich sortierten Gruppe von Datenpunkten jeden Datenpunkt durch den Zeitraum (in Sekunden), um den Durchsatz in diesem Stichprobenzeitraum zu erhalten.

Wenn Sie den Cursor über einen Datenpunkt bewegen, werden Informationen über den Datenpunkt angezeigt, einschließlich seines Werts und der hochgeladenen Byte. Dividieren Sie diesen Wert durch den Wert für Period (Zeitraum) (5 Minuten), um den Durchsatz an diesem Stichprobenpunkt zu erhalten. Wenn der Durchsatz vom Gateway zum beispielsweise 555.544.576 Byte über einen Zeitraum von 300 Sekunden AWS beträgt, beträgt der ungefähre Durchsatz pro Sekunde 1,85 Megabyte pro Sekunde.



So messen Sie die Latenz pro Operation eines Gateways

1. Öffnen Sie die Konsole unter. CloudWatch https://console.aws.amazon.com/cloudwatch/
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Gateway-Metriken aus und suchen Sie das Volume, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metriken `ReadTime` und `WriteTime` aus.
5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die `Average`-Statistik aus.
7. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

8. Addieren Sie in der resultierenden zeitlich sortierten Gruppe von Punkten (eine für `ReadTime` und eine für `WriteTime`) die Datenpunkte der gleichen zeitlichen Stichprobe, um die gesamte Latenz in Millisekunden zu erhalten.

Um die Datenlatenz von einem Gateway zu zu messen AWS

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Storage Gateway.
3. Wählen Sie die Dimension Gateway-Metriken aus und suchen Sie das Volume, mit dem Sie arbeiten möchten.
4. Wählen Sie die Metrik `CloudDownloadLatency` aus.
5. Wählen Sie einen Wert für Zeitraum aus.
6. Wählen Sie die `Average`-Statistik aus.
7. Wählen Sie für Zeitraum einen Wert von 5 Minuten aus, was der Standardberichtszeit entspricht.

Die resultierende zeitlich sortierte Gruppe von Datenpunkten enthält die Latenz in Millisekunden.

Um einen Alarm für den oberen Schwellenwert für den Durchsatz eines Gateways auf einzustellen AWS

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Alarms (Alarme).
3. Wählen Sie Alarm erstellen, um den Assistenten zum Erstellen von Alarmen zu starten.
4. Wählen Sie die Dimension Storage Gateway aus und suchen Sie das Gateway, mit dem Sie arbeiten möchten.
5. Wählen Sie die Metrik `CloudBytesUploaded` aus.
6. Zum Definieren des Alarms legen Sie den Alarmstatus fest, wenn die `CloudBytesUploaded`-Metrik für eine bestimmte Zeit größer als oder gleich einem angegebenen Wert ist. Sie können beispielsweise einen Alarmstatus festlegen, wenn die `CloudBytesUploaded`-Metrik für 60 Minuten größer als 10 MB ist.
7. Konfigurieren Sie die auszuführenden Aktionen für den Alarmstatus. Sie können beispielsweise eine E-Mail-Benachrichtigung an sich selbst senden lassen.
8. Wählen Sie Alarm erstellen.

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 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.

Volumenmetriken verstehen

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

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

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
`AvailabilityNotification`	Die Anzahl der vom Volume gesendeten Verfügbarkeitsbenachrichtigungen. Einheiten: Anzahl	Ja	Ja
`CacheHitPercent`	Prozentsatz der Anwendungsleseoperationen vom Volume aus dem Cache. Die Stichprobe wird am Ende des Berichtszeitraums entnommen. Wenn keine Anwendungsleseoperationen vom Volume vorhanden sind, wird dieser Metrikwert mit 100 % angegeben. Einheiten: Prozent	Ja	Nein
`CachePercentDirty`	Der Anteil des Volumes am Gesamtprozentsatz des Gateway-Caches, der nicht für AWS beibehalten wurde. Die Stichprobe wird am Ende des Berichtszeitraums entnommen.	Ja	Ja

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
	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		

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

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

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
`MemoryUsage`	Der Prozentsatz des Speichers, der gegenwärtig vom Volume verwendet wird. Einheiten: Prozent	Ja	Nein
`ReadBytes`	Die Gesamtzahl in Byte, die in Ihren lokalen Anwendungen im Berichtszeitraum 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	Ja	Ja

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

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
`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	Ja	Ja
`WriteTime`	Die Gesamtzahl der Millisekunden, die im Berichtszeitraum für Schreiboperationen in Ihren On-Premise-Anwendungen aufgewendet wurden. Verwenden Sie diese Metrik mit der `Average`-Statistik, um die Latenz zu messen. Einheiten: Millisekunden	Ja	Ja

Metrik	Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
`QueuedWrites`	Die Anzahl der Byte, in die geschrieb en werden muss AWS, gemessen am Ende des Berichtsz eitraums. Einheiten: Byte	Ja	Ja

Warten eines Gateways

Die Wartung Ihres Volume Gateways 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 für Pufferung und Speicherung zuweisen.
- Verwaltung der Bandbreite für Ihr Volume 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 Volume 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:

- Volume Gateways:
  - Gespeicherte Gateways benötigen mindestens eine Festplatte als Upload-Puffer.
  - Cached-Gateways benötigen mindestens zwei Festplatten. Ein für die Verwendung als Cache, und eine als Upload-Puffer.

In der folgenden Tabelle sind Empfehlungen für Größen für lokalen Festplattenspeicher für Ihr bereitgestelltes Gateway aufgeführt. Nach dem Einrichten des Gateways können Sie entsprechend der steigenden Auslastung weiteren lokalen Speicher zuweisen.

Lokaler Speicher	Description	
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 I/O auf einem Volume oder Band ausgeführ t wird, speichert das Gateway die Daten für den Zugriff mit geringer Latenz im Cache-Spe icher. Wenn die Anwendung Daten	

Lokaler Speicher	Description	
	von einem Volume oder Band anfordert, überprüft das Gateway zunächst den Cache-Speicher auf Daten, bevor die Daten von AWS heruntergeladen werden.	

> **Note**
>
> Bei der Bereitstellung von Festplatten wird dringend empfohlen, keine lokalen Festplatten für den Upload-Puffer und Cache-Speicher bereitzustellen, die die gleiche physische Speicherressource (d. h. die gleiche Festplatte) verwenden. Die zugrunde liegenden physischen Speicherressourcen werden als Datenspeicher in VMware dargestellt. Wenn Sie die Gateway-VM bereitstellen, wählen Sie einen Datenspeicher für die Speicherung der VM-Dateien. Wenn Sie eine lokale Festplatte bereitstellen (z. B. zur Verwendung als Cache-Speicher oder Upload-Puffer), haben Sie die Möglichkeit, die virtuelle Festplatte im gleichen Datenspeicher wie die VM oder in einem anderen Datenspeicher zu speichern.
> Wenn Sie über mehr als einen Datenspeicher verfügen, sollten Sie unbedingt einen Datenspeicher als Cache-Speicher und einen anderen als Upload-Puffer festlegen. Ein Datenspeicher, der nur durch eine zugrunde liegende physische Festplatte oder durch eine weniger leistungsfähige RAID-Konfiguration wie RAID 1 gesichert wird, kann in einigen Situationen zu schlechter Leistung führen, wenn er sowohl als Cache-Speicher als auch als Upload-Puffer verwendet wird. Dies gilt auch, wenn 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**
>
> Bei Volume Gateways wechselt das Volume in den Status PASS THROUGH, wenn der Upload-Puffer seine Kapazität erreicht. In diesem Status werden neue von der Anwendung geschriebene Daten lokal gespeichert, aber nicht sofort an AWS hochgeladen. Daher können Sie keine neuen Snapshots aufnehmen. Wenn Kapazität des Upload-Puffers frei wird, wechselt das Volume in den Status BOOTSTRAPPING. In diesem Status werden alle neuen Daten, die lokal gespeichert wurden, hochgeladen. AWS Schließlich wechselt das Volume wieder zum Status ACTIVE zurück. Storage Gateway nimmt dann die normale Synchronisation der lokal gespeicherten Daten mit der Kopie wieder auf AWS, und Sie können mit der Erstellung neuer Snapshots beginnen. Weitere Informationen zum Volume-Status finden Sie unter Grundlagen zu Status und Übergängen bei Volumes.

Zur Schätzung der Menge des zuzuordnenden Upload-Puffers können Sie die erwarteten eingehenden und ausgehenden Datenraten bestimmen und in der folgenden Formel verwenden.

Rate der eingehenden Daten

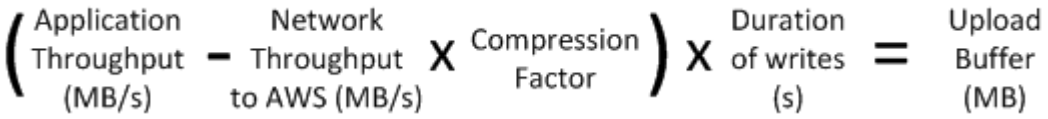
Diese Rate bezieht sich auf den Anwendungsdurchsatz, die Rate, zu der die lokalen Anwendungen Daten in einem bestimmten Zeitraum an das Gateway schreiben.

Rate der ausgehenden Daten

Diese Rate bezieht sich auf die Netzwerkdurchsatz, die Rate, mit der das Gateway Daten an AWS hochladen kann. Diese Rate hängt von Ihrer Netzwerkgeschwindigkeit und der Auslastung sowie davon ab, ob Sie die Bandbreitendrosselung aktiviert haben. Diese Rate sollte unter Berücksichtigung der Komprimierung angepasst werden. Beim Hochladen von Daten in 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.



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 in der Amazon-EC2-Instance erstellen. Entfernen Sie keine Festplatten oder ändern Sie nicht die Größe vorhandener Festplatten, die bereits als Cache- oder Upload-Puffer zugewiesen wurden.

So konfigurieren Sie zusätzlichen Upload-Puffer oder Cache-Speicher für Ihr Gateway

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

> **Note**
>
> UPLOAD BUFFER ist die einzige verfügbare Option für die Zuweisung von Festplatten auf Volume Gateways für gespeicherte Volumes.

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

Verwaltung der Bandbreite für Ihr Volume Gateway

Sie können den Upload-Durchsatz vom Gateway zu oder den Download-Durchsatz von AWS zu Ihrem Gateway einschränken (AWS oder drosseln). Mithilfe der Bandbreitendrosselung können Sie die Menge der von Ihrem Gateway verwendeten Netzwerkbandbreite kontrollieren. Standardmäßig hat ein aktiviertes Gateway keine Ratenbegrenzungen für Upload oder Download.

Sie können das Ratenlimit mithilfe der AWS-Managementkonsole 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 mit dem 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 mit dem 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 Gateway-Appliance wie eine verwaltete virtuelle Maschine behandeln und nicht versuchen, auf ihre Installation oder ihren Inhalt zuzugreifen oder sie in irgendeiner Weise zu ändern. Der Versuch, Softwarepakete mit anderen Methoden als dem normalen AWS Gateway-Aktualisierungsmechanismus (z. B. SSM- oder Hypervisor-Tools) zu installieren oder zu aktualisieren, kann zu Fehlfunktionen des Gateways führen.
Storage Gateway patcht die Appliance automatisch und regelmäßig, um Sicherheit und Stabilität zu gewährleisten. Storage Gateway Gateway-Appliances verwenden Amazon Linux als Basisbetriebssystem. Sie können den Status der erkannten Common Vulnerabilities and Exposures (CVE) -Probleme im Amazon Linux Security Center überprüfen. CVE-Patches werden automatisch innerhalb von 30 Tagen nach ihrer Veröffentlichung installiert, wie im Amazon Linux Security Center angegeben. Patches werden während Ihres Gateway-Wartungsplans installiert, sofern Ihr Gateway online ist.
Storage Gateway unterstützt die manuelle Aktualisierung eines EC2 Amazon-Gateways mithilfe von Cloud-Init-Direktiven nicht. Wenn Sie diese Methode verwenden, um ein Gateway zu aktualisieren, können Interoperabilitätsprobleme auftreten, die Sie daran hindern, die Gateway-Appliance zu aktivieren oder zu verwenden.

Aktualisierungshäufigkeit und erwartetes Verhalten

AWS aktualisiert die Cloud-Services-Komponente nach Bedarf, ohne dass die bereitgestellten Gateways unterbrochen werden. Ihre bereitgestellten Gateway-Appliances erhalten 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 und den Versionshinweisen für die Volume Gateway-Appliance-Software.

Monatliche Wartungsupdates können zu einer kurzen Betriebsunterbrechung führen. Der VM-Host des Gateways muss während der Updates nicht neu gestartet werden, aber das Gateway ist für kurze Zeit nicht verfügbar, solange das Gateway-Gerät aktualisiert und neu gestartet wird. 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 einzustellen, dass er an den Tagen 29 bis 31 beginnt.
      > Wenn Sie bei der Konfiguration dieser Einstellung eine Fehlermeldung erhalten, kann dies bedeuten, dass Ihre Gateway-Software veraltet ist. Erwägen Sie, Ihr Gateway zunächst manuell zu aktualisieren und dann erneut zu versuchen, den Zeitplan für das Wartungsfenster zu konfigurieren.

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

Sie können die aktualisierten Einstellungen auf der Registerkarte Details für das ausgewählte Gateway in der Storage Gateway Gateway-Konsole überprüfen.

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. Obwohl sich dieser Abschnitt auf das Starten und Stoppen Ihres Gateways mithilfe der Storage Gateway Management Console konzentriert, können Sie Ihr Gateway auch mithilfe Ihrer lokalen VM-Konsole oder der Storage Gateway Gateway-API starten und stoppen. 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 Volume Gateway anmelden.
- Storage Gateway Gateway-API — siehe ShutdownGateway

Starten und Anhalten eines Volume Gateways

So beenden Sie ein Volume 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 Volume 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.

Sie können ein Gateway mithilfe der Storage-Gateway-Konsole oder programmgesteuert löschen. Im Folgenden finden Sie Informationen zum Löschen eines Gateways mit der Storage-Gateway-

Konsole. Informationen zum programmgesteuerten Löschen eines Gateways finden Sie unter AWS Storage Gateway API-Referenz..

Themen

- Löschen eines Gateways mithilfe der Storage-Gateway-Konsole
- Entfernen von Ressourcen von einem lokal bereitgestellten Gateway
- Entfernen von Ressourcen von einem auf einer Amazon-EC2-Instance bereitgestellten Gateway

Löschen eines Gateways mithilfe der Storage-Gateway-Konsole

Die Schritte zum Löschen eines Gateways sind für alle Gateway-Typen gleich. Abhängig von dem Typ des Gateways, das Sie löschen möchten, und dem Host, auf dem es bereitgestellt wird, müssen Sie jedoch möglicherweise zusätzliche Aufgaben zum Entfernen von dem Gateway zugeordneten Ressourcen ausführen. Durch das Entfernen dieser Ressourcen wird verhindert, dass Sie für Ressourcen zahlen, die Sie voraussichtlich nicht mehr verwenden werden.

> **Note**
>
> Bei Gateways, die auf einer Amazon-EC2-Instance bereitgestellt werden, existiert die Instance weiterhin, bis Sie sie löschen.
> Bei Gateways, die auf einer virtuellen Maschine (VM) bereitgestellt sind, ist die Gateway-VM nach dem Löschen des Gateways weiterhin in der Virtualisierungsumgebung vorhanden. Um die VM zu entfernen, verwenden Sie den VMware vSphere-Client, Microsoft Hyper-V Manager oder den Linux Kernel-based Virtual Machine (KVM) -Client, um eine Verbindung zum Host herzustellen und die VM zu entfernen. Beachten Sie, dass Sie die gelöschte Gateway-VM nicht erneut verwenden können, um ein neues Gateway zu aktivieren.

So löschen Sie ein Gateway

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie Gateways und anschließend ein oder mehrere Gateways zum Löschen aus.
3. Wählen Sie für Aktionen die Option Gateway löschen aus. Das Bestätigungsdialogfeld wird angezeigt.

> **Warning**
>
> Bevor Sie diesen Schritt ausführen, stellen Sie sicher, dass derzeit keine Anwendungen in die Gateway-Volumes schreiben. Wenn Sie das Gateway löschen, während es verwendet wird, kann ein Datenverlust auftreten. Wenn ein Gateway gelöscht wird, gibt es keine Möglichkeit, es wiederherzustellen.

4. Vergewissern Sie sich, dass Sie die angegebenen Gateways löschen möchten, geben Sie dann das Wort löschen in das Bestätigungsfeld ein und wählen Sie Löschen aus.
5. (Optional) Wenn Sie Feedback zu Ihrem gelöschten Gateway geben möchten, füllen Sie das Feedback-Dialogfeld aus und wählen Sie dann Absenden. Wählen Sie andernfalls Überspringen aus.

> **Important**
>
> Sie bezahlen nach dem Löschen eines Gateways keine Gebühren mehr für die Software, jedoch bleiben Ressourcen wie virtuelle Bänder, Amazon Elastic Block Store (Amazon EBS)-Snapshots und Amazon-EC2-Instances bestehen. Diese Ressourcen werden Ihnen weiterhin berechnet. Sie können Amazon-EC2-Instances und Amazon EBS-Snapshots entfernen, indem Sie Ihr Amazon-EC2-Abonnement kündigen. Wenn Sie Ihr Amazon-EC2-Abonnement behalten möchten, können Sie Ihre Amazon-EC2-Snapshots mithilfe der Amazon-EC2-Konsole löschen.

Entfernen von Ressourcen von einem lokal bereitgestellten Gateway

Anhand der folgenden Anweisungen können Sie Ressourcen von einem Gateway entfernen, das lokal bereitgestellt wird.

Entfernen von Ressourcen von einem auf einer VM bereitgestellten Volume Gateway

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

- Löschen Sie das Gateway. Detaillierte Anweisungen finden Sie unter Löschen eines Gateways mithilfe der Storage-Gateway-Konsole.

- Löschen Sie alle Amazon EBS-Snapshots, die Sie nicht benötigen. Anweisungen finden Sie unter Löschen eines Amazon EBS-Snapshots im Amazon EC2 EC2-Benutzerhandbuch.

Entfernen von Ressourcen von einem auf einer Amazon-EC2-Instance bereitgestellten Gateway

Wenn Sie ein Gateway löschen möchten, das Sie auf einer Amazon EC2 EC2-Instance bereitgestellt haben, empfehlen wir Ihnen, die AWS Ressourcen zu bereinigen, die mit dem Gateway verwendet wurden, insbesondere die Amazon EC2 EC2-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 auf Amazon EC2 bereitgestellten Cached-Volumes

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

1. Löschen Sie das Gateway in der Storage-Gateway-Konsole wie unter Löschen eines Gateways mithilfe der Storage-Gateway-Konsole gezeigt.
2. Stoppen Sie in der Amazon-EC2-Konsole die EC2-Instance, wenn Sie die Instance erneut verwenden möchten. Andernfalls beenden Sie die Instance. Wenn Sie das Löschen von Volumes planen, notieren Sie sich die Blockgeräte, die der Instance zugeordnet sind, sowie die Geräte-IDs, bevor Sie die Instance beenden. Diese benötigen Sie zur Identifizierung der Volumes, die Sie löschen möchten.
3. Entfernen Sie in der Amazon-EC2-Konsole alle Amazon-EBS-Volumes, die der Instance zugeordnet sind, wenn Sie sie nicht erneut verwenden möchten. Weitere Informationen finden Sie unter Clean Up Your Instance and Volume im Amazon EC2 EC2-Benutzerhandbuch.

Durchführung von Wartungsaufgaben über die lokale Konsole

Dieser Abschnitt enthält die folgenden Themen, die Informationen zur Durchführung von Wartungsaufgaben mit 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 VMware-, Hyper-V- oder Linux-KVM-Virtualisierungshost auf die lokale Konsole zu. Bei Amazon EC2 EC2-Gateways greifen Sie auf die Konsole zu, indem Sie sich über SSH mit der Amazon EC2 EC2-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 die lokale Konsole verwenden, um grundlegende Einrichtungsaufgaben und erweiterte Konfigurationsaufgaben für ein lokales Gateway durchzuführen, z. B. einen HTTP-Proxy zu konfigurieren, den Status der Systemressourcen anzuzeigen oder Terminalbefehle auszuführen.
- Ausführen von Aufgaben in der lokalen Amazon-EC2-Konsole- Erfahren Sie, wie Sie sich bei der lokalen Konsole anmelden, um grundlegende Einrichtungsaufgaben und erweiterte Konfigurationsaufgaben für ein Amazon EC2 EC2-Gateway durchzuführen, z. B. einen HTTP-Proxy zu konfigurieren, den Status der Systemressourcen anzuzeigen oder Terminalbefehle auszuführen.

Zugreifen auf die lokale 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 Volume Gateway-Konsole 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 Volume Gateway-Konsole 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 Volume Gateway-Konsole 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 Volume 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 Volume 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 Volume Gateway anmelden

Sobald Sie sich an die VM anmelden können, wird der Anmeldebildschirm angezeigt. Wenn Sie sich zum ersten Mal an der lokalen Konsole der VM anmelden, verwenden Sie die temporären Anmeldeinformationen, um sich anzumelden. Mit diesen temporären Anmeldeinformationen haben Sie Zugriff auf Menüs, in denen Sie die Gateway-Netzwerkeinstellungen konfigurieren und das Passwort von der lokalen Konsole aus ändern können. Der ursprüngliche Benutzername lautet `admin` und das temporäre Passwort lautet`password`. Sie müssen das Passwort bei der ersten Anmeldung ändern.

Um das temporäre Passwort zu ändern

1. Geben Sie im Hauptmenü AWS Geräteaktivierung — Konfiguration die entsprechende Zahl für die Gateway-Konsole ein.
2. Führen Sie den Befehl `passwd` aus. Weitere Informationen zum Ausführen des Befehls finden Sie unter Storage-Gateway-Befehle in der lokalen Konsole für ein lokales Gateway ausführen.

> **Important**
>
> Bei älteren Versionen von Volume Gateway 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.

Einstellen des Kennworts für die lokale Konsole von der Storage Gateway Gateway-Konsole aus

Sie können das Passwort der lokalen Konsole auch über die webbasierte Storage Gateway Gateway-Konsole verwalten. Alle erfolgreichen Kennwortaktualisierungen, die mit der webbasierten Konsole vorgenommen wurden, setzen das von der lokalen Konsole der Gateway-VM verwendete Passwort außer Kraft, einschließlich des temporären Passworts, falls Sie sich noch nie lokal angemeldet haben. Wenn das Gateway derzeit nicht über das Netzwerk erreichbar ist, schlägt die Kennwortaktualisierung fehl.

So legen Sie das Passwort für die lokale Konsole auf der Storage-Gateway-Konsole fest

1. Öffnen Sie die Storage Gateway Gateway-Konsole https://console.aws.amazon.com/storagegateway/zu Hause.
2. Wählen Sie im Navigationsbereich Gateways und anschließend das Gateway aus, für das Sie ein neues Passwort einrichten möchten.
3. Wählen Sie im Menü Actions (Aktionen) die Option Set Local Console Password (Passwort für lokale Konsole einrichten) aus.
4. Geben Sie in das Dialogfeld Set Local Console Password (Passwort für lokale Konsole einrichten) ein neues Passwort ein, bestätigen Sie das Passwort und wählen Sie anschließend Save (Speichern).

   Ihr neues Passwort ersetzt das aktuelle Passwort. Storage Gateway speichert, speichert oder protokolliert das Passwort nicht, sondern überträgt es stattdessen sicher über einen verschlüsselten Kanal an die VM, wo es sicher gespeichert wird.

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	

Zur Ausführung dieser Aufgabe	Vorgehensweise
	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	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. Eine Liste der Adapternamen wird angezeigt, und Sie werden aufgefordert, einen Adapternamen einzugeben, z. B. **`eth0`**. Wenn der von Ihnen angegebene Adapter verwendet wird, werden die folgenden Informationen zum Adapter angezeigt: • Media Access Control-Adresse (MAC) • IP-Adresse • Netzmaske • Gateway-IP-Adresse • DHCP-aktivierter Status

Zur Ausführung dieser Aufgabe	Vorgehensweise
	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	Description
[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.
IP6-Tabellen	Administrationstool für IPv6 Paketfilterung und NAT.
ncport	Testen Sie die Konnektivität zu einem bestimmten TCP-Port in einem Netzwerk.
nping	Sammeln Sie die Ausgaben von nping zur Netzwerkfehlerbehebung.
open-support-channel	Connect zum AWS Support her.
passwd	Aktualisieren Sie die Authentifizierungstoken.
save-iptables	IP-Tabellen speichern.
save-routing-table	Speichern Sie den neu hinzugefügten Eintrag in der Routingtabelle.

Befehl	Funktion
sslcheck	Gibt die Ausgabe mit dem Zertifikatsaussteller zurück **Note** Storage Gateway verwendet die Überprüfung durch den Zertifikatsaussteller und unterstützt keine SSL-Inspektion. Wenn dieser Befehl einen anderen Aussteller als aws-appliance@amazon.com zurückgibt, ist es wahrscheinlich, dass eine Anwendung eine SSL-Inspektion durchführt. In diesem Fall empfehlen wir, die SSL-Inspektion für die Storage Gateway Gateway-Appliance zu umgehen.
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	Description
[OK]	Die Ressource hat die Systemressourcenprüfung bestanden.
[WARNING] ([WARNUNG])	Die Ressource erfüllt nicht die empfohlenen Anforderungen, aber das Gateway ist weiterhin funktionsfähig. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.
[FAIL] ([FEHLGESCHLAGEN])	Die Ressource erfüllt nicht die Mindestanforderungen. Das Gateways funktioniert möglicherweise nicht ordnungsgemäß. Storage Gateway zeigt eine Meldung mit einer Beschreibung der Ergebnisse der Ressourcenprüfung an.

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

Ausführen von Aufgaben in der lokalen Amazon-EC2-Konsole

Einige Storage Gateway Gateway-Wartungsaufgaben erfordern, dass Sie sich bei der lokalen Gateway-Konsole für ein Gateway anmelden, das Sie auf einer Amazon EC2 EC2-Instance bereitgestellt haben. Sie können mit einem Secure Shell (SSH) -Client auf die lokale Gateway-Konsole auf Ihrer Amazon EC2 EC2-Instance zugreifen. In den Themen in diesem Abschnitt wird beschrieben, wie Sie sich bei der lokalen Gateway-Konsole anmelden und Wartungsaufgaben ausführen.

Topics

- Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways- Erfahren Sie, wie Sie Ihre Amazon EC2 EC2-Instance mithilfe eines Secure Shell (SSH) -Clients mit der lokalen Gateway-Konsole verbinden und sich dort anmelden können.
- Weiterleitung des auf EC2 bereitgestellten Gateways 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 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.

Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways

Sie können über einen Secure Shell (SSH)-Client eine Verbindung mit der Amazon-EC2-Instance herstellen. Detaillierte Informationen finden Sie unter Verbinden mit der Instance im Amazon-EC2-Benutzerhandbuch. Für diese Art des Verbindungsaufbaus benötigen Sie das SSH-Schlüsselpaar, das Sie beim Starten der Instance angegeben haben. Weitere Informationen über Amazon-EC2-Schlüsselpaare finden Sie unter Amazon-EC2-Schlüsselpaare im Amazon- EC2- Benutzerhandbuch.

So melden Sie sich bei der lokalen Konsole des Gateways an

1. Melden Sie sich bei der lokalen Konsole an. Wenn Sie auf einem Windows-Computer eine Verbindung zu Ihrer EC2-Instance herstellen, melden Sie sich als admin an.
2. Nach der Anmeldung wird das Hauptmenü AWS Storage Gateway – Konfiguration angezeigt, wo Sie verschiedene Aufgaben ausführen können.

Für weitere Informationen zu dieser Aufgabe	Siehe folgendes Thema
Konfigurieren eines SOCKS-Proxy für Ihr Gateway	Weiterleitung des auf EC2 bereitgestellten Gateways über einen HTTP-Proxy
Testen der Netzwerkverbindung	Testen der Gateway-Netzwerkkonnektivität
Ausführen von Storage-Gateway-Konsolenbefehlen	Ausführen von Storage Gateway-Befehlen auf der lokalen Konsole
Anzeigen einer Systemressourcenprüfung	Anzeigen des Gateway-Systemressourcen-Status.

Wenn Sie das Gateway beenden möchten, geben Sie **0** ein.

Zum Beenden der Konfigurationssitzung geben Sie **X** ein.

Weiterleitung des auf EC2 bereitgestellten Gateways über einen HTTP-Proxy

Storage Gateway unterstützt die Konfiguration einer Socket Secure-Proxy Version 5 (SOCKS5) zwischen dem auf Amazon EC2 und AWS bereitgestellten Gateway.

Wenn das Gateway einen Proxy-Server für die Kommunikation mit dem Internet verwenden muss, müssen Sie die HTTP-Proxy-Einstellungen für das Gateway konfigurieren. Dazu geben Sie eine IP-Adresse und die Portnummer für den Host an, auf dem der Proxy ausgeführt wird. 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 Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
2. Geben Sie im Hauptmenü AWS -Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um HTTP-Proxy aktivieren auszuwählen.
3. Geben Sie im Menü AWS Appliance-Aktivierung HTTP-Proxy-Konfiguration die entsprechende Zahl für die Aufgabe ein, die Sie ausführen möchten:

   - Konfigurieren eines HTTP-Proxy konfigurieren – Sie müssen einen Hostnamen und einen Port eingeben, um die Konfiguration abzuschließen.
   - Anzeigen der aktuellen HTTP-Proxy-Konfiguration – Wenn kein HTTP-Proxy konfiguriert ist, wird die Nachricht `HTTP Proxy not configured` angezeigt. Ist ein HTTP-Proxy konfiguriert, werden der Hostname und Port des Proxys angezeigt.
   - Entfernen einer HTTP-Proxy-Konfiguration – Die Nachricht `HTTP Proxy Configuration Removed` wird angezeigt.

Testen der 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 Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
2. Geben Sie im Hauptmenü AWS -Appliance-Aktivierung – Konfiguration die entsprechende Zahl ein, um Netzwerkkonnektivität testen auszuwählen.

   Wenn Ihr Gateway bereits aktiviert wurde, beginnt der Konnektivitätstest sofort. Für Gateways, die noch nicht aktiviert wurden, müssen Sie den Endpunkttyp AWS-Region wie in den folgenden Schritten beschrieben angeben.
3. Wenn Ihr Gateway noch nicht aktiviert ist, geben Sie die entsprechende Zahl ein, um den Endpunkttyp für Ihr Gateway auszuwählen.
4. Wenn Sie den öffentlichen Endpunkttyp ausgewählt haben, geben Sie die entsprechende Zahl ein, um den Endpunkttyp auszuwählen AWS-Region , den Sie testen möchten. Unterstützte Endpunkte AWS-Regionen und eine Liste der AWS Dienstendpunkte, die Sie mit Storage

Gateway verwenden können, finden Sie unter AWS Storage Gateway Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Im Verlauf des Tests zeigt jeder Endpunkt entweder [PASSED] oder [FAILED] an, womit der Status der Verbindung wie folgt angegeben wird:

Fehlermeldung	Description
[PASSED] ([BESTANDEN)]	Storage Gateway verfügt über Netzwerkkonnektivität.
[FAILED] ([FEHLGESCHLAGEN])	Storage Gateway hat keine Netzwerkkonnektivität.

Anzeigen des Gateway-Systemressourcen-Status

Beim Starten überprüft Ihr Gateway seine virtuellen CPU-Kerne, Stamm-Volume-Größe und RAM. Er kann dann bestimmen, ob ausreichend Systemressourcen für die ordnungsgemäße Funktionsweise Ihres Gateways verfügbar sind. Sie können die Ergebnisse dieser Prüfung auf der lokalen Gateway-Konsole anzeigen.

So zeigen Sie den Status einer Systemressourcenprüfung an

1. Melden Sie sich bei der lokalen Konsole des Gateways an. Detaillierte Anweisungen finden Sie unter Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
2. Geben Sie im Hauptmenü AWS -Geräteaktivierung – Konfiguration) die entsprechende Zahl ein, um Systemressourcenprüfung anzeigen auszuwählen.

   Für jede Ressource wird [OK], [WARNING] oder [FAIL] angezeigt, was den Status der Ressource wie folgt angibt:

Fehlermeldung	Description
[OK]	Die Ressource hat die Systemressourcenprüfung bestanden.

Fehlermeldung	Description
[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 Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.
2. Geben Sie im Hauptmenü AWS -Geräteaktivierung – Konfiguration die entsprechende Zahl ein, um Gateway-Konsole auszuwählen.
3. Geben Sie in der Eingabeaufforderung der Gateway-Konsole h ein.

   Die Konsole zeigt das Menü VERFÜGBARE BEFEHLE mit den verfügbaren Befehlen an:

Befehl	Funktion
dig	Sammeln Sie die Ausgaben von dig für die DNS-Fehlerbehebung.
exit	Kehren Sie zum Konfigurationsmenü zurück.
h	Zeigen Sie die Liste der verfügbaren Befehle an.
ifconfig	Netzwerkschnittstellen anzeigen oder konfigurieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren.
ip	Routing, Geräte und Tunnel anzeigen/manipulieren. **Note** Wir empfehlen, die Netzwerk- oder IP-Einstellungen über die Storage-Gateway-Konsole oder die spezielle Menüoption der lokalen Konsole zu konfigurieren.
iptables	Administrationstool für IPv4 Paketfilterung und NAT.

Befehl	Funktion
IP6-Tabellen	Administrationstool für IPv6 Paketfilterung und NAT.
ncport	Testen Sie die Konnektivität zu einem bestimmten TCP-Port in einem Netzwerk.
nping	Sammeln Sie die Ausgaben von nping zur Netzwerkfehlerbehebung.
open-support-channel	Connect zum AWS Support her.
save-iptables	IP-Tabellen speichern.
save-routing-table	Speichern Sie den neu hinzugefügten Eintrag in der Routingtabelle.
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 Volume Gateway

In diesem Abschnitt wird die Leistung von Storage Gateway beschrieben.

Themen

- Optimierung der Gateway-Leistung

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 24 dedizierte physische CPU-Kerne
- Für ein Volume Gateway sollte Ihre Hardware die folgenden Mengen an RAM reservieren:
  - Mindestens 16 GiB reservierter RAM für Gateways mit einer Cache-Größe von bis zu 16 TiB
  - Mindestens 32 GiB reservierter RAM für Gateways mit einer Cache-Größe von 16 TiB bis 32 TiB
  - Mindestens 48 GiB reservierter RAM für Gateways mit einer Cache-Größe von 32 TiB bis 64 TiB
- Festplatte 1, die wie folgt als Gateway-Cache verwendet werden soll:
  - SSD mit einem NVMe Controller.
- Festplatte 2, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
  - SSD mit einem NVMe Controller.
- Festplatte 3, die wie folgt als Gateway-Upload-Puffer verwendet werden soll:
  - SSD mit einem NVMe Controller.
- 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 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. Eine verbesserte Festplattenleistung führt im Allgemeinen zu einem besseren Durchsatz und mehr input/output Operationen 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. .

  > **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. Durch das Hinzufügen weiterer Upload-Pufferplatten kann die Anzahl der gleichzeitigen I/O Operationen, die auf jeder einzelnen Festplatte ausgeführt werden, reduziert werden. 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.

> **Note**
>
> Ihre beobachtete Gateway-Leistung wird aufgrund anderer hier aufgelisteter einschränkender Faktoren, wie z. B. der cache/upload Pufferfestplattendurchsatz, die Anzahl der CPU-Kerne, die Gesamt-RAM-Größe oder die Bandbreite zwischen Ihrem Initiator und dem Gateway, wahrscheinlich niedriger sein als Ihre Netzwerkbandbreite. Darüber hinaus umfasst der normale Betrieb Ihres Gateways viele Maßnahmen zum

Schutz Ihrer Daten, was dazu führen kann, dass die beobachtete Leistung geringer als die Netzwerkbandbreite ist.

Ändern der Volumes-Konfiguration

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

Weitere Informationen zu diesen Metriken finden Sie unter Messung der Leistung zwischen Ihrer Anwendung und dem Gateway.

Optimieren von iSCSI-Einstellungen

Sie können die iSCSI-Einstellungen auf Ihrem iSCSI-Initiator optimieren, um eine höhere E/A-Leistung zu erzielen. Wir empfehlen die Auswahl von 256 KiB für `MaxReceiveDataSegmentLength` und `FirstBurstLength` sowie von 1 MiB für `MaxBurstLength`. Weitere Hinweise zum Konfigurieren von iSCSI-Einstellungen finden Sie unter Anpassen von iSCSI-Einstellungen.

> **Note**
>
> Diese empfohlenen Einstellungen können eine insgesamt bessere Leistung ermöglichen. Die spezifischen iSCSI-Einstellungen, die zur Leistungsoptimierung erforderlich sind, variieren jedoch je nach verwendeter Backup-Software. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Backup-Software.

Hinzufügen von Ressourcen zu Ihrer Anwendungsumgebung

Erhöhen der Bandbreite zwischen Ihrem Anwendungsserver und Ihrem Gateway

Die Verbindung zwischen Ihrem iSCSI-Initiator und dem Gateway kann die Upload- und Download-Leistung einschränken. Wenn Ihr Gateway eine deutlich schlechtere Leistung als erwartet aufweist und Sie die Anzahl der CPU-Kerne und den Festplattendurchsatz bereits verbessert haben, sollten Sie Folgendes in Betracht ziehen:

- Rüsten Sie Ihre Netzwerkkabel auf, um eine höhere Bandbreite zwischen Ihrem Initiator und dem Gateway zu erreichen.

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

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

Hinzufügen von CPU-Ressourcen zu Ihrer Anwendungsumgebung

Wenn Ihre Anwendung zusätzliche CPU-Ressourcen verwenden kann, CPUs kann das Hinzufügen weiterer CPU-Ressourcen dazu beitragen, dass Ihre Anwendung ihre I/O Auslastung 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
- Konformitätsprüfung für AWS Storage Gateway
- Resilienz im AWS Storage Gateway
- Infrastruktursicherheit im AWS Storage Gateway
- AWS Bewährte Methoden im Bereich Sicherheit
- Einloggen und Überwachen AWS Storage Gateway

Datenschutz in AWS Storage Gateway

Das AWS Modell der gilt für den Datenschutz in AWS Storage Gateway. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme ausgeführt AWS Cloud werden. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit 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 SDKs AWS-Services verwenden. AWS CLI Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung 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?

Konfigurieren der CHAP-Authentifizierung für Ihre Volumes

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

So konfigurieren Sie CHAP-Anmeldeinformationen

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

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

Anzeigen und Bearbeiten von CHAP-Anmeldeinformationen

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

So fügen Sie CHAP-Anmeldeinformationen hinzu

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

So entfernen Sie CHAP-Anmeldeinformationen

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

So aktualisieren Sie CHAP-Anmeldeinformationen

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

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

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung bei Identität und Zugriff auf AWS Storage Gateway).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert AWS Storage Gateway mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für Storage Gateway).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-

Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert AWS Storage Gateway mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf AWS SGW verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen mit SGW verwendet werden können. AWS

IAM-Funktionen, die Sie mit AWS Storage Gateway verwenden können

IAM-Feature	AWS SGW-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

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

Identitätsbasierte Richtlinien für SGW AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für SGW AWS

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

Ressourcenbasierte Richtlinien innerhalb von SGW AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Aktionen für SGW AWS

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS SGW-Aktionen finden Sie unter Von AWS Storage Gateway definierte Aktionen in der Service Authorization Reference.

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

```
sgw
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

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

Politische Ressourcen für SGW AWS

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS SGW-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von AWS Storage Gateway definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Storage Gateway definierte Aktionen.

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

Bedingungsschlüssel für Richtlinien für SGW AWS

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS SGW-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Storage Gateway in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Storage Gateway definierte Aktionen.

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

ACLs AWS in SGW

Unterstützt ACLs: Nein

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

ABAC mit SGW AWS

Unterstützt ABAC (Tags in Richtlinien): Teilweise

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

Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, um Operationen zu ermöglichen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit SGW AWS

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Zugriffssitzungen für AWS SGW weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

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

Servicerollen für SGW AWS

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern

und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS SGW-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AWS SGW Sie dazu anleitet.

Servicebezogene Rollen für SGW AWS

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Storage Gateway

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS SGW-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS SGW definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Storage Gateway in der Service Authorization Reference.

Themen

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

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS SGW-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON)

und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der SGW-Konsole AWS

Um auf die AWS Storage Gateway Gateway-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS SGW-Ressourcen in Ihrem AWS-Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS SGW-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS SGW `ConsoleAccess` - oder `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der 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, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS SGW diese Funktionen unterstützt, finden Sie unter. So funktioniert AWS Storage Gateway mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsprüfung für AWS Storage Gateway

Externe Prüfer bewerten die Sicherheit und Konformität von AWS Storage Gateway im Rahmen mehrerer AWS Compliance-Programme. Dazu gehören SOC, PCI, ISO, FedRAMP, HIPAA, 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 CSPM— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen können AWS , ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Resilienz im AWS Storage Gateway

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones.

An AWS-Region ist ein physischer Standort auf der ganzen Welt, an dem Rechenzentren gebündelt sind. Jede Gruppe logischer Rechenzentren wird als Availability Zone (AZ) bezeichnet. Jedes AWS-Region besteht aus mindestens drei isolierten und physisch getrennten Einheiten AZs innerhalb eines geografischen Gebiets. Im Gegensatz zu anderen Cloud-Anbietern, die eine Region häufig als ein einzelnes Rechenzentrum definieren, AWS-Region bietet das Design mit mehreren AZ-Anschlüssen deutliche Vorteile. Jede AZ verfügt über unabhängige Stromversorgung, Kühlung und physische Sicherheit und ist über redundante ultra-low-latency Netzwerke verbunden. Wenn

Ihre Bereitstellung einen Schwerpunkt auf Hochverfügbarkeit erfordert, können Sie Dienste und Ressourcen so konfigurieren, dass mehrere Dienste und Ressourcen verfügbar sind, AZs um eine höhere Fehlertoleranz zu erreichen.

AWS-Regionen erfüllen die höchsten Standards in Bezug auf Infrastruktursicherheit, Compliance und Datenschutz. Der gesamte Verkehr zwischen beiden AZs ist verschlüsselt. Die Netzwerkleistung reicht aus, um eine synchrone Replikation zwischen AZs zu erreichen. AZs vereinfacht die Partitionierung von Diensten und Ressourcen für hohe Verfügbarkeit. Wenn Ihre Bereitstellung übergreifend partitioniert ist AZs, sind Ihre Ressourcen besser isoliert und vor Problemen wie Stromausfällen, Blitzeinschlägen, Tornados, Erdbeben und mehr geschützt. AZs sind physisch durch eine nennenswerte Entfernung von allen anderen AZ getrennt, obwohl sich alle innerhalb von 100 km (60 Meilen) voneinander befinden.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur 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.
- Verwenden Sie AWS Backup es, um Ihre Volumes zu sichern. Weitere Informationen finden Sie unter Sicherung Ihrer Volumes.
- Klonen Sie Ihr Volume von einem Wiederherstellungspunkt aus. Weitere Informationen finden Sie unter Klonen eines zwischengespeicherten Volumes von einem Recovery Point.

Infrastruktursicherheit im 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 unterVerwaltung von Gateway-Updates.

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, Volumes, Hochverfügbarkeit, Datenwiederherstellung und Snapshots. Die Informationen zur Fehlerbehebung bei lokalen Gateways beziehen sich auf Gateways, die auf unterstützten Virtualisierungsplattformen bereitgestellt werden. Die Informationen zur Fehlerbehebung bei Hochverfügbarkeitsproblemen beziehen sich auf Gateways, die auf der VMware vSphere High Availability (HA) -Plattform ausgeführt werden.

Topics

- Fehlerbehebung: Gateway-Offline-Probleme- Erfahren Sie, wie Sie Probleme diagnostizieren, die dazu führen können, dass Ihr Gateway in der Storage Gateway Gateway-Konsole als offline angezeigt wird.
- 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.
- Fehlerbehebung bei 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.
- Fehlerbehebung bei Volume-Problemen- Hier finden Sie Informationen zu den häufigsten Problemen, die bei der Arbeit mit Volumes auftreten können, und zu den Maßnahmen, die wir Ihnen zur Behebung dieser Probleme empfehlen.
- 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 zur 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.

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 Amazon EC2 EC2-Instance bereitgestellt werden, ob die Ports in der Sicherheitsgruppe der Instance geöffnet sind. Um zu überprüfen, ob die Ports geöffnet sind, führen Sie auf dem öffentlichen Endpunkt von einem Server aus einen Telnet-Befehl aus. Dieser Server muss sich im selben Subnetz wie das Gateway befinden. Mit den folgenden Telnet-Befehlen wird beispielsweise die Verbindung zu Port 443 getestet:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
```

```
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Um zu überprüfen, ob das Gateway selbst den Endpunkt erreichen kann, greifen Sie auf die lokale VM-Konsole des Gateways zu (für lokal bereitgestellte Gateways). Oder Sie können eine SSH-Verbindung zur Gateway-Instance herstellen (für Gateways, die auf Amazon EC2 bereitgestellt werden). Führen Sie dann einen Netzwerkverbindungstest durch. Vergewissern Sie sich, dass der Test zurückkehrt`[PASSED]`. Weitere Informationen finden Sie unter Testen Ihrer Gateway-Verbindung zum 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. Weitere Informationen finden Sie unter .

Die Option System Time Management ist auf Gateways, die auf Amazon EC2 EC2-Instances gehostet werden, nicht verfügbar. Um sicherzustellen, dass Amazon EC2 EC2-Gateways die Zeit ordnungsgemäß synchronisieren können, stellen Sie sicher, dass die Amazon EC2 EC2-Instance über die Ports UDP und TCP 123 eine Verbindung zur folgenden NTP-Serverpool-Liste herstellen kann:

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

Beheben Sie Fehler bei der Aktivierung Ihres Gateways über einen Amazon VPC-Endpunkt

Um Aktivierungsfehler bei der Aktivierung Ihres Gateways über einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt zu beheben, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Überprüfen Sie die erforderlichen Ports

Stellen Sie sicher, dass die erforderlichen Ports innerhalb Ihrer lokalen Firewall (für lokal bereitgestellte Gateways) oder Sicherheitsgruppe (für in Amazon EC2 bereitgestellte Gateways) geöffnet sind. Die Ports, die für die Verbindung eines Gateways mit einem Storage Gateway Gateway-VPC-Endpunkt erforderlich sind, unterscheiden sich von denen, die für die Verbindung eines Gateways mit öffentlichen Endpunkten erforderlich sind. Die folgenden Ports sind für die Verbindung mit einem Storage Gateway Gateway-VPC-Endpunkt erforderlich:

- TCP 443

- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Weitere Informationen finden Sie unter 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. Weitere Informationen finden Sie unter .

Die Option System Time Management ist auf Gateways, die auf Amazon EC2 EC2-Instances gehostet werden, nicht verfügbar. Um sicherzustellen, dass Amazon EC2 EC2-Gateways die Zeit ordnungsgemäß synchronisieren können, stellen Sie sicher, dass die Amazon EC2 EC2-Instance über die Ports UDP und TCP 123 eine Verbindung zur folgenden NTP-Serverpool-Liste herstellen kann:

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

Suchen Sie nach einem HTTP-Proxy und bestätigen Sie die zugehörigen Sicherheitsgruppeneinstellungen

Prüfen Sie vor der Aktivierung, ob Sie einen HTTP-Proxy auf Amazon EC2 auf der lokalen Gateway-VM als Squid-Proxy auf Port 3128 konfiguriert haben. Bestätigen Sie in diesem Fall Folgendes:

- Die Sicherheitsgruppe, die an den HTTP-Proxy auf Amazon EC2 angehängt ist, muss über eine Regel für eingehenden Datenverkehr verfügen. Diese Regel für eingehenden Datenverkehr muss Squid-Proxyverkehr auf Port 3128 von der IP-Adresse der Gateway-VM aus zulassen.
- Die Sicherheitsgruppe, die dem Amazon EC2 VPC-Endpunkt zugeordnet ist, muss Regeln für eingehenden Datenverkehr haben. Diese Regeln für eingehenden Datenverkehr müssen den Verkehr auf den Ports 1026-1028, 1031, 2222 und 443 von der IP-Adresse des HTTP-Proxys auf Amazon EC2 zulassen.

Beheben Sie Fehler, wenn Sie Ihr Gateway über einen öffentlichen Endpunkt aktivieren und es in derselben VPC einen Storage Gateway Gateway-VPC-Endpunkt gibt

Um Fehler bei der Aktivierung Ihres Gateways über einen öffentlichen Endpunkt zu beheben, wenn sich in derselben VPC ein Amazon Virtual Private Cloud (Amazon VPC) -Endpoint befindet, führen Sie die folgenden Prüfungen und Konfigurationen durch.

Vergewissern Sie sich, dass die Einstellung Privaten DNS-Namen aktivieren auf Ihrem Storage Gateway Gateway-VPC-Endpunkt nicht aktiviert ist

Wenn Enable Private DNS Name aktiviert ist, können Sie keine Gateways von dieser VPC zum öffentlichen Endpunkt aktivieren.

So deaktivieren Sie die Option für private DNS-Namen:

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, um Ihnen bei der Behebung von Problemen mit Ihrem Gateway Support zu helfen.

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. • Das SSL-Zertifikat validation/inspection sollte nicht aktiviert sein. Storage Gateway verwendet eine gegenseitige TLS-Authentifizierung, die fehlschlagen würde, wenn eine Drittanbieteranwendung versucht, eines der Zertifikate zu intercept/sign erhalten. • Falls Sie den Netzwerkdatenverkehr mithilfe einer Firewall oder eines Routers filtern oder einschränken, müssen Sie die Firewall und den Router so konfigurieren, dass diese Service-Endpunkte für die ausgehende Kommunikation mit AWS verwendet werden dürfen. Weitere Informationen zum Netzwerk und Firewall-Anforderungen finden Sie unter Netzwerk- und Firewall-Anforderungen.
Die Aktivierung des Gateways schlägt fehl,	• Überprüfen Sie, dass auf die Gateway-VM zugegriffen werden kann, indem Sie die VM Ihres Clients anpingen.

Problem	Maßnahme
wenn Sie in der Storage-Gateway-Managementk onsole auf die Schaltflä che Weiter zur Aktivierung klicken.	• Stellen Sie sicher, dass Ihre VM eine Netzwerkverbindung zum Internet hat. Andernfalls müssen Sie die Konfiguration eines SOCKS-Proxy vornehmen. Weitere Informationen zur Verfahren sweise finden Sie unter 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 automatis ch 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. • Das SSL-Zertifikat validation/inspection sollte nicht aktiviert sein. Storage Gateway verwendet eine gegenseitige TLS-Authentifizier ung, die fehlschlagen würde, wenn eine Drittanbieteranwendung versucht, eines der Zertifikate zu intercept/sign erhalten. • 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 Anforderungen für die Einrichtung von Volume 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 zwischen Ihrem Gateway und verbessern, AWS indem Sie Ihre Internetverbindung AWS auf einem Netzwerkadapter (NIC) einrichten, der von dem Netzwerkadapter (NIC) getrennt ist, der Ihre Anwendungen und die Gateway-VM verbindet. Dieser Ansatz ist nützlich, wenn Sie eine Verbindung mit hoher Bandbreite haben AWS und Bandbreitenkonflikte vermeiden möchten, insbesondere bei einer Snapshot-Wiederherstellung. Für Workloads mit hohem Durchsatz können Sie Direct Connect verwenden, um eine dedizierte Netzwerkverbindung zwischen dem lokalen Gateway und AWS herzustellen. Verwenden Sie die `CloudBytesUploaded` Metriken `CloudBytesDownloaded` und des Gateways AWS, um die Bandbreite der Verbindung von Ihrem Gateway zu zu messen. Weitere Informationen zu diesem Thema finden Sie unter Messung der Leistung zwischen Ihrem 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 Informationen zur Messung des Durchsatzes zu und von Ihrem Gateway und AWS finden Sie unter Messung der Leistung zwischen Ihrem 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 Fehlerbehebung weiterhelfen Support können.
6. Wenn die Supportsitzung beendet ist, geben Sie **`q`** ein, um sie zu beenden. Schließen Sie die Sitzung erst, wenn Sie vom Amazon Web Services Support darüber informiert werden, dass die Support-Sitzung abgeschlossen ist.
7. Geben Sie 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` 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 Anforderungen für die Einrichtung von Volume 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 Anforderungen für die Einrichtung von Volume 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.

Fehlerbehebung bei Problemen mit Amazon-EC2-Gateway

In den folgenden Abschnitten werden typische Probleme beschrieben, die bei der Arbeit mit dem auf Amazon EC2 bereitgestellten Gateway auftreten können. Weitere Informationen über den Unterschied zwischen einem On-Premises-Gateway und einem Gateway, das auf Amazon EC2 bereitgestellt ist, finden Sie unter Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume Gateway bereit.

Themen

- Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.
- EC2-Gateway-Instance in der Instance-Liste nicht gefunden
- Sie haben ein Amazon-EBS-Volume erstellt, können es aber nicht an die EC2-Gateway-Instance anfügen
- Sie können keinen Initiator an ein Volume-Ziel auf dem EC2-Gateway anfügen
- Beim Hinzufügen von Speicher-Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind
- Sie möchten einen als Upload-Pufferspeicher zugewiesenen Datenträger entfernen, um die Größe des Upload-Pufferspeichers zu reduzieren

- Durchsatz zum oder vom EC2-Gateway sinkt auf Null
- Sie Support möchten bei der Fehlerbehebung Ihres EC2-Gateways helfen
- Sie möchten sich mit Ihrer Gateway-Instance über die serielle Amazon-EC2-Konsole verbinden

Die Aktivierung Ihres Gateways ist nach einigen Momenten nicht erfolgt.

Prüfen Sie in der Amazon-EC2-Konsole Folgendes:

- Port 80 ist in der Sicherheitsgruppe aktiviert, die Sie mit der Instance verknüpft haben. Weitere Informationen zum Hinzufügen einer Sicherheitsgruppenregel finden Sie unter Hinzufügen einer Sicherheitsgruppenregel im Amazon EC2 EC2-Benutzerhandbuch.
- Die Gateway-Instance ist als laufend markiert. In der Amazon-EC2-Konsole für die Instance sollte der State-Wert der Instance RUNNING lauten.
- Stellen Sie sicher, dass der Typ der Amazon-EC2-Instance die unter Speicheranforderungen beschriebenen Mindestanforderungen erfüllt.

Versuchen Sie erneut, das Gateway zu aktivieren, nachdem Sie das Problem behoben haben. Öffnen Sie dazu die Storage-Gateway-Konsole, wählen Sie Neues Gateway auf Amazon EC2 bereitstellen aus und geben Sie die IP-Adresse der Instance erneut ein.

EC2-Gateway-Instance in der Instance-Liste nicht gefunden

Wenn Sie die Instance nicht mit einem Ressourcen-Tag versehen haben und viele Instances ausführt werden, ist es schwierig, die von Ihnen gestarteten Instances zu benennen. In diesem Fall können Sie die folgenden Aktionen ausführen, um die Gateway Instance zu finden:

- Prüfen Sie den Namen des Amazon Machine Image (AMI) auf der Registerkarte Description (Beschreibung) der Instance. Eine Instance auf der Grundlage der Storage Gateway AMI muss mit dem Text **`aws-storage-gateway-ami`** beginnen.
- Wenn Sie über mehrere Instances verfügen, die auf der Storage Gateway AMI basieren, prüfen Sie die Startzeit der Instance, um die richtige Instance zu finden.

Sie haben ein Amazon-EBS-Volume erstellt, können es aber nicht an die EC2-Gateway-Instance anfügen

Stellen Sie sicher, dass sich dieses Amazon-EBS-Volume in derselben Availability Zone wie die Gateway-Instance befindet. Falls eine Abweichung in den Availability Zones besteht, erstellen Sie ein neues Amazon-EBS-Volume, das sich in derselben Availability Zone wie die Instance befindet.

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

Stellen Sie sicher, dass die Sicherheitsgruppe, mit der Sie die Instance gestartet haben, eine Regel enthält, die den Port zulässt, den Sie für den iSCSI-Zugriff verwenden. Der Port wird in der zu 3260 festgesetzt. Weitere Informationen zum Verbinden zu Volumes finden Sie unter Von einem Windows-Client aus eine Verbindung zu Ihren Volumes herstellen.

Beim Hinzufügen von Speicher-Volumes erhalten Sie die Meldung, dass keine Datenträger verfügbar sind

Für ein neu aktiviertes Gateway ist kein Volume-Speicher definiert. Bevor Sie Volume-Speicher definieren können, müssen Sie die lokale Festplatten zum Gateway zuweisen, die Sie als Upload-Puffer und Cache-Speicher verwenden. Für ein Gateway, das auf Amazon EC2 bereitgestellt ist, entsprechen die lokalen Datenträger Amazon-EBS-Volumes, die an die Instance angefügt sind. Dieser Fehler tritt wahrscheinlich auf, weil keine Amazon-EBS-Volumes für die Instance definiert sind.

Prüfen Sie Block-Geräte, die für die Instance definiert sind, die das Gateway ausführt. Wenn es nur zwei Block-Geräte (Geräte mit der Standard-AMI) gibt, dann sollten Sie Speicher hinzufügen. Weitere Informationen zur Verfahrensweise finden Sie unter Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume 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.

Durchsatz zum oder vom EC2-Gateway sinkt auf Null

Verifizieren Sie, dass die Gateway-Instance ausgeführt wird. Wenn die Instance gestartet wird, z. B. durch einen Neustart, warten Sie, bis die Instance neu gestartet ist.

Verifizieren Sie außerdem, dass sich die Gateway-IP-Adresse nicht geändert hat. Wenn die Instance beendet wurde und anschließend neu gestartet wurde, hat sich die IP-Adresse der Instance möglicherweise geändert. In diesem Fall müssen Sie ein neues Gateway aktivieren.

Sie können den Durchsatz zu und von Ihrem Gateway 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 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 aktivieren diesen Zugriff über die lokale Amazon-EC2-Konsole. Sie melden sich über Secure Shell (SSH) bei der lokalen Amazon-EC2-Konsole an. Für eine erfolgreiche Anmeldung über SSH, muss die Sicherheitsgruppe Ihrer Instance über eine Regel verfügen, die den TCP-Port 22 öffnet.

> **Note**
>
> Wenn Sie eine neue Regel zu einer vorhandenen Sicherheitsgruppe hinzufügen, gilt die neue Regel für alle Instances, die diese Sicherheitsgruppe nutzen. Weitere Informationen zu Sicherheitsgruppen und zum Hinzufügen einer Sicherheitsgruppenregel finden Sie unter Amazon-EC2-Sicherheitsgruppen im Amazon-EC2-Benutzerhandbuch.

Um eine Support Verbindung zu Ihrem Gateway herzustellen, melden Sie sich zunächst bei der lokalen Konsole für die Amazon EC2 EC2-Instance an, navigieren zur Storage Gateway-Konsole und gewähren dann den Zugriff.

Um den Support Zugriff auf ein Gateway zu aktivieren, das auf einer Amazon EC2 EC2-Instance bereitgestellt wird

1. Melden Sie sich bei der lokalen Konsole für Ihre Amazon-EC2-Instance an. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Instance im Amazon-EC2-Benutzerhandbuch.

   Sie können den folgenden Befehl verwenden, um sich bei der lokalen EC2-Konsole der Instance anzumelden.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > Das *PRIVATE-KEY* ist die `.pem` Datei, die das private Zertifikat des EC2-Schlüsselpaars enthält, das Sie zum Starten der Amazon EC2 EC2-Instance verwendet haben. Weitere Informationen finden Sie unter Abrufen des öffentlichen Schlüssels für Ihr Schlüsselpaar im Amazon-EC2-Benutzerhandbuch.
   > Das *INSTANCE-PUBLIC-DNS-NAME* ist der öffentliche DNS-Name (Domain Name System) Ihrer Amazon EC2 EC2-Instance, auf der Ihr Gateway läuft. Sie erhalten diesen öffentlichen DNS-Namen, indem Sie die Amazon-EC2-Instance in der EC2-Konsole auswählen und auf die Registerkarte Beschreibung klicken.

2. Geben Sie an der Eingabeaufforderung **`6 - Command Prompt`** ein, um die Channel-Konsole für Support zu öffnen.
3. Geben Sie **h** ein, um das Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) zu öffnen.
4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Ihr Gateway einen öffentlichen Endpunkt verwendet, geben Sie im Fenster VERFÜGBARE BEFEHLE **`open-support-channel`** ein, um eine Verbindung zum Storage-Gateway-Kundensupport herzustellen. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.
   - Wenn Ihr Gateway einen VPC-Endpunkt verwendet, geben Sie im Fenster AVAILABLE COMMANDS (VERFÜGBARE BEFEHLE) **`open-support-channel`** ein. Wenn Ihr Gateway

nicht aktiviert ist, geben Sie den VPC-Endpunkt oder die IP-Adresse ein, für die eine Verbindung mit dem Storage-Gateway-Kundensupport hergestellt werden soll. Geben Sie TCP-Port 22 frei, damit Sie einen Support-Kanal für AWSöffnen können. Wenn Sie eine Verbindung mit dem Kunden-Support herstellen, weist Ihnen Storage Gateway eine Support-Nummer zu. Notieren Sie sich Ihre Support-Nummer.

> **Note**
>
> Die Kanalnummer ist keine Portnummer (Transmission ControlProtocol/User Datagram Protocol (TCP/UDP). Stattdessen stellt das Gateway eine Secure Shell (SSH) (TCP 22)-Verbindung zu den Storage-Gateway-Servern her und stellt den Support-Kanal für die Verbindung bereit.

5. Nachdem der Support-Kanal eingerichtet wurde, geben Sie Ihre Support-Servicenummer an, Support damit wir Ihnen bei der 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 sich mit Ihrer Gateway-Instance über die serielle Amazon-EC2-Konsole verbinden

Sie können die serielle Amazon-EC2-Konsole zur Fehlerbehebung beim Booten, bei der Netzwerkkonfiguration und anderen Problemen verwenden. Anweisungen und Tipps zur Fehlerbehebung finden Sie unter Serielle Amazon-EC2-Konsole im Benutzerhandbuch zu Amazon Elastic Compute Cloud.

Fehlerbehebung bei Hardware-Appliance-Problemen

In den folgenden Themen werden Probleme, die im Zusammenhang mit der Hardware-Appliance für Storage Gateway auftreten können, sowie Lösungsvorschläge beschrieben.

Festlegen der Service-IP-Adresse nicht möglich

Wenn Sie versuchen, eine Verbindung mit Ihrem Service herzustellen, stellen Sie sicher, dass Sie die Service-IP-Adresse und nicht die Host-IP-Adresse verwenden. Konfigurieren Sie die Service-IP-Adresse in der Servicekonsole und die Host-IP-Adresse in der Hardwarekonsole. Die Hardwarekonsole wird angezeigt, wenn die Hardware-Appliance gestartet wird. Um die Servicekonsole über die Hardwarekonsole zu öffnen, wählen Sie Open Service Console (Servicekonsole öffnen).

Wie lässt sich eine Zurücksetzung auf die Werkseinstellungen durchführen?

Wenn Sie die Appliance auf die Werkseinstellungen zurücksetzen müssen, wenden Sie sich an das Hardware-Appliance-Team für Storage Gateway, um wie im folgenden Support-Abschnitt beschrieben Unterstützung zu erhalten.

Wie erfolgt der Remote-Neustart?

Wenn Sie einen Remote-Neustart Ihrer Appliance durchführen müssen, können Sie dazu die Dell iDRAC-Verwaltungsschnittstelle verwenden. Weitere Informationen finden Sie unter 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. Beispiel:

   Status: Auf Port 19599 geöffnet
3. Notieren Sie sich die Portnummer und geben Sie sie an Support.

Fehlerbehebung bei Volume-Problemen

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

Themen

- Die Konsole behauptet, dass Ihre Volume nicht konfiguriert ist
- Die Konsole gibt an, dass Ihre Volume verloren ist

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

Die Konsole behauptet, dass Ihre Volume nicht konfiguriert ist

Wenn die Storage-Gateway-Konsole angibt, dass Ihr Volume den Status UPLOAD BUFFER NOT CONFIGURED besitzt, fügen Sie Upload-Pufferkapazität zu Ihrem Gateway hinzu. Sie können ein Gateway nicht zum Speichern Ihrer Anwendungsdaten verwenden, wenn der Upload-Puffer für das Gateway nicht konfiguriert ist. Weitere Informationen finden Sie unter So konfigurieren Sie zusätzlichen Upload-Puffer oder Cache-Speicher für Ihr Gateway.

Die Konsole gibt an, dass Ihre Volume verloren ist

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

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

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

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

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

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

Die Konsole gibt an, das Ihre Volume PASS THROUGH Status hat

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

Ein Beispiel für wann Sie etwas unternehmen sollten, wenn Ihre Volume den Status PASS THROUGH hat, ist, wenn Ihr Gateway keinen Upload-Pufferspeicherplatz mehr hat. Um zu überprüfen, ob Ihr Upload-Puffer in der Vergangenheit überschritten wurde, können Sie sich die

`UploadBufferPercentUsed` Metrik in der CloudWatch Amazon-Konsole ansehen. Weitere Informationen finden Sie unterÜberwachen des Upload-Puffers. Wenn Ihr Gateway den Status PASS THROUGH aufweist, weil kein Upload-Pufferspeicher mehr verfügbar ist, sollten Sie Ihrem Gateway mehr Upload-Pufferspeicher zuweisen. Wenn Sie mehr Pufferspeicher hinzufügen, wechselt der Status Ihres Volumes von PASS THROUGH über BOOTSTRAPPING automatisch zu AVAILABLE. Während das Volume den Status BOOTSTRAPPING aufweist, liest das Gateway Daten vom Datenträger des Volumes, lädt diese Daten in Amazon S3 und holt nach Bedarf auf. Nachdem das Gateway wieder den gewünschten Status hat und die Volume-Daten in Amazon S3 gespeichert wurden, lautet der Volume-Status AVAILABLE und Snapshots können erneut gestartet werden. Beachten Sie, wenn Ihr Volume den PASS THROUGH oder BOOTSTRAPPING Status besitzt können Sie damit fortfahren, die Daten von der Volume Festplatte zu lesen und schreiben. Weitere Informationen zum Hinzufügen weiterer Upload-Pufferspeicher finden Sie unter Bestimmen der Größe des zuzuordnenden Upload-Puffers.

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

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

Selten, gibt der Status PASS THROUGH an, dass eine Festplatte die einem Upload-Puffer zugeordnet wurde fehlgeschlagen ist. In diesem Fall sollten Sie die Festplatte entfernen. Weitere Informationen finden Sie unter Arbeiten mit Volume Gateway-Speicherressourcen. Informationen zum Volume-Status finden Sie unter Grundlagen zu Status und Übergängen bei Volumes.

Sie möchten Volume-Integrität überprüfen und möglicher Fehler beheben

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

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

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

Sie möchten den iSCSI-Volumen-Zielnamen ändern

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

Ihr geplanter Volume Snapshot taucht nicht auf

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

Sie müssen eine Festplatte entfernen oder ersetzen, die ausgefallen ist

Wenn Sie einen ausgefallenen Volume-Datenträger austauschen müssen oder ein Volume entfernen möchten, weil es nicht benötigt wird, sollten Sie das Volume zuerst mithilfe der Storage-Gateway-Konsole entfernen. Weitere Informationen finden Sie unter So löschen Sie ein Volume. Anschließend verwenden Sie den Hypervisor-Client, um den Backup-Speicher zu entfernen:

- Entfernen Sie zum VMware ESXi Beispiel den Backing-Speicher, wie unter beschriebenLöschen von Speichervolumes.
- Für Microsoft Hyper-V, entfernen Sie den Backup-Speicher.

Durchsatz von Ihrer Anwendung zu einem Volume ist auf Null abgefallen

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

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

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

In 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 flüchtiger Laufwerke oder Datenträger ab.

Ein Volume Snapshot hat einen PENDING Status länger als erwartet

Wenn ein Volume-Snapshot länger als erwartet im Status PENDING bleibt, ist die Gateway-VM möglicherweise unerwartet abgestürzt oder der Status eines Volumes hat sich zu PASS THROUGH oder IRRECOVERABLE geändert. Wenn einer dieser Vorkommnisse der Fall ist, bleibt der Snapshot im PENDING Status und der Snapshot wird nicht vollständig ausgeführt. In diesen Fällen empfehlen wir, dass Sie den Snapshot löschen. Weitere Informationen finden Sie unter Löschen von Snapshots Ihrer Speichervolumes.

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

High Availability-Zustandsbenachrichtigungen

Wenn Sie Ihr Gateway auf der VMware vSphere High Availability (HA) -Plattform ausführen, erhalten Sie möglicherweise 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
- Kennzahlen

Zustandsbenachrichtigungen

Wenn Sie Ihr Gateway auf VMware vSphere HA ausführen, senden alle Gateways die folgenden Integritätsbenachrichtigungen an Ihre konfigurierte CloudWatch Amazon-Protokollgruppe. Diese Benachrichtigungen werden in einem Protokollstream mit dem Namen `AvailabilityMonitor` erfasst.

Themen

- Benachrichtigung: Reboot
- Benachrichtigung: HardReboot
- Benachrichtigung: HealthCheckFailure
- Benachrichtigung: AvailabilityMonitorTest

Benachrichtigung: Reboot

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

Maßnahme

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

Benachrichtigung: HardReboot

Sie können eine `HardReboot`-Benachrichtigung erhalten, wenn die Gateway-VM unerwartet neu gestartet wird. Ein solcher Neustart kann auf Stromausfall, einen Hardwarefehler oder ein anderes Ereignis zurückzuführen sein. Bei VMware Gateways kann ein Reset durch vSphere High Availability Application Monitoring dieses Ereignis auslösen.

Maßnahme

Wenn Ihr Gateway in einer solchen Umgebung ausgeführt wird, überprüfen Sie, ob die `HealthCheckFailure` Benachrichtigung vorhanden ist, und lesen Sie im VMware Ereignisprotokoll für die VM nach.

Benachrichtigung: HealthCheckFailure

Für ein Gateway auf VMware vSphere HA können Sie eine `HealthCheckFailure` Benachrichtigung erhalten, wenn eine Integritätsprüfung fehlschlägt und ein VM-Neustart angefordert wird. Dieses Ereignis tritt auch während eines Tests zum Überwachen der Verfügbarkeit auf, der durch die Benachrichtigung `AvailabilityMonitorTest` angezeigt wird. In diesem Fall wird die Benachrichtigung `HealthCheckFailure` erwartet.

> **Note**
>
> Diese Benachrichtigung gilt nur für VMware Gateways.

Maßnahme

Wenn dieses Ereignis wiederholt ohne die Benachrichtigung `AvailabilityMonitorTest` auftritt, überprüfen Sie die VM-Infrastruktur auf Probleme (Speicher, Arbeitsspeicher usw.). Wenn Sie zusätzliche Unterstützung benötigen, wenden Support Sie sich an.

Benachrichtigung: AvailabilityMonitorTest

Für ein Gateway auf VMware vSphere HA können Sie eine `AvailabilityMonitorTest` Benachrichtigung erhalten, wenn Sie einen Test des Verfügbarkeits- und Anwendungsüberwachungssystems in VMware ausführen.

Kennzahlen

Die Metrik `AvailabilityNotifications` ist auf allen Gateways verfügbar. Diese Metrik ist eine Zählung der Anzahl an Zustandsbenachrichtigungen im Zusammenhang mit der Verfügbarkeit, die vom Gateway generiert werden. Verwenden Sie die Statistik `Sum`, um zu beobachten, ob Ereignisse im Zusammenhang mit der Verfügbarkeit im Gateway auftreten. Einzelheiten zu den Ereignissen erhalten Sie von Ihrer konfigurierten CloudWatch Protokollgruppe.

Bewährte Methoden für Volume 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
- Reduzierung der Menge des fakturierten Speichers auf einem Volume

Bewährte Methoden: Wiederherstellung Ihrer Daten

Obwohl ist es selten vorkommt, könnte in Ihrem Gateway ein Dauerfehler aufgetreten sein. Solche Fehler können in Ihrer virtuellen Maschine (VM), im Gateway selbst, dem lokalen Speicher oder an anderer Stelle auftreten. Wenn ein Fehler auftritt, empfehlen wir, dass Sie die Anweisungen im entsprechenden Abschnitt befolgen um Ihre Daten wiederherzustellen.

> **Important**
>
> Das Wiederherstellen einer Gateway-VM von einem Snapshot, der von Ihrem Hypervisor oder aus Ihrem Amazon-EC2-Computerabbild (AMI) erstellt wurde, wird von Storage Gateway nicht unterstützt. Wenn Ihre Gateway VM, ein neues Gateway aktiviert und Ihre Daten auf diesem Gateway wiederhergestellt werden, dann folgen Sie folgenden Anweisungen.

Themen

- Wiederherstellung nach dem unerwarteten Herunterfahren einer virtuellen Maschine
- Wiederherstellen Ihrer Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM
- Wiederherstellung Ihrer Daten von einem nicht wiederherstellbaren Volume
- Wiederherstellen Ihrer Daten von einem fehlerhaften Cache-Datenträger

- Wiederherstellen Ihrer Daten von einem beschädigten Datensystem
- Wiederherstellen Ihrer Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann

Wiederherstellung nach dem unerwarteten Herunterfahren einer virtuellen Maschine

Wenn Ihr VM unerwartet heruntergefahren wird, z. B. während eines Stromausfalls, ist Ihr Gateway nicht mehr erreichbar. Wenn Strom- und Netzwerkverbindungen wiederhergestellt werden, wird Ihr Gateway erreichbar und beginnt normal zu funktionieren. Im Folgenden werden einige Schritte beschrieben, die Ihnen helfen können Ihre Daten wiederherzustellen:

- Wenn ein Ausfall dafür sorgt, dass Netzwerkverbindungs Problemen auftreten, dann können Sie diese Probleme beheben. Weitere Informationen zum Testen der Netzwerkverbindung finden Sie unter Testen Sie Ihre Gateway-Verbindung zum Internet.
- Wenn Ihr Gateway in Konfigurationen mit zwischengespeicherten Volumes erreichbar ist, werden Ihre Volumes in den BOOTSTRAPPING-Status versetzt. Diese Funktion stellt sicher, dass Ihre lokal gespeicherten Daten weiterhin mit synchronisiert werden. AWS Weitere Informationen, zu diesem Status, finden Sie unter Grundlagen zu Status und Übergängen bei Volumes.
- Wenn Ihre Gateway fehlerhaft ist und Probleme mit Ihren Volumes oder Bändern auftreten und das im Zusammenhang mit einem unerwarteten Herunterfahren steht, dann können Sie Daten wiederherstellen. Weitere Informationen dazu, wie Sie Ihre Daten wiederherstellen, finden Sie in den folgenden Abschnitten, die auf Ihren Fall passen.

Wiederherstellen Ihrer Daten von einem fehlerhafte Gateway oder einer fehlerhaften VM

Wenn Ihr Gateway oder Ihre virtuelle Maschine nicht richtig funktioniert, können Sie Daten wiederherstellen, die auf ein Volume in Amazon S3 hochgeladen AWS und dort gespeichert wurden. Für Cached-Volumes-Gateways, können Sie Daten von einem Recovery-Snapshot aus wiederherstellen. Bei Gateways für gespeicherte Volumes können Sie Daten von Ihrem letzten Amazon-EBS-Snapshot des Volumes wiederherstellen. Bei Tape Gateways stellen Sie ein oder mehrere Bänder von einem Wiederherstellungspunkt auf einem neuen Tape Gateway wieder her.

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

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

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

Wiederherstellung Ihrer Daten von einem nicht wiederherstellbaren Volume

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

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

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

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

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

Wiederherstellen Ihrer Daten von 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.

Wiederherstellen Ihrer Daten von einem beschädigten Datensystem

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

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

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

   Weitere Informationen, wie Sie einen Recovery-Snapshot erstellen, finden Sie unter Ihr Cache-Gateway ist unerreichbar und Sie möchten Ihre Daten wiederherstellen.
2. Verwenden Sie den Befehl **`fsck`**, um zu überprüfen, ob Ihr Dateisystem Fehler aufweist, und versuchen Sie, es zu reparieren.
3. Starten Sie Ihre Gateway-VM neu.
4. Wenn Ihr Hypervisor-Host anfängt zu booten, halten Sie die Umschalttaste gedrückt, um in das Grub-Boot-Menü zu gelangen.
5. Drücken Sie zum Bearbeiten im Menü **`e`**.

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

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

Wiederherstellen Ihrer Daten aus einem Rechenzentrum, auf das nicht zugegriffen werden kann

Wenn aus irgendeinem Grund nicht auf Ihr Gateway oder Rechenzentrum zugegriffen werden kann, können Sie Ihre Daten in einem anderen Gateway in einem anderen Rechenzentrum oder in einem Gateway, das auf einer Amazon-EC2-Instance gehostet ist, wiederherstellen. Wenn Sie keinen Zugriff auf ein anderes Rechenzentrum haben, empfehlen wir, das Gateway auf einer Amazon-EC2-Instance anzulegen. Die weiteren Schritte sind abhängig vom Gateway-Typ, von dem aus Sie die Daten wiederherstellen.

So stellen Sie Daten von einem Volume Gateway in einem Rechenzentrum wieder her, auf das nicht zugegriffen werden kann

1. Erstellen und aktivieren Sie ein neues Volume Gateway auf einem Amazon-EC2-Host. Weitere Informationen finden Sie unter Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume Gateway bereit.

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

2. Erstellen Sie ein neues Volume, und wählen Sie die EC2-Gateway als Ziel-Gateway. Weitere Informationen finden Sie unter Ein Speichervolume erstellen.

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

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

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

Säuberung unnötiger Ressourcen

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

So bereinigen Sie nicht benötigte Ressourcen

1. Löschen Sie alle Snapshots. Detaillierte Anweisungen finden Sie unter Löschen von Snapshots Ihrer Speichervolumes.
2. Falls Sie das Gateway nicht weiterhin verwenden möchten, löschen Sie es. Weitere Informationen 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 Amazon EC2-Instance erstellt haben, beenden Sie die Instance.

Reduzierung der Menge des fakturierten Speichers auf einem Volume

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

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

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 Volume Gateway-Speicherressourcen- Erfahren Sie mehr über Verfahren im Zusammenhang mit Volume Gateway-Speicherressourcen, z. B. das Entfernen lokaler Festplatten und das Verwalten von Amazon EBS-Volumes auf EC2 Gateway-Amazon-Instances.
- 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 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.
- IPv6 Unterstützung- Erfahren Sie mehr über die Anforderungen für IPv6.
- 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 Limits und Kontingente für Volume Gateway, einschließlich maximaler Beschränkungen für Volume-Größe und -Menge, und Empfehlungen zur lokalen Festplattengröße.

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 Appliances, die auf VMware-, Hyper-V- oder Linux-KVM ausgeführt werden, und Appliances, die auf Amazon EC2 EC2-Instances in der Cloud ausgeführt werden. AWS

Topics

- Stellen Sie einen Amazon EC2 EC2-Standardhost für Volume Gateway bereit- Erfahren Sie, wie Sie ein auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mithilfe der Standardspezifikationen bereitstellen und aktivieren.
- Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume Gateway bereit- Erfahren Sie, wie Sie ein auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mithilfe benutzerdefinierter Einstellungen bereitstellen und aktivieren.
- Metadatenoptionen Amazon EC2 EC2-Instances ändern- Erfahren Sie, wie Sie Ihre Amazon EC2 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 NTP-Server (Network Time Protocol) 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 Amazon EC2 EC2-Standardhost für Volume Gateway bereit

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

Sie können ein auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance bereitstellen und aktivieren. Das AWS Storage Gateway-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 Amazon-EC2-Instance finden Sie unter Bereitstellen einer Amazon-EC2-Instance als Host für Ihr Volume Gateway.
2. Wählen Sie Launch Instance aus, um die AWS Storage Gateway AMI-Vorlage in der Amazon EC2 EC2-Konsole zu öffnen und zusätzliche Einstellungen wie Instance-Typen, Netzwerkeinstellungen und Speicher konfigurieren anzupassen.
3. Optional können Sie in der Storage-Gateway-Konsole die Option Standardeinstellungen verwenden auswählen, um eine Amazon-EC2-Instance mit der Standardkonfiguration bereitzustellen.

   Die Amazon-EC2-Instance, die mit Standardeinstellungen verwenden erstellt wurde, hat die folgenden Standardspezifikationen:

   - Instance-Typ – m5.xlarge

- Netzwerkeinstellungen
  - Wählen Sie unter VPC die VPC aus, in der Ihre EC2-Instanz ausgeführt werden soll.
  - Geben Sie für Subnet das Subnetz an, in dem Ihre EC2-Instance gestartet werden soll.

    > **Note**
    >
    > VPC-Subnetze werden nur dann in der Drop-down-Liste angezeigt, wenn für sie die Einstellung zur automatischen Zuweisung öffentlicher IPv4 Adressen in der VPC-Managementkonsole aktiviert ist.

  - Öffentliche IP automatisch zuweisen – Aktiviert

Eine EC2-Sicherheitsgruppe wird erstellt und der EC2-Instance zugeordnet. Die Sicherheitsgruppe hat die folgenden eingehenden Regeln:

> **Note**
>
> Während der Gateway-Aktivierung muss Port 80 geöffnet sein. Der Port wird unmittelbar nach der Aktivierung geschlossen. Danach kann auf Ihre EC2-Instance nur über die anderen Ports von der ausgewählten VPC aus zugegriffen werden.
> Auf die iSCSI-Ziele auf Ihrem Gateway kann nur von den Hosts aus zugegriffen werden, die sich in derselben VPC wie das Gateway befinden. Wenn auf die iSCSI-Ziele von Hosts außerhalb der VPC zugegriffen werden muss, sollten Sie die entsprechenden Sicherheitsgruppenregeln aktualisieren.
> Sie können Sicherheitsgruppen jederzeit bearbeiten, indem Sie zur Detailseite der Amazon-EC2-Instances navigieren, Sicherheit auswählen, zu Sicherheitsgruppendetails navigieren und die Sicherheitsgruppen-ID auswählen.

Port	Protocol (Protokoll)	Dateisystem-Protokoll				
80	TCP	HTTP-Zugriff zur Aktivierung				
3260	TCP	iSCSI				

- Speicher konfigurieren

Standardeinstellungen	AMI-Root-Volume	Volume 2 Cache	Volume 3 Cache			
Gerätename		/dev/sdf	/dev/sdf			
Größe	80 GiB	250 GiB	250 GiB			
Volume-Typ	gp3	gp3	gp3			
E/A\Sek	3000	3000	3000			
Beim Beenden löschen	Ja	Ja	Ja			
Verschlüsselt	Nein	Nein	Nein			
Durchsatz	125	125	125			

Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume Gateway bereit

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

> **Note**
>
> AMIs Die Storage Gateway Gateway-Community wird veröffentlicht und vollständig unterstützt von AWS. Sie können sehen, dass es sich bei dem Herausgeber um einen verifizierten Anbieter handelt AWS.
> Volume 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`

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

1. Richten Sie mit der Storage-Gateway-Konsole ein neues Gateway ein. Anweisungen finden Sie unter Einrichten eines Volume Gateways. Wenn Sie den Bereich Plattform-Optionen erreichen, wählen Sie Amazon EC2 als Host-Plattform aus und führen Sie dann die folgenden Schritte aus, um die Amazon-EC2-Instance zu starten, die Ihr Volume Gateway hosten wird.

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

2. Wählen Sie Launch instance, um die AWS Storage Gateway AMI-Vorlage in der Amazon EC2 EC2-Konsole zu öffnen, wo Sie zusätzliche Einstellungen konfigurieren können.

   Verwenden Sie Schnellstart, um die Amazon-EC2-Instance mit Standardeinstellungen zu starten. Weitere Informationen zu den Standardspezifikationen von Amazon-EC2-Schnellstart finden Sie unter . Schnellstart-Konfigurationsspezifikationen für Amazon EC2.

3. Geben Sie unter Name einen Namen für die Amazon-EC2-Instance ein. Nachdem die Instance bereitgestellt wurde, können Sie nach diesem Namen suchen, um Ihre Instance auf Listenseiten in der Amazon-EC2-Konsole zu finden.

4. Für Instance-Typ können Sie aus der Liste Instance-Typ die Hardware-Konfiguration für Ihre Instance auswählen. Die Hardwarekonfiguration muss bestimmte Mindestanforderungen erfüllen, um Ihr Gateway zu unterstützen. Wir empfehlen, mit dem Instance-Typ m4.xlarge zu beginnen, der die Mindestanforderungen erfüllt, damit das Gateway korrekt funktioniert. Weitere Informationen finden Sie unter Anforderungen für Amazon-EC2-Instance-Typen.

   Sie können die Größe der Instance nach dem Start bei Bedarf ändern. Weitere Informationen finden Sie unter Größenänderung Ihrer Instance im Amazon EC2 EC2-Benutzerhandbuch.

   > **Note**
   >
   > Bestimmte Instance-Typen, insbesondere i3 EC2, verwenden NVMe SSD-Festplatten. Dies kann zu Problemen führen, wenn Sie ein Volume Gateway starten oder beenden. Beispielsweise können Sie Daten aus dem Cache verlieren. Überwachen Sie die `CachePercentDirty` CloudWatch Amazon-Metrik und starten oder stoppen Sie Ihr System nur, wenn dieser Parameter aktiviert ist`0`. Weitere Informationen zu Monitoring-Metriken für Ihr Gateway finden Sie in der CloudWatch Dokumentation unter Storage Gateway Gateway-Metriken und -Dimensionen.

5. Wählen Sie im Abschnitt Schlüsselpaar (Anmeldung) für Schlüsselpaarname – erforderlich das Schlüsselpaar aus, das Sie für die sichere Verbindung mit Ihrer Instance verwenden möchten. Bei Bedarf können Sie ein neues Schlüsselpaarname erstellen. Weitere Informationen dazu finden Sie unter Erstellen eines Schlüsselpaares im Amazon-Elastic-Compute-Cloud-Benutzerhandbuch für Linux-Instances.

6. Überprüfen Sie im Abschnitt Netzwerkeinstellungen die vorkonfigurierten Einstellungen und wählen Sie Bearbeiten, um Änderungen an den folgenden Feldern vorzunehmen:

   a. Wählen Sie für VPC — erforderlich die VPC aus, auf der Sie Ihre Amazon-EC2-Instance starten möchten. Weitere Informationen zur Funktionsweise von Amazon VPC finden Sie im Amazon Virtual Private Cloud-Benutzerhandbuch.

   b. (Optional) Wählen Sie unter Subnetz das Subnetz aus, in dem Sie Ihre Amazon-EC2-Instance starten möchten.

   c. Wählen Sie für Öffentlche IP automatisch zuweisen Aktivieren aus.

7. Überprüfen Sie im Unterabschnitt Firewall (Sicherheitsgruppen) die vorkonfigurierten Einstellungen. Sie können den Standardnamen und die Beschreibung der neuen Sicherheitsgruppe, die für Ihre Amazon-EC2-Instance erstellt werden soll, ändern, wenn Sie

möchten, oder sich dafür entscheiden, stattdessen Firewallregeln aus einer vorhandenen Sicherheitsgruppe anzuwenden.

8. Fügen Sie im Unterabschnitt Eingehende Sicherheitsgruppenregeln Firewallregeln hinzu, um die Ports zu öffnen, über die Clients eine Verbindung zu Ihrer Instance herstellen. Weitere Informationen zu den für erforderlichen Ports finden Sie unter . Weitere Informationen finden Sie unter Sicherheitsgruppenregeln im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances.

   > **Note**
   >
   > Volume Gateway setzt voraus, dass der TCP-Port 80 für eingehenden Datenverkehr und für einmaligen HTTP-Zugriff während der Gateway-Aktivierung geöffnet ist. Nach der Aktivierung können Sie diesen Port schließen.
   > Darüber hinaus müssen Sie den TCP-Port 3260 für den iSCSI-Zugriff öffnen.

9. Überprüfen Sie im Unterabschnitt Erweiterte Netzwerkkonfiguration die vorkonfigurierten Einstellungen und nehmen Sie gegebenenfalls Änderungen vor.
10. Wählen Sie im Abschnitt Speicher hinzufügen die Option Neues Volume hinzufügen, um der Gateway-Instance Speicher hinzuzufügen.

    > **Important**
    >
    > Sie müssen zusätzlich zum vorkonfigurierten Root-Volume mindestens ein Amazon EBS-Volume mit mindestens 165 GiB Kapazität für den Cache-Speicher und mindestens ein Amazon EBS-Volume mit mindestens 150 GiB Kapazität für den Upload-Puffer hinzufügen. Für eine höhere Leistung empfehlen wir, mehrere EBS-Volumes für den Cache-Speicher mit jeweils mindestens 150 GiB zuzuweisen.

11. Überprüfen Sie im Abschnitt Erweiterte Details die vorkonfigurierten Einstellungen und nehmen Sie gegebenenfalls Änderungen vor.
12. Wählen Sie Instance starten, um Ihre neue Amazon-EC2-Gateway-Instance mit den konfigurierten Einstellungen zu starten.
13. Um zu überprüfen, ob Ihre neue Instance erfolgreich gestartet wurde, navigieren Sie zur Seite Instances in der Amazon-EC2-Konsole und suchen Sie anhand des Namens nach Ihrer neuen Instance. Stellen Sie sicher, dass der Instance-Status mit einem grünen Häkchen als Wird ausgeführt angezeigt wird und dass die Statusprüfung abgeschlossen ist und dass ein grünes Häkchen angezeigt wird.

14. Wählen Sie Ihre Instance auf der Detailseite aus. Kopieren Sie die öffentliche IPv4 Adresse aus dem Abschnitt Instanzübersicht und kehren Sie dann zur Seite Gateway einrichten in der Storage Gateway Gateway-Konsole zurück, um mit der Einrichtung Ihres fortzufahren.

Sie können die AMI-ID ermitteln, die für den Start eines 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 Volume 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 Amazon EC2 EC2-Konsole zu öffnen.

  Sie werden zur AMI-Seite der EC2-Community weitergeleitet, auf der Sie die AMI-ID für Ihre AWS Region in der URL sehen können.
- Führen Sie eine Abfrage des Systems Manager-Parameterspeichers durch. Sie können die AWS CLI oder Storage Gateway Gateway-API verwenden, um den öffentlichen Parameter von Systems Manager unter dem Namespace `/aws/service/storagegateway/ami/CACHED/latest` für Cached Volume Gateways oder `/aws/service/storagegateway/ami/STORED/latest` für Stored Volume Gateways abzufragen. Wenn Sie beispielsweise den folgenden CLI-Befehl verwenden, wird die ID des aktuellen AMI in der von AWS-Region Ihnen angegebenen zurückgegeben.

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  STORED/latest
  ```

  Dieser CLI-Befehl gibt etwa die folgende Ausgabe zurück:

  ```
  {
      "Parameter": {
          "Type": "String",
          "LastModifiedDate": 1561054105.083,
          "Version": 4,
          "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
  STORED/latest",
          "Name": "/aws/service/storagegateway/ami/STORED/latest",
          "Value": "ami-123c45dd67d891000"
  ```

```
    }
}
```

Metadatenoptionen Amazon EC2 EC2-Instances ändern

Der Instance-Metadaten-Service (IMDS) ist eine On-Instance-Komponente, die sicheren Zugriff auf Amazon EC2 EC2-Instance-Metadaten bietet. Eine Instance kann so konfiguriert werden, dass sie eingehende Metadatenanfragen akzeptiert, die IMDS Version 1 (IMDSv1) verwenden, oder verlangt, dass alle Metadatenanfragen IMDS Version 2 verwenden (). IMDSv2 IMDSv2 verwendet sitzungsorientierte Anfragen und behebt verschiedene Arten von Sicherheitslücken, die beim Versuch, auf das IMDS zuzugreifen, genutzt werden könnten. Weitere Informationen dazu IMDSv2 finden Sie unter So funktioniert Instance Metadata Service Version 2 im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Wir empfehlen, dass Sie IMDSv2 für alle Amazon EC2 EC2-Instances benötigen, die Storage Gateway hosten. IMDSv2 ist standardmäßig für alle neu gestarteten Gateway-Instances erforderlich. Wenn Sie über bestehende Instances verfügen, die noch so konfiguriert sind, dass sie IMDSv1 Metadatenanfragen akzeptieren, finden Sie unter Verwendung von erforderlich IMDSv2 im Amazon Elastic Compute Cloud-Benutzerhandbuch Anweisungen, wie Sie Ihre Instance-Metadatenoptionen so ändern können, dass sie die Verwendung von erfordern IMDSv2. Für die Anwendung dieser Änderung ist kein Neustart der Instance erforderlich.

Synchronisieren Sie die VM-Zeit mit der Hyper-V- oder Linux-KVM-Hostzeit

Für ein Gateway, das auf installiert ist 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 SAN/storage der Infrastruktur.
> 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 Volume Gateway beschrieben.

Bereitstellen des Gateways

Stellen Sie das OVA-Image in Ihrem konfigurierten Cluster auf einem der Cluster-Hosts bereit.

So stellen Sie das OVA-Image des Gateways bereit

1. Stellen Sie das OVA-Image auf einem der Hosts im Cluster bereit.
2. Stellen Sie sicher, dass die Datenspeicher, die Sie für den Stamm-Datenträger und den Cache wählen, für alle Hosts im Cluster verfügbar sind. Bei der Bereitstellung der 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 Override-Optionen für andere in VMs Ihrem Cluster hinzuzufügen

1. Wählen Sie auf der Übersichtsseite in VMware vSphere Ihren Cluster aus, um die Clusterseite zu öffnen, und wählen Sie dann Configure aus.
2. Wählen Sie die Registerkarte Configuration (Konfiguration) und dann VM Overrides (VM-Überschreibungen)aus.
3. Fügen Sie eine neue VM-Überschreibungsoption hinzu, um die einzelnen Werte zu ändern.

   Legen Sie die folgenden Werte für jede Option unter vSphere HA — VM-Überwachung fest:

   - VM-Überwachung: Override Enabled — VM- und Anwendungsüberwachung
   - Empfindlichkeit der VM-Überwachung: Override aktiviert — VM- und Anwendungsüberwachung
   - VM-Überwachung: Benutzerdefiniert
   - Ausfallintervall: **30** Sekunden
   - Mindestverfügbarkeit: Sekunden **120**
   - Maximum per-VM resets (Maximale Zurücksetzungen pro VM): **5**
   - Zeitfenster für maximale Rücksetzungen: 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 Volume Gateway mit AWS
  b. Überprüfen von Einstellungen und Aktivieren Ihres Volume Gateways
  c. Konfigurieren von Volume 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 Volume Gateway-Integritätsprotokollen mit CloudWatch Protokollgruppen.

Arbeiten mit Volume Gateway-Speicherressourcen

In den Themen in diesem Abschnitt wird beschrieben, wie Sie die Speicherressourcen verwalten können, die mit Ihrer Volume Gateway-Appliance und ihrer virtuellen Hostplattform verknüpft sind. Dazu gehören Ressourcen wie physische Festplatten, die an die Hypervisor-Hostplattform eines Gateways angeschlossen sind, mit spezifischen Verfahren zum Entfernen von Festplatten aus VMware vSphere ESXi-, Microsoft Hyper-V- oder Linux Kernel-based Virtual Machine (KVM) -Virtualisierungshosts. Dazu gehört auch die Verwaltung der Amazon EBS-Volumes, die an die Amazon EC2-Instance eines Gateways für Gateways angehängt sind, die auf Amazon EC2 in der Cloud gehostet werden. AWS

Topics

- Entfernen von Datenträgern aus dem Gateway- Erfahren Sie, was zu tun ist, wenn Sie eine Festplatte von der VMware vSphere- ESXi, Microsoft Hyper-V- oder Linux Kernel-based Virtual Machine (KVM) -Virtualisierungshostplattform für Ihr Gateway entfernen müssen, z. B. wenn Sie einen physischen Festplattenausfall haben.
- Verwaltung von Amazon EBS-Volumes auf Amazon EC2 EC2-Gateways- 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 vorgesehen sind, das auf einer Amazon EC2 EC2-Instance gehostet wird, z. B. wenn Ihr Anwendungsspeicherbedarf im Laufe der Zeit steigt oder sinkt.

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 EC2 EC2-Gateways

Wenn Sie Ihr Gateway ursprünglich für die Ausführung als Amazon-EC2-Instance konfiguriert haben, haben Sie Amazon-EBS-Volumes zur Verwendung als Upload-Puffer und Cache-Speicher zugewiesen. Wenn im Laufe der Zeit Änderungen an Ihren Anwendungen erforderlich sind, können Sie für diesen Zweck zusätzliche Amazon-EBS-Volumes zuordnen. Sie können auch den zugewiesenen Speicher verringern, indem Sie zuvor zugewiesene Amazon-EBS-Volumes entfernen. Weitere Informationen zu Amazon EBS finden Sie unter Amazon Elastic Block Store (Amazon EBS) im Amazon EC2 EC2-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 Amazon EC2 EC2-Benutzerhandbuch.
2. Fügen Sie das Amazon-EBS-Volume an Ihre Amazon-EC2-Instance an. Anweisungen finden Sie unter Anhängen eines Amazon EBS-Volumes an eine Instance im Amazon EC2 EC2-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.

1. Fahren Sie das Gateway mit dem im Abschnitt Herunterfahren der Gateway-VM beschriebenen Verfahren herunter.
2. Trennen Sie das Amazon-EBS-Volume von Ihrer Amazon-EC2-Instance. Anweisungen finden Sie unter Trennen eines Amazon EBS-Volumes von einer Instance im Amazon EC2 EC2-Benutzerhandbuch.
3. Löschen Sie das Amazon-EBS-Volume. Anweisungen finden Sie unter Löschen eines Amazon EBS-Volumes im Amazon EC2 EC2-Benutzerhandbuch.
4. Starten Sie das Gateway mit dem im Abschnitt Herunterfahren der Gateway-VM beschriebenen Verfahren.

Abrufen eines Aktivierungsschlüssels für das Gateway

Um einen Aktivierungsschlüssel für Ihr Gateway zu erhalten, stellen Sie eine Webanforderung an die virtuelle Gateway-Maschine (VM). Die VM gibt eine Umleitung zurück, die den Aktivierungsschlüssel enthält, der als einer der Parameter für die `ActivateGateway`-API-Aktion zur Angabe der Konfiguration Ihres Gateways übergeben wird. Weitere Informationen finden Sie 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.

Standard-Endpunkte

Um den Aktivierungsschlüssel für einen Standardendpunkt zu erhalten:

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

Dual-Stack-Endpunkte

Um den Aktivierungsschlüssel für einen Dual-Stack-Endpunkt zu erhalten:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

FIPS-Endpunkte

Um den Aktivierungsschlüssel für einen FIPS-Endpunkt zu erhalten:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

VPC-Endpunkte

So rufen Sie den Aktivierungsschlüssel für einen VPC-Endpunkt ab:

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

Linux (bash/zsh)

Das folgende Beispiel zeigt, wie Sie mit Linux (bash/zsh) die HTTP-Antwort abfangen, HTTP-Header analysieren und den Aktivierungsschlüssel abrufen.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

Das folgende Beispiel zeigt Ihnen, wie Sie Microsoft Windows verwenden, PowerShell um die HTTP-Antwort abzurufen, HTTP-Header zu analysieren und den Aktivierungsschlüssel abzurufen.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Verwenden der lokalen Konsole

Die folgenden Beispiele zeigen Ihnen, wie Sie Ihre lokale Konsole verwenden, um einen Aktivierungsschlüssel zu generieren und anzuzeigen.

Auf Amazon Linux 2 (AL2) basierende Gateways

Sie können entweder Standard- oder FIPS-Endpunkte für Gateways auswählen, die auf basieren. AL2

> **Note**
>
> FIPS-Endpunkte sind nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter FIPS-Endpunkte nach Dienst.

Um einen Aktivierungsschlüssel für Ihr AL2 basiertes Gateway von Ihrer lokalen Konsole zu erhalten

1. Melden Sie sich als Administrator bei Ihrer lokalen Konsole an.
2. Wählen Sie im Hauptmenü AWS Appliance-Aktivierung — Konfiguration `0` die Option Aktivierungsschlüssel abrufen aus.

3. Wählen Sie die Option Storage Gateway für die Gateway-Produktreihe aus.
4. Geben Sie die AWS Region ein, in der Sie Ihr Gateway aktivieren möchten.
5. Geben Sie als Netzwerktyp 1 für Öffentlich oder 2 für VPC ein.
6. Geben Sie als Endpunkttyp 1 für Standard oder 2 für Federal Information Processing Standard (FIPS) ein.

Gateways auf Basis von Amazon Linux 2023 (AL2023)

Für Gateways, die auf AL2 023 basieren, sind die folgenden Endpunkte verfügbar:

- Standard-Endpunkte (nur Support) IPv4
- FIPS-Endpunkte (nur Support) IPv4
- Dual-Stack-Endpunkte (Unterstützung und) IPv4 IPv6
- Dual-Stack-FIPS-Endpunkte (Unterstützung und) IPv4 IPv6

Weitere Informationen finden Sie unter Endpunkttypen.

Um einen Aktivierungsschlüssel für Ihr AL2 023-basiertes Gateway von Ihrer lokalen Konsole zu erhalten

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. Wählen Sie im Hauptmenü AWS Appliance-Aktivierung — Konfiguration `0` die Option Aktivierungsschlüssel abrufen aus.
3. Wählen Sie die Option Storage Gateway für die Gateway-Produktreihe aus.
4. Geben Sie die AWS Region ein, in der Sie Ihr Gateway aktivieren möchten.
5. Geben Sie als Netzwerktyp 1 für Öffentlich oder 2 für VPC-Endpunkt ein.
6. Geben Sie für Endpunkttyp auswählen die Option FIPS aktivieren? , geben Sie ein, `Y` um FIPS zu aktivieren oder einen `N` Nicht-FIPS-Endpunkt zu verwenden.
7. Geben Sie als Endpunkttyp den Wert 1 für Standardendpunkt oder 2 für Dual-Stack-Endpunkt ein.
    - Geben Sie für einen Dual-Stack-Endpunkt für Select IP version or exit: 1 for IPv4 oder 2 for ein. IPv6

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

- Von einem Windows-Client aus eine Verbindung zu Ihren Volumes herstellen
- Verbinden Sie Ihre Volumes 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.

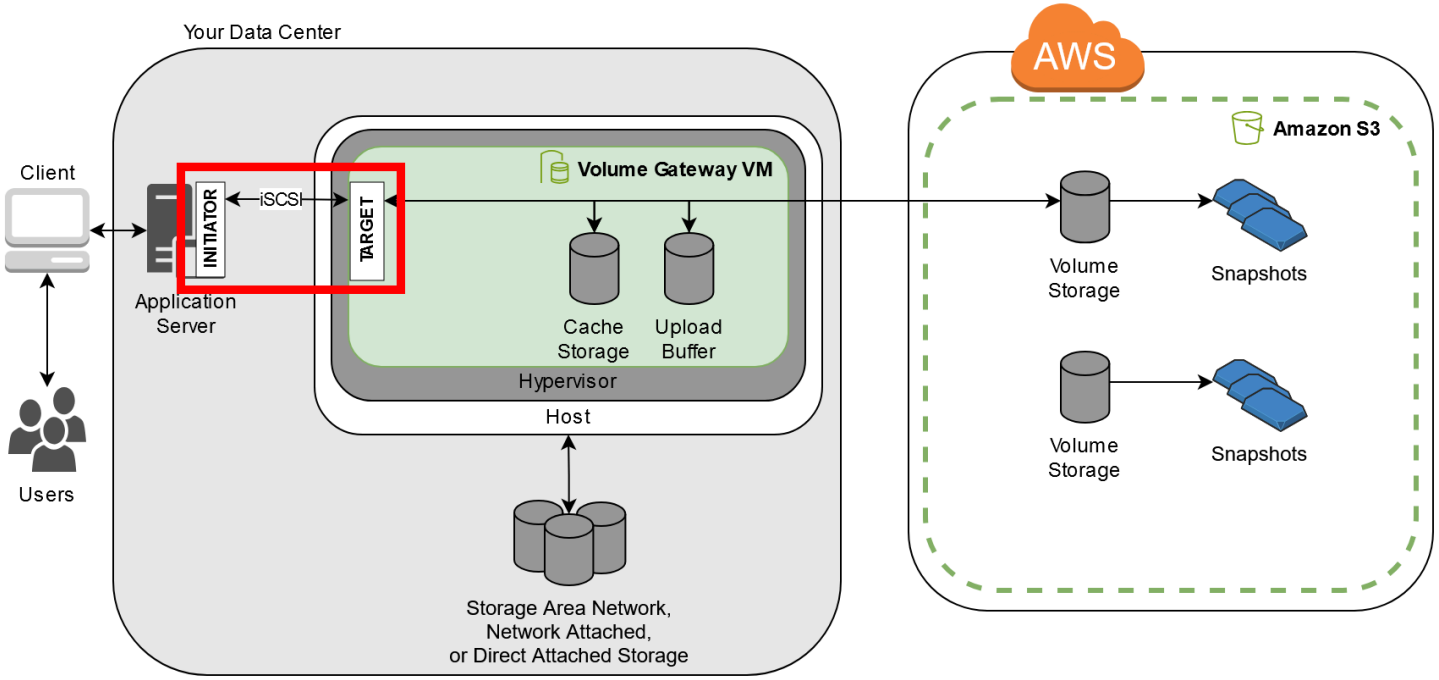
Alle Typen von Gateways lassen sich mit iSCSI-Geräten verbinden und diese Verbindungen können Sie auch anpassen. Die entsprechenden Anleitungen finden Sie nachfolgend.

Von einem Windows-Client aus eine Verbindung zu Ihren Volumes herstellen

Ein Volume Gateway macht alle Volumes, die Sie für dieses Gateway erstellt haben, als iSCSI-Ziele verfügbar. Weitere Informationen finden Sie unter Verbinden Sie Ihre Volumes mit Ihrem Client.

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

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



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

Ihr Gateway macht Ihr Volume als iSCSI-Ziel verfügbar, unter einem benutzerdefinierten Namen, dem `iqn.1997-05.com.amazon:` vorangestellt wird. Wenn Sie für Ihr Ziel beispielsweise den Namen `myvolume` festlegen, lautet der Name des iSCSI-Ziels, über das die Verbindung mit dem Volume hergestellt wird, `iqn.1997-05.com.amazon:myvolume`. Weitere Informationen dazu, wie Sie Ihre Anwendungen so konfigurieren können, dass Volumes über iSCSI gemountet werden, finden Sie unter Von einem Windows-Client aus eine Verbindung zu Ihren Volumes herstellen.

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

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

1. Geben Sie im Menü Start Ihres Windows-basierten Client-Computers **`iscsicpl.exe`** in das Feld Programme und Dateien durchsuchen ein, suchen Sie nach dem iSCSI-Initiator-Programm und führen Sie es aus.

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

2. Klicken Sie bei Aufforderung auf Ja, um den Microsoft iSCSI-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 iSCSI-Ziels ein und wählen Sie OK aus. Die IP-Adresse Ihres Gateways finden Sie auf der Registerkarte Gateway in der Storage-Gateway-Konsole. Wenn Sie Ihr Gateway in einer Amazon-EC2-Instance bereitgestellt haben, finden Sie die öffentliche IP-Adresse oder die DNS-Adresse auf der Registerkarte Beschreibung in der Amazon-EC2-Konsole.

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

   > **Warning**
   >
   > Auf Gateways, die in einer Amazon-EC2-Instance bereitgestellt werden, kann nicht über eine öffentliche Internetverbindung zugegriffen werden. Die Elastic IP-Adresse der Amazon-EC2-Instance kann nicht als Zieladresse verwendet werden.

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

   a. Wählen Sie die Registerkarte Ziele.

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

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

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

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

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

> **Note**
>
> Obwohl es im Rahmen dieser Übung nicht erforderlich ist, empfehlen wir Ihnen dringend, Ihre iSCSI-Einstellungen wie unter Anpassen der Windows iSCSI-Einstellungen beschrieben für eine reale Anwendung anzupassen.

Verbinden Sie Ihre Volumes 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 Connect-Befehl den richtigen *[GATEWAY_IP]* und den richtigen IQN angeben müssen.

> **Warning**
>
> Auf Gateways, die in einer Amazon-EC2-Instance bereitgestellt werden, kann nicht über eine öffentliche Internetverbindung zugegriffen werden. Die Elastic IP-Adresse der Amazon-EC2-Instance kann nicht als Zieladresse verwendet werden.

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

5. Überprüfen Sie mit dem folgenden Befehl, ob das Volume mit dem Client-Computer (Initiator) verbunden ist.

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

Die Ausgabe des Befehls gleicht der folgenden Beispielausgabe.

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

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

Anpassen von iSCSI-Einstellungen

Es wird dringend empfohlen, nach der Einrichtung des Initiators Ihre iSCSI-Einstellungen anzupassen, um die Trennung der Verbindung des Initiators zum Ziel zu vermeiden.

Durch Erhöhen der iSCSI-Werte für Zeitbegrenzungen, wie in den folgenden Schritten beschrieben, wird Ihre Anwendung besser im Umgang mit Schreibvorgängen, die viel Zeit in Anspruch nehmen und besser in anderen transienten Aufgaben wie Netzwerk-Unterbrechungen.

> **Note**
>
> Bevor Sie Änderungen an der Registrierung vornehmen, sollten Sie eine Sicherungskopie der Registrierung vornehmen. Informationen zum Erstellen einer Sicherungskopie und 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 Linux-Festplatten-Timeout-Einstellungen für Volume Gateways

Anpassen der Windows iSCSI-Einstellungen

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

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.

Anpassen der Linux-Festplatten-Timeout-Einstellungen für Volume Gateways

Wenn Sie ein Volume Gateway verwenden, können Sie zusätzlich zu den im vorigen Abschnitt beschriebenen iSCSI-Einstellungen die folgenden Linux-Festplatten-Timeout-Einstellungen anpassen.

So passen Sie Ihre Linux-Festplatten-Timeout-Einstellungen an

1. Erhöhen Sie die Datenträger-Zeitüberschreitungswert in den Regeldateien.

   a. Wenn Sie den RHEL 5 Initiator verwenden, öffnen Sie die `/etc/udev/rules.d/50-udev.rules` Datei und suchen Sie die folgende Zeile.

   ```
   ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

   Diese Regeldateien existieren nicht in RHEL 6- oder 7-Initiatoren, Sie müssen Sie deshalb mit der folgenden Regel erstellen.

   ```
   ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

   Um Zeitbeschränkungswert in RHEL 6 zu modifizieren, verwenden Sie den folgenden Befehl und fügen Sie dann die Zeile an Codes hinzu, wie oben angezeigt.

   ```
   sudo vim /etc/udev/rules.d/50-udev.rules
   ```

   Um Zeitbeschränkungswert in RHEL 7 zu modifizieren, verwenden Sie den folgenden Befehl und fügen Sie dann die Zeile an Codes hinzu, wie oben angezeigt.

   ```
   sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
   ```

   b. Setzen Sie den *[timeout]* Wert auf. **600**

   Dieser Wert stellt ein Timeout von 600 Sekunden dar.

2. Um sicherzustellen, dass die neuen Konfigurationswerte wirksam werden, starten Sie Ihr System erneut.

   Bevor Sie Ihr Gerät neu starten, stellen Sie sicher, dass die Ergebnisse aller Schreibvorgänge auf Ihren Volumes geleert wurden. Zu diesem Zweck unmounten Sie die Speicher-Volumes, bevor Sie den Neustart durchführen.

3. Sie können die Konfiguration testen, indem Sie den folgenden Befehl eingeben.

   ```
   udevadm test [PATH_TO_ISCSI_DEVICE]
   ```

Dieser Befehl zeigt die udev-Regeln, die auf den iSCSI-Gerät angewendet werden.

Konfigurieren von CHAP-Authentifizierung für iSCSI-Ziele

Storage Gateway unterstützt die Authentifizierung zwischen Ihrem Gateway und iSCSI-Initiatoren mithilfe des Challenge-Handshake Authentication Protocol (CHAP). CHAP bietet Schutz vor Playback-Angriffen, indem die Identität eines iSCSI-Initiators, der für den Zugriff auf ein Volume und ein VTL-Gerätеziel authentifiziert wurde, regelmäßig überprüft wird.

> **Note**
>
> Die CHAP-Konfiguration ist optional, wird jedoch dringend empfohlen.

Zur Einrichtung von CHAP müssen Sie das Protokoll sowohl in der Storage-Gateway-Konsole als auch in der iSCSI-Initiator-Software konfigurieren, über die Sie die Verbindung mit dem Ziel herstellen. Storage Gateway arbeitet mit wechselseitiger CHAP-Authentifizierung: Der Initiator authentifiziert das Ziel und das Ziel authentifiziert den Initiator.

Eine wechselseitige CHAP-Authentifizierung richten Sie wie folgt für Ihre Ziele ein:

1. Konfigurieren Sie CHAP in der Storage-Gateway-Konsole wie unter So konfigurieren Sie CHAP für ein Volume-Ziel in der Storage-Gateway-Konsole beschrieben.
2. Konfigurieren Sie CHAP in der Initiator-Software auf Ihrem Client:
   - Wie Sie die wechselseitige CHAP-Authentifizierung auf einem Windows-Client konfigurieren, erfahren Sie unter Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.
   - Wie Sie die wechselseitige CHAP-Authentifizierung auf einem Red Hat Linux-Client konfigurieren, erfahren Sie unter Auf einem Red Hat Linux-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.

So konfigurieren Sie CHAP für ein Volume-Ziel in der Storage-Gateway-Konsole

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

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

      Den Namen des Initiators finden Sie in Ihrer iSCSI-Initiator-Software. Auf Windows-Clients beispielsweise ist der Name der Wert auf der Registerkarte Konfiguration des iSCSI-Initiators. Weitere Informationen finden Sie unter Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:.

      > **Note**
      >
      > Wenn Sie den Namen des Initiators ändern möchten, müssen Sie zunächst CHAP deaktivieren. Anschließend ändern Sie den Namen des Initiators in Ihrer iSCSI-Initiator-Software und aktivieren dann CHAP mit dem neuen Namen.

   b. Geben Sie unter Für Authentifizierung des Initiators verwendeter geheimer Schlüssel den entsprechenden geheimen Schlüssel ein.

      Dieser geheime Schlüssel muss mindestens 12 Zeichen lang sein und darf höchstens 16 Zeichen lang sein. Dieser Wert ist der geheime Schlüssel, den der Initiator (Windows-Client) kennen muss, um an der CHAP-Authentifizierung mit dem Ziel teilnehmen zu können.

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

      Dieser geheime Schlüssel muss mindestens 12 Zeichen lang sein und darf höchstens 16 Zeichen lang sein. Dieser Wert ist der geheime Schlüssel, den das Ziel kennen muss, um an der CHAP-Authentifizierung mit dem Initiator teilnehmen zu können.

> **Note**
>
> Für die Authentifizierung des Ziels müssen Sie einen anderen geheimen Schlüssel verwenden als für die Authentifizierung des Initiators.

d. Wählen Sie Speichern.

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

Auf einem Windows-Client konfigurieren Sie die wechselseitige CHAP-Authentifizierung wie folgt:

In dieser Anleitung konfigurieren Sie CHAP im Microsoft iSCSI-Initiator. Hierzu verwenden Sie dieselben Schlüssel wie bei der konsolenbasierten Konfiguration von CHAP für das Volume.

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

   a. Wählen Sie die Registerkarte Konfiguration aus.

   > **Note**
   >
   > Der Wert im Feld Initiatorname ist für Ihren Initiator und Ihre Firma eindeutig. 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 Red Hat Enterprise Linux-Client.
2. Trennen Sie die Verbindung zu dem Ziel, für das Sie CHAP konfigurieren möchten, und entfernen Sie alle bereits vorhandenen Konfigurationen.

   a. Listen Sie mithilfe des folgenden Befehls die gespeicherten Konfigurationen auf, um den Zielnamen zu ermitteln und sich zu vergewissern, dass es sich um eine definierte Konfiguration handelt:

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. Trennen Sie die Verbindung mit dem Ziel.

   Der folgende Befehl trennt die Verbindung mit dem Ziel **`myvolume`**, das im qualifizierten Amazon-iSCSI-Namen (IQN) definiert ist. Passen Sie den Zielnamen und den IQN entsprechend Ihrer konkreten Umgebung an.

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. Entfernen Sie die Konfiguration des Ziels.

   Der folgende Befehl entfernt die Konfiguration für das Ziel **`myvolume`**.

   ```
   sudo /sbin/iscsiadm --mode node --op delete --targetname
    iqn.1997-05.com.amazon:myvolume
   ```

3. Bearbeiten Sie die iSCSI-Konfigurationsdatei, um CHAP zu aktivieren.

   a. Rufen Sie den Namen des Initiators ab (also den des Clients, den Sie verwenden).

Der folgende Befehl ruft den Namen des Initiators aus der Datei `/etc/iscsi/initiatorname.iscsi` ab:

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

Die Ausgabe dieses Befehls sieht in etwa wie folgt aus:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. Öffnen Sie die `/etc/iscsi/iscsid.conf` Datei.

c. 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.

Konfigurationseinstellung	Wert
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 Red Hat Enterprise Linux-Client.

Verwendung Direct Connect mit Storage Gateway

Direct Connect verbindet Ihr internes Netzwerk mit der Amazon Web Services Cloud. Durch die Verwendung Direct Connect mit Storage Gateway können Sie eine Verbindung für Workload-Anforderungen mit hohem Durchsatz herstellen und so eine dedizierte Netzwerkverbindung zwischen Ihrem lokalen Gateway und bereitstellen. AWS

Storage Gateway verwendet öffentliche Endpunkte. Wenn eine Direct Connect Verbindung besteht, können Sie eine öffentliche virtuelle Schnittstelle erstellen, über die der Datenverkehr an die Storage Gateway Gateway-Endpunkte weitergeleitet werden kann. Die öffentliche virtuelle Schnittstelle umgeht Internetdienstanbieter in Ihrem Netzwerkpfad. Der öffentliche Endpunkt des Storage Gateway Gateway-Dienstes kann sich in derselben AWS Region wie der Direct Connect Standort oder in einer anderen AWS Region befinden.

Die folgende Abbildung zeigt ein Beispiel für die Direct Connect Funktionsweise mit Storage Gateway.
Netzwerkarchitektur, die zeigt, dass Storage Gateway über AWS Direct Connect mit der Cloud verbunden ist.

In der folgenden Vorgehensweise wird davon ausgegangen, dass Sie bereits ein funktionsfähiges Gateway erstellt haben.

Zur Verwendung Direct Connect mit Storage Gateway

1. Erstellen und stellen Sie eine AWS Direct Connect Verbindung zwischen Ihrem lokalen Rechenzentrum und Ihrem Storage Gateway Gateway-Endpunkt her. Weitere Informationen zum Erstellen einer Verbindung finden Sie unter Erste Schritte mit Direct Connect im Benutzerhandbuch zu Direct Connect .
2. Connect Sie Ihre lokale Storage Gateway Gateway-Appliance mit dem Direct Connect Router.
3. Erstellen Sie eine öffentliche virtuelle Schnittstelle und konfigurieren Sie Ihren lokalen Router entsprechend. Auch bei Direct Connect müssen VPC-Endpoints mit dem erstellt werden. HAProxy Weitere Informationen finden Sie unter Erstellen einer virtuellen Schnittstelle im Benutzerhandbuch zu Direct Connect .

Einzelheiten dazu finden Sie Direct Connect unter Was ist? Direct Connect im Direct Connect Benutzerhandbuch.

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. Im Fall von Amazon-EC2-Gateways können Sie die IP-Adresse Ihrer Amazon-EC2-Instance auch aus der Amazon-EC2-Management-Konsole abrufen. Informationen zum Abrufen der IP-Adresse des Gateways finden unter:

- VMware 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-Host: Abrufen einer IP-Adresse von einem Amazon-EC2-Host

Wenn Sie die IP-Adresse gefunden haben, notieren Sie sie. Kehren Sie dann zur Storage-Gateway-Konsole zurück und geben Sie die IP-Adresse in der Konsole ein.

Abrufen einer IP-Adresse von einem Amazon-EC2-Host

Um die IP-Adresse der Amazon-EC2-Instance abzurufen, auf der das Gateway bereitgestellt wird, melden Sie sich bei der lokalen Konsole der EC2-Instance an. Rufen Sie dann die IP-Adresse am oberen Rand der Konsolenseite ab. Detaillierte Anweisungen finden Sie unter Anmelden bei der lokalen Amazon-EC2-Konsole des Gateways.

Sie können auch die IP-Adresse aus der Amazon-EC2-Management-Konsole abrufen. Wir empfehlen die Verwendung einer öffentlichen IP-Adresse für die Aktivierung. Verwenden Sie Verfahren 1, um die öffentliche IP-Adresse abzurufen. Wenn Sie die Elastic IP-Adresse verwenden möchten, gehen Sie wie unter Vorgehensweise 2 beschrieben vor.

Verfahren 1: Herstellen einer Verbindung mit dem Gateway über die öffentliche IP-Adresse

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann die EC2-Instance aus, auf der Ihr Gateway bereitgestellt wurde.
3. Wählen Sie unten die Registerkarte Description (Beschreibung) aus und notieren Sie die öffentliche IP-Adresse. Mit dieser IP-Adresse stellen Sie eine Verbindung zum Gateway her. Kehren Sie zur Storage-Gateway-Konsole zurück und geben Sie die IP-Adresse ein.

Wenn Sie die Elastic IP-Adresse für die Aktivierung verwenden möchten, gehen Sie wie folgt vor.

Verfahren 2: Herstellen einer Verbindung mit dem Gateway über die Elastic IP-Adresse

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann die EC2-Instance aus, auf der Ihr Gateway bereitgestellt wurde.
3. Wählen Sie unten die Registerkarte Description (Beschreibung) aus und notieren Sie den Wert für Elastic IP (Elastische IP). Mit der Elastic IP-Adresse stellen Sie eine Verbindung zum Gateway her. Kehren Sie zur Storage-Gateway-Konsole zurück und geben Sie die Elastic IP-Adresse ein.
4. Nachdem Ihr Gateway aktiviert wurde, wählen Sie das Gateway aus, das Sie gerade aktiviert haben, und dann die Registerkarte VTL devices (VTL-Geräte) im unteren Bereich aus.
5. Rufen Sie die Namen aller VTL-Geräte ab.
6. Führen Sie für jedes Ziel den folgenden Befehl aus, um das Ziel zu konfigurieren.

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. Führen Sie für jedes Ziel den folgenden Befehl aus, um sich anzumelden.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   Ihr Gateway ist jetzt mit der Elastic IP-Adresse der EC2 Instance verbunden.

IPv6 Unterstützung

IPv6 Unterstützung ist nur für Gateway-Appliance-Versionen 3.x oder höher verfügbar. Die Gateway-Appliance-Versionen 1.x und 2.x können nicht auf 3.x aktualisiert werden. Sie müssen Ihre Gateway-Appliance-Version 1.x oder 2.x migrieren oder ersetzen, um Support zu erhalten. IPv6

Die folgenden Dual-Stack-Endpunkte sind erforderlich für. IPv6 Weitere Informationen finden Sie unter Endpunkttypen.

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

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`

Ressourcentyp	ARN-Format
Volume-ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/volume/`*`volume-id`*
Ziel-ARN (iSCSI-Ziel)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*

Storage Gateway unterstützt auch die Verwendung von EC2-Instances sowie EBS-Volumes und -Snapshots. Diese Ressourcen sind Amazon-EC2-Ressourcen, die in Storage Gateway verwendet werden.

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 hat die Form einer Ressourcen-ID, gefolgt von einem Bindestrich und einer eindeutigen Kombination aus acht Buchstaben und Zahlen oder 17 Zahlen und Buchstaben für ein Volume oder einen Snapshot. Eine Gateway-ID hat beispielsweise die Form, in der es `sgw-12A3456B` sich um die Ressourcen-ID für Gateways `sgw` handelt, während eine Volume-ID die Form `vol-112233AABBCCDDEEF` hat, in der es sich um die Ressourcen-ID für Volumes `vol` handelt.

Ressourcen-IDs von Storage Gateway werden in Großbuchstaben geschrieben. Wenn Sie diese Ressourcen-IDs jedoch mit der Amazon EC2-API verwenden, erwartet Amazon EC2 Ressourcen-IDs in Kleinbuchstaben. Sie müssen Ihre Ressourcen-ID in Kleinbuchstaben ändern, um Sie mit der EC2-API verwenden zu können. Bei einem Storage Gateway beispielsweise könnte die ID für ein Volume `vol-112233AABBCCDDEEF` lauten. Wenn Sie diese ID mit der EC2-API verwenden, müssen Sie sie in ändern. `vol-112233aabbccddeef` 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 Volumes
- Empfohlene Kapazität für die lokalen Datenträger des Gateways

Kontingente für Volumes

In der folgenden Tabelle sind Kontingente für Volumes aufgeführt.

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

Beschreibung	Zwischengespeicherte Volumes	Stored Volumes
Note Wenn Sie einen Snapshot von einem zwischengespeicherten Volume erstellen, das größer als 16 TiB ist, können Sie das Volume in ein Storage-Gateway-Volume wiederherstellen. Eine Wiederherstellung in ein Amazon-EBS-Volume (Amazon Elastic Block Store) ist jedoch nicht möglich.		
Maximale Anzahl von Volumes pro Gateway	32	32
Gesamtgröße aller Volumes pro Gateway	1,024 TiB	512 TiB

Empfohlene Kapazität für die lokalen Datenträger des Gateways

Gateway-Typ	Cache (Minimum)	Cache (Maximum)	Upload-Puffer (Minimum)	Upload-Puffer (Maximum)
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.

Topics

- 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	Description
`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	Description
`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 ISO8601 Basic im Format YYYYMMDD'T'HHMMSS'Z' sein. Wenn sowohl der Header als auch verwendet werden, `Date` muss das Format des `x-amz-date` Date-Headers nicht verwendet werden. ISO8601 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	In diesem Header werden die Version der API und die angefragte Operation angegeben. Die Werte des Ziel-Headers werden durch Verknüpfung der API-Version mit dem API-Namen gebildet und haben folgendes Format. `x-amz-target: StorageGateway_ APIversion .operationName` Der OperationName-Wert (z. B. "ActivateGateway„) kann in der API-Liste gefunden werden. Storage-Gateway-API-Referenz

Signieren von Anforderungen

Storage Gateway erfordert, dass Sie jede gesendete Anforderung durch eine Signatur authentifizieren. Zum Signieren einer Anforderung berechnen Sie eine digitale Signatur mit einer kryptografischen Hash-Funktion. Ein kryptografischer Hash ist eine Funktion, die auf Grundlage der Eingabe einen einzigartigen Hash-Wert zurückgibt. Die Eingabe in die Hash-Funktion besteht aus dem Text Ihrer Anforderung und Ihrem geheimen Zugriffsschlüssel. Die Hash-Funktion gibt einen Hash-Wert zurück, den Sie in die Anforderung als Ihre Signatur einfügen. Die Signatur ist Teil des Headers `Authorization` in der Anforderung.

Nach dem Erhalt Ihrer Anforderung berechnet Storage Gateway die Signatur mit derselben Hash-Funktion und den von Ihnen zum Signieren der Anforderung eingegebenen Daten neu. Wenn die so berechnete Signatur mit der Signatur in der Anforderung übereinstimmt, verarbeitet Storage Gateway die Anforderung. Andernfalls wird die Anforderung abgelehnt.

Storage Gateway unterstützt die Authentifizierung mittels AWS Signature Version 4. Der Prozess zum Berechnen einer Signatur lässt sich in drei Aufgaben untergliedern:

- Aufgabe 1: Erstellen einer kanonischen Anforderung

  Ordnen Sie Ihre HTTP-Anforderung in einem kanonischen Format neu an. Die Verwendung eines kanonischen Formats ist erforderlich, weil Storage Gateway das gleiche kanonische Format verwendet, wenn eine Signatur erneut berechnet wird, um sie mit der von Ihnen gesendeten Signatur zu vergleichen.
- Aufgabe 2: Erstellen einer zu signierenden Zeichenfolge

  Erstellen Sie eine Zeichenfolge, die Sie als einen der Eingabewerte für die kryptografische Hash-Funktion nutzen. Die als zu signierende Zeichenfolge bezeichnete Zeichenfolge ist eine Kombination aus dem Namen des Hash-Algorithmus, dem Anforderungsdatum, einer Zeichenfolge mit dem Umfang der Anmeldeinformationen und der kanonischen Anforderung aus der vorherigen Aufgabe. Die Zeichenfolge mit dem Umfang der Anmeldeinformationen selbst ist eine Kombination aus Datum, Region und Serviceinformationen.
- Aufgabe 3: Erstellen einer Signatur

  Erstellen Sie eine Signatur für Ihre Anforderung. Verwenden Sie dazu eine kryptografische Hash-Funktion, die zwei Eingabezeichenfolgen akzeptiert: die zu signierende Zeichenfolge und einen abgeleiteten Schlüssel. Der abgeleitete Schlüssel wird berechnet, indem Sie mit Ihrem

geheimen Zugriffsschlüssel beginnen und anhand der Zeichenfolge für den Gültigkeitsbereich der Anmeldeinformationen eine Reihe von Hash-basierten Nachrichtenauthentifizierungscodes () 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, lautet die berechnete Signatur:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Der letzte Schritt besteht im Erstellen des `Authorization`-Headers. Für den Demo-Zugriffsschlüssel AKIAIOSFODNN7EXAMPLE (mit hinzugefügten Zeilenumbrüchen zur besseren Lesbarkeit) lautet der Header:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Fehlermeldungen

Themen

- 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`	Für die AWS Access Key ID ist ein Abonnement für den Dienst erforderlich.	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
`MaximumVolumeCount Exceeded`	Die maximale Volume-Anzahl wurde überschri tten.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	Die Gateway-N etzwerkkonfiguration wurde geändert.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`NotSupported`	Die angegebene Operation wird nicht unterstützt.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	Das angegebene Gateway ist nicht mehr auf dem neuesten Stand.	ActivateGateway
`SnapshotInProgressException`	Der angegeben e Snapshot wird bearbeitet.	DeleteVolume
`SnapshotIdInvalid`	Der angegebene Snapshot ist nicht gültig.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`StagingAreaFull`	Der Staging-Bereich ist voll.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetAlreadyExists`	Das angegebene Ziel ist bereits vorhanden.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	Das angegebene Ziel ist nicht gültig.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	Das angegebene Ziel wurde nicht gefunden.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`UnsupportedOperationForGatewayType`	Die angegebene Operation ist für den Typ des Gateways nicht gültig.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Das angegebene Volume ist bereits vorhanden.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	Das angegebene Volume ist nicht gültig.	DeleteVolume
`VolumeInUse`	Das angegebene Volume wird bereits verwendet.	DeleteVolume

Operationsfehlercode	Fehlermeldung	Operation, die den Fehlercode zurückgibt
`VolumeNotFound`	Das angegebene Volume wurde nicht gefunden.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	Das 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 Volume Gateway Benutzerhandbuch

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
IPv6 Unterstützung	IPv6Support ist für Gateway-Appliance-Versionen 3.x oder höher verfügbar.	10. September 2025
Hinweis zur Änderung der Verfügbarkeit für FSx File Gateway	Amazon FSx File Gateway ist für Neukunden nicht mehr verfügbar. Bestandskunden von FSx File Gateway können den Service weiterhin normal nutzen. Informationen zu Funktionen, die FSx File Gateway ähneln, finden Sie in diesem Blogbeitrag.	28. Oktober 2024
Hinweis zur Änderung der Verfügbarkeit von FSx File Gateway	AWS Storage Gateway FSx File Gateway wird ab dem 28.10.24 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 verwalten 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 .	24. Oktober 2023

Die empfohlenen CloudWatch Alarme wurden aktualisiert	Der CloudWatch `HealthNotifications` Alarm gilt jetzt für alle Gateway-Typen und Hostplattformen und wird für diese empfohlen. Die empfohlenen Konfigurationseinstellungen wurden auch für `HealthNotifications` und `AvailabilityNotifications` aktualisiert. Weitere Informationen finden Sie unter zu CloudWatch Alarmen.	2. Oktober 2023
Separate Benutzerhandbücher für Tape und Volume Gateway	Das Storage Gateway-Benutzerhandbuch, das zuvor Informationen sowohl zu den Tape- als auch zu den Volume Gateway-Typen enthielt, wurde in das Tape Gateway-Benutzerhandbuch und das Volume Gateway-Benutzerhandbuch aufgeteilt, die jeweils nur Informationen zu einem Gateway-Typ enthalten. Weitere Informationen finden Sie im Tape Gateway-Benutzerhandbuch und im Volume Gateway-Benutzerhandbuch.	23. März 2022

Aktualisierte Verfahren zur Gateway-Erstellung	Die Verfahren zum Erstellen aller Gateway-Typen mit der Storage-Gateway-Konsole wurden aktualisiert. Weitere Informationen finden Sie unter Erstellen eines Gateways.	18. Januar 2022
Neue Bandoberfläche	Die Seite 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
Support für FIPS-Endpunkte (Federal Information Processing Standard) in neuen Regionen AWS	Sie können jetzt ein Gateway mit FIPS-Endpunkten in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Nordkalifornien), USA West (Oregon) und Kanada (Zentral) aktivieren. Weitere Informationen finden Sie unter AWS Storage Gateway - Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	31. Juli 2020
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 zu CloudWatch Alarmen.	29. Mai 2020

Unterstützung von Endpunkten für den Federal Information Processing Standard (FIPS)	Sie können nun ein Gateway mit FIPS-Endpunkten in den AWS GovCloud (US) -Regionen aktivieren. Informationen zum Auswählen eines FIPS-Endpunkts für ein Volume-Gateway finden Sie unter Auswählen eines Service-Endpunkts. Informationen zur Auswahl eines FIPS-Endpunkts für ein Tape Gateway finden Sie unter Verbinden Ihres Tape Gateways mit AWS.	22. Mai 2020
Neue AWS Regionen	Storage Gateway ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar. Weitere Informationen finden Sie unter AWS Storage Gateway -Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.	7. Mai 2020

Unterstützung für die S3 Intelligent-Tiering-Speicherklasse	Storage Gateway unterstützt jetzt die S3 Intelligent-Tiering-Speicherklasse. Die S3 Intelligent-Tiering-Speicherklasse optimiert die Speicherkosten, indem Daten automatisch auf die kostengünstigste Zugriffsebene übertragen werden, ohne dass sich dies auf die Leistungsfähigkeit oder den Betriebsaufwand auswirkt. Weitere Informationen finden Sie unter Speicherklasse zum automatischen Optimieren häufig und selten aufgerufener Objekte im Amazon-Simple-Storage-Service-Benutzerhandbuch.	30. April 2020
Erhöhung der Schreib- und Leseleistung des Band-Gateways auf das Doppelte	Storage Gateway verdoppelt die Schreib- und Leseleistung auf und von virtuellen Bändern in Tape Gateway für schnellere Backups und Wiederherstellungen als zuvor. Weitere Informationen finden Sie unter Leistungsleitfaden für Tape Gateways im Storage Gateway-Benutzerhandbuch.	23. April 2020

Unterstützung für die automatische Banderstellung	Storage Gateway bietet jetzt die Möglichkeit, neue virtuelle Bänder automatisch zu erstellen. Tape Gateway erstellt automatisch neue virtuelle Bänder, um die Anzahl der von Ihnen konfiguri erten 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 Automatis ches Erstellen von Bändern im Storage Gateway-Benutzerha ndbuch.	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-Refer enz.	12. März 2020

Unterstützung für Linux KVM-Hypervisor (Kernel-basierte virtuelle Maschine)	Storage Gateway unterstützt jetzt die Bereitstellung eines On-Premises-Gateways auf der KVM-Virtualisierungsplattform. Gateways, die auf KVM bereitgestellt werden, verfügen über die gleiche Funktionalität und Funktionen wie die vorhandenen lokalen Gateways. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Hostanforderungen im Storage Gateway-Benutzerhandbuch.	4. Februar 2020
Support für VMware vSphere High Availability	Storage Gateway bietet jetzt Unterstützung für Hochverfügbarkeit, VMware um Storage-Workloads vor Hardware-, Hypervisor- oder Netzwerkausfällen zu schützen. Weitere Informationen finden Sie unter Verwenden von VMware vSphere High Availability mit Storage Gateway im Storage Gateway Gateway-Benutzerhandbuch. Diese Version enthält auch Leistungsverbesserungen. Weitere Informationen finden Sie unter Leistung im Storage Gateway-Benutzerhandbuch.	20. November 2019

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 es jetzt verwenden AWS Backup , um lokale Geschäftsanwendungen zu sichern, 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-Managementkonsole verwalten. Die Appliance kann Datei-, Band- und Volume Gateways hosten. Weitere Informationen finden Sie unter Verwenden der Storage Gateway-Hardware-Appliance.	18. September 2018
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.

Änderungen	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

Änderungen	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

Änderungen	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

Änderungen	Beschreibung	Änderungsdatum
Updates bei den Einstellungen für Dateifreigaben Unterstützung für die Cache-Aktualisierung in Dateifreigaben	Die Einstellungen für Dateifreigaben in der File Gateway-Konfiguration wurden um Mounting-Optionen erweitert. Nun stehen für Dateifreigaben eine Squash-Option und eine schreibgeschützte Option zur Verfügung. Weitere Informationen finden Sie unter Erstellen einer Dateifreigabe. In der File-Gateway-Konfiguration lassen sich nun alle Objekte im Amazon-S3-Bucket finden, die hinzugefügt oder entfernt wurden, seit das Gateway letztmals die Inhalte des Buckets aufgelistet und die Ergebnisse zwischengespeichert hat. Weitere Informationen finden Sie RefreshCachein der API-Referenz.	28. März 2017
Unterstützung für 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
Unterstützung für File Gateways in Amazon EC2	AWS Storage Gateway bietet jetzt die Möglichkeit, ein File Gateway in Amazon EC2 bereitzustellen. Sie können in Amazon EC2 einen File Gateway auf der Basis des Storage Gateway-Amazon Machine Image (AMI) starten, das nun als Community-AMI verfügbar ist. Informationen darüber, wie Sie ein File Gateway erstellen und 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 Amazon-EC2-Host oder Bereitstellen eines FSx File Gateways auf einem Amazon-EC2-Host.	08. Februar 2017

Änderungen	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

Änderungen	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

Änderungen	Beschreibung	Änderungsdatum
Längeres Volume 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 Einstellen des Kennworts für die lokale Konsole von der Storage Gateway Gateway-Konsole aus.	21. März 2016

Änderungen	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 Verwalten Ihres Volume Gateways.	

Änderungen	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

Änderungen	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

Änderungen	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. Für weitere Informationen siehe 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 Anforderungen für die Einrichtung von Volume 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	

Änderungen	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 Hypervisors Microsoft Hyper-V war bereits zuvor implementiert. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	30. April 2015
Kompatibilität mit Symantec Backup E:	Tape Gateway ist nun mit Symantec Backup Exec 15 kompatibel. Sie können nun Symantec Backup Exec 15 verwenden, um Ihre Daten in Amazon S3 zu sichern und direkt in Offline-Speicher (S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive) zu archivieren. Weitere Informationen finden Sie unter Testen Ihrer Konfiguration mithilfe von Veritas Backup Exec.	6. April 2015
Unterstützung für die CHAP-Auth entifizierung für Speicher-Volumes	Storage Gateway unterstützt jetzt die Konfiguration von CHAP-Authentifizierung für Speicher-Volumes. Weitere Informationen finden Sie unter Konfigurieren der CHAP-Authentifizierung für Ihre Volumes.	2. April 2015
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 zusätzlich zur Unterstützung der VMware ESXi Hypervisor-Versionen 4.1 und 5.0. Weitere Informationen finden Sie unter Unterstützte Hypervisoren und Host-Anforderungen.	30. März 2015

Änderungen	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

Änderungen	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

Änderungen	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

Änderungen	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. Weitere Informationen zur Durchführung von Konfigurationsaufgaben für Gateways, die in einer EC2-Instance bereitgestellt sind, finden Sie unter Ausführen von Aufgaben in der lokalen Amazon-EC2-Konsole oder Ausführen von Aufgaben in der lokalen Amazon-EC2-Konsole.	31. Januar 2014

Änderungen	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

Änderungen	Beschreibung	Änderungsdatum
Unterstützung für die Bereitstellung von Gateways in Amazon EC2	Storage Gateway bietet nun die Möglichkeit, ein Gateway in Amazon Elastic Compute Cloud (Amazon EC2) bereitzustellen. Sie können eine Gateway-Instance in Amazon EC2 mit dem Storage-Gateway-AMI starten, das im AWS Marketplace verfügbar ist. Informationen zu den ersten Schritten für die Bereitstellung eines Gateways mithilfe des Storage Gateway-AMI finden Sie unter Stellen Sie eine benutzerdefinierte Amazon EC2 EC2-Instance für Volume Gateway bereit.	15. Januar 2013

Änderungen	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 Volume Gateway. Sie können auch eine Testkonfiguration einrichten. Anweisungen finden Sie unter Erstellen eines Tape Gateways.	29. Oktober 2012

Änderungen	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

Migrationskampagne von Storage Gateway AL2 zu AL2023

AWS stellt das Betriebssystem (OS) der Storage Gateway Gateway-Appliance von Amazon Linux 2 auf AL2023 um, um neue Hybrid-Cloud-Speicherfunktionen zu ermöglichen und optimale Leistungs- und Sicherheitsstandards aufrechtzuerhalten. Dieser Übergang wird sich auf alle AL2-based Storage Gateway Gateway-Appliance-Versionen S3 File Gateway Version 1.x, Tape Gateway Version 2.x und Volume Gateway Version 2.x auswirken. Sie müssen die Migration vor dem 30. Juni 2026 abschließen, da der Support für AWS diese Systeme danach eingestellt wird.

Sie können anhand mehrerer Methoden feststellen, ob Ihre Gateways migriert werden müssen. Die AWS Konsole zeigt auf der Registerkarte „Details“ des Gateways für die betroffenen Gateways eine Meldung über eine veraltete Version an. Darüber hinaus bietet die `DescribeGatewayInformation`API programmatischen Zugriff, um das Feld mit dem Verfallsdatum zu überprüfen. Das AWS Health Dashboard listet die betroffenen Gateways auf der Registerkarte Betroffene Ressourcen auf. Die Liste wird jedoch nicht unmittelbar nach der Migration eines Gateways aktualisiert. Der Migrationsprozess selbst ist so konzipiert, dass die Datensicherheit oberste Priorität hat. AWS Vor Beginn der Migration wird eine Kopie der lokalen Gateway-VM-Daten gespeichert, um bei Bedarf eine einfache Wiederherstellung zu ermöglichen.

AWS bietet umfassende Migrationsleitfäden, die für jeden Gateway-Typ spezifisch sind. Nach Abschluss der Migration sollten Sie überprüfen, ob die Migration erfolgreich war, indem Sie überprüfen, ob auf der Registerkarte Gateway-Details der AWS Konsole keine Verfallswarnungen mehr angezeigt werden, oder indem Sie die `DescribeGatewayInformation`API verwenden, um zu bestätigen, dass das Feld für das Verfallsdatum nicht vorhanden ist. Entscheidend ist, dass Sie nach erfolgreicher Migration auf AL2023 nicht zu Ihrem AL2-Gateway zurückkehren dürfen, da eine Wiederherstellung zu Betriebsproblemen führen kann.

Während des gesamten Migrationszeitraums AWS erhalten Sie monatliche Erinnerungsbenachrichtigungen per E-Mail und die Registerkarte Geplante Änderungen im AWS Health Dashboard, um Sie bei der Planung und Durchführung Ihrer Migrationen zu unterstützen. Wenn Sie während der Migration auf Probleme stoßen, wenden Sie sich an den AWS Support, um Unterstützung und Anleitungen zur Fehlerbehebung zu erhalten.

Schnelllinks und Ressourcen

Referenz zur Migration von Gateway-Versionen

Anhand der Versionsnummer der Gateway-Software ist es einfach zu verstehen, welche Gateways migriert werden müssen. Es ist wichtig zu beachten, dass selbst kürzlich aktivierte Gateways, die auf dem Betriebssystem Amazon Linux 2 basieren, noch bis zum 30. Juni 2026 migriert werden müssen.

Gateway-Typ	AL2-Version (erfordert Migration)	AL203-Version (Ziel)
S3-Dateigateway	Version 1.x	Ausführung 2.x
Tape Gateway	Ausführung 2.x	Ausführung 3.x
Volume Gateway	Ausführung 2.x	Ausführung 3.x

Zeitplan für die Migration

Der Zeitplan für die Migration umfasst mehrere wichtige Meilensteine:

- 28. Oktober 2025: Alle neuen Gateway-Bereitstellungen, die über die Storage Gateway Gateway-Konsole initiiert werden, verwenden standardmäßig AL203-Images.
- 5. Januar 2026: AWS beginnt mit der Einschränkung neuer AL2-Gateway-Aktivierungen.
- 30. Juni 2026: AL2-based Gateways erhalten keine Softwareupdates mehr und der Support wird eingestellt. AWS Nach diesem Datum können Sie die AL2-based Appliances zwar weiterhin verwenden, sie erhalten jedoch keine neuen Softwareupdates, Sicherheitspatches oder Bugfixes. Die Wartung dieser Systeme liegt in Ihrer alleinigen Verantwortung.

Pre-migration Checkliste

> **Important**
>
> Bevor Sie mit dem Migrationsprozess beginnen, überprüfen Sie die folgenden Anforderungen, um eine erfolgreiche Migration sicherzustellen.

- Verwenden Sie das neueste Gateway-Image. Gehen Sie beim Erstellen der neuen Storage Gateway Gateway-VM wie folgt vor:
  - Verwenden Sie für Amazon EC2 EC2-Gateways das neueste AMI aus dem öffentlichen SSM-Parameter oder verwenden Sie die Storage Gateway Gateway-Konsole.
  - Laden Sie für lokale Gateways das neueste VM-Image von der Storage Gateway Gateway-Konsole herunter.
- Passen Sie die Hardwarekonfiguration an. Stellen Sie sicher, dass die neue Gateway-VM dieselbe CPU, denselben Arbeitsspeicher und denselben Netzwerkdurchsatz verwendet wie das vorhandene Gateway. Verwenden Sie für EC2-Gateways denselben Instanztyp.
- Überprüfen Sie die Größe der Root-Festplatte. Die Stammfestplatte der neuen Gateway-VM muss mindestens dieselbe Größe wie die Stammfestplatte des vorhandenen Gateways haben. Wenn auf der vorhandenen Root-Festplatte weniger als 20 GB verfügbarer Speicherplatz zur Verfügung stehen, passen Sie die Größe der neuen Root-Festplatte wie folgt an: (Größe der vorhandenen Root-Festplatte) + (20 GB abzüglich des verfügbaren Speicherplatzes auf der vorhandenen Root-Festplatte).
- Wenden Sie ausstehende Softwareupdates an. Bevor Sie mit der Migration beginnen, wenden Sie alle ausstehenden Softwareupdates auf dem vorhandenen Gateway an. Öffnen Sie die Storage Gateway Gateway-Konsole, wählen Sie Ihr Gateway aus und wählen Sie Jetzt aktualisieren, falls verfügbar.
- Überprüfen Sie die Netzwerkkonnektivität vom neuen Gateway aus. Bevor Sie mit der Migration beginnen, stellen Sie sicher, dass die neue Gateway-VM Folgendes erreichen kann:
  - Storage Gateway Gateway-Dienstendpunkte (oder Ihre VPC-Endpunkte).
  - Verwenden Sie den Netzwerkverbindungstest der lokalen Gateway-Konsole, um zu überprüfen, ob alle Endpunkte erfolgreich sind.

Leitfäden zur Migration

- Leitfaden zur Migration von S3 File Gateway
- Leitfaden zur Migration von Tape Gateway
- Leitfaden zur Migration von Volume Gateway

Support und Überwachung

- Storage Gateway Gateway-Konsole

- AWS Personal Health Dashboard
- AWS Support kontaktieren

Häufig gestellte Fragen

Was passiert mit meinen Daten während der Migration?

Ihre Daten bleiben während des AWS gesamten Migrationsprozesses dauerhaft gespeichert. Das Migrationsverfahren umfasst das Speichern einer Kopie Ihrer lokalen Gateway-VM-Daten AWS zur einfachen Wiederherstellung, falls erforderlich.

Wird es während der Migration zu Ausfallzeiten kommen?

Der Zeitpunkt der Migration und mögliche Serviceunterbrechungen hängen vom Typ und der Konfiguration Ihres Gateways ab. Ausführliche Informationen finden Sie im Gateway-spezifischen Migrationsleitfaden für Ihre Bereitstellung.

Was passiert, wenn ich nicht bis zum 30. Juni 2026 migriere?

Ihr Gateway wird weiterhin normal funktionieren und die Daten bleiben sicher gespeichert. Sie müssen die betroffenen Gateways AWS jedoch bis zum 30. Juni 2026 migrieren, um weiterhin Updates und Support zu erhalten.

Kann ich mein AL2-basiertes Gateway nach der Migration weiter verwenden?

Nein, Sie sollten Ihr AL2-Gateway nach erfolgreicher Migration nicht zusammen mit Ihrem AL2023 AL2023-Gateway verwenden. Verwenden Sie in Zukunft nur noch Ihr neues AL2023-based Gateway. Die gleichzeitige Verwendung von AL2- und AL203-Gateways kann zu Betriebsproblemen führen.

Ich habe Probleme bei der Migration. Was soll ich tun?

Wenden Sie sich an den AWS Support, um Unterstützung zu erhalten Unser Support-Team kann Ihnen bei der Behebung von Migrationsproblemen helfen und Sie durch den Prozess führen.

Versionshinweise für die Volume Gateway-Gerätesoftware

In diesen Versionshinweisen werden die neuen und aktualisierten Funktionen, Verbesserungen und Korrekturen beschrieben, die in jeder Version der enthalten sind. Jede Softwareversion wird durch ihr Veröffentlichungsdatum und eine eindeutige Versionsnummer identifiziert.

Sie können die Softwareversionsnummer eines Gateways ermitteln, indem Sie die Seite „Details“ in der Storage Gateway Gateway-Konsole überprüfen oder die DescribeGatewayInformationAPI-Aktion mit einem AWS CLI Befehl aufrufen, der dem folgenden ähnelt:

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

Die Versionsnummer wird im `SoftwareVersion` Feld der API-Antwort zurückgegeben.

> **Note**
>
> Ein Gateway meldet unter den folgenden Umständen keine Informationen zur Softwareversion:
>
> - Das Gateway ist offline.
> - Auf dem Gateway wird ältere Software ausgeführt, die keine Versionsberichterstattung unterstützt.
> - Der Gateway-Typ ist FSx File Gateway.

Weitere Informationen zu , einschließlich der Änderung des standardmäßigen automatischen Wartungs- und Aktualisierungszeitplans für ein Gateway, finden Sie unter verwalten Gateway-Updates mit der AWS Storage Gateway Console verwalten.

Weitere Informationen zur Migration von Volume Gateway von Amazon Linux 2 auf AL2023 finden Sie unter. Migration von AL2 nach AL2023

Gateways auf Basis von Amazon Linux 2023 (AL2023)

In der folgenden Tabelle sind die Versionshinweise für Gateways aufgeführt, die auf AL2023 basieren.

> **Note**
>
> Die Gateway-Versionen 2.x.x können nicht auf 3.x.x aktualisiert werden.

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-05-04	3,2,5	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways • Das Problem mit der standardmäßigen Netzwerk-MTU-Einstellung, die Gateways betraf, wurde behoben HyperV-based
2026-04-01	3.2.4	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2026-03-02	3.2.3	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways • Das Problem mit Gateway-Protokollen auf einigen Gateways wurde behoben

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-02-12	3.2.2	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways • Es wurde ein Problem mit Softwareupdates auf AL2023-Gateways behoben, bei denen VPC-Endpunkte (VPCE) auf statische IP-Adressen eingestellt waren
2026-02-02	3.2.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2026-01-06	3.1.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-12-04	3,0.6	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-11-06	3.0.5	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-10-10	3.0.4	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-09-12	3.0.3	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-08-29	3.0.2	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways • Probleme mit der statische n IP-Konfiguration wurden behoben

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-08-18	3.0.1	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
16.07.2025	3.0.0	• Erste Veröffentlichung des neuen Betriebssystems • IPv6-Unterstützung hinzugefügt

Amazon Linux 2 (AL 2) basierte Gateways

In der folgenden Tabelle sind die Versionshinweise für Gateways aufgeführt, die auf basieren. AL2

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2026-05-04	2.14.4	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2026-04-01	2.14.3	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2026-03-02	2,14,2	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung

Veröffentlichungsdatum	Softwareversion	Versionshinweise
		der Sicherheit und Leistung neuer und vorhandener Gateways
2026-02-02	2.14.1	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2026-01-05	2.14.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-12-05	2.13.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-11-03	2.12,15	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-10-01	2.12,14	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-09-02	2.12,13	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
31.07.2025	2.12,12	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-07-01	2.12,11	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-06-02	2.12,10	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2025-05-01	2.12,9	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-05-01	2.12,8	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-04-01	2.12,7	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
2025-03-04	2.12,6	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways

Veröffentlichungsdatum	Softwareversion	Versionshinweise
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
2024-11-06	2.12,1	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-10-03	2.12.0	• Es wurde ein Problem behoben, bei dem der iSCSI-Initiator nach einem Gateway-Neustart oder einem Gateway-Softwareupdate nicht automatisch wieder eine Verbindung zu Volumes herstellte • Betriebssystem und Softwareelemente wurden aktualisiert, um die Sicherheit und Leistung neuer und vorhandener Gateways zu verbessern
2024-08-30	2.11.0	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways
29.07.2024-07	2.10.0	• Aktualisierte Betriebssystem- und Softwareelemente zur Verbesserung der Sicherheit und Leistung neuer und vorhandener Gateways • Verschiedene Bugfixes und Verbesserungen

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 des SOCKS5-Proxys wurde behoben
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

Veröffentlichungsdatum	Softwareversion	Versionshinweise
2024-03-06	2.8.0	• Aktualisierte Betriebss ystem- und Softwaree lemente zur Verbesserung der Sicherheit und Leistung neuer Gateways • Sicherheitspatch-Updates
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	• Wartungsversion

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.