



Panduan Pengguna Tape Gateway

AWS Storage Gateway



Versi API 2013-06-30

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

AWS Storage Gateway: Panduan Pengguna Tape Gateway

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

.....	x
Apa itu Tape Gateway?	1
Gerbang Pita	1
Apakah Anda pengguna Storage Gateway pertama kali?	2
Cara kerja Tape Gateway	2
Gerbang Pita	2
Harga	5
Rencanakan penerapan gateway Anda	5
Memulai	7
Mendaftar untuk AWS Storage Gateway	7
AWS Daerah	8
Persyaratan	8
Persyaratan perangkat keras dan penyimpanan	8
Persyaratan jaringan dan firewall	10
Hypervisor dan persyaratan host yang didukung	21
Pemrakarsa iSCSI yang didukung	23
Aplikasi cadangan pihak ketiga yang didukung	23
Mengakses AWS Storage Gateway	25
Menggunakan alat perangkat keras	26
Informasi Pemesanan	27
AWS Wilayah yang didukung	27
Menyiapkan alat perangkat keras Anda	27
Memasang rak dan menghubungkan alat perangkat keras ke daya	29
Dimensi alat perangkat keras	29
Mengkonfigurasi parameter jaringan	34
Mengaktifkan alat perangkat keras Anda	37
Membuat gateway	38
Mengkonfigurasi alamat IP untuk gateway	39
Mengkonfigurasi gateway Anda	41
Menghapus gateway	41
Menghapus alat perangkat keras Anda	42
Membuat Gateway Anda	43
Ikhtisar - Aktivasi Gateway	43
Siapkan gateway	43

Connect ke AWS	43
Tinjau dan aktifkan	43
Ikhtisar - Konfigurasi Gateway	44
Ikhtisar - Sumber Daya Penyimpanan	44
Membuat Tape Gateway	44
Membuat Gateway	44
Membuat Kolam Tape Kustom	50
Membuat Kaset	53
Menggunakan Tape Gateway Anda	59
Mengaktifkan gateway Anda di cloud pribadi virtual	146
Membuat Endpoint VPC untuk Storage Gateway	147
Mengelola Gateway Anda	149
Mengelola Tape Gateway Anda	149
Mengedit Informasi Gateway	150
Menambahkan Kaset	150
Mengelola Pembuatan Pita Otomatis	151
Kaset Pengarsipan	153
Memindahkan Tape dari Pengambilan Fleksibel Gletser S3 ke S3 Glacier Deep Archive	154
Mengambil Kaset yang Diarsipkan	155
Penggunaan Tape Melihat	156
Menghapus Kaset	157
Menghapus Kolam Pita Kustom	158
Menonaktifkan Tape Gateway Anda	159
Memahami Status Pita	160
Memindahkan data Anda ke gateway baru	162
Memindahkan kaset virtual ke Tape Gateway baru	163
Memantau Storage Gateway	168
Memahami metrik gateway	168
Dimensi untuk metrik Storage Gateway	171
Memantau buffer unggahan	172
Memantau penyimpanan cache	175
Memahami CloudWatch alarm	176
Membuat CloudWatch alarm yang direkomendasikan	178
Membuat CloudWatch alarm khusus	179
Memantau Tape Gateway Anda	181
Mendapatkan Log Kesehatan Tape Gateway	181

Menggunakan Metrik CloudWatch Amazon	183
Memahami Metrik Pita Virtual	184
Mengukur Kinerja Antara Tape Gateway Anda dan AWS	186
Mempertahankan Gateway Anda	190
Mematikan VM Gateway Anda	190
Memulai dan Menghentikan Tape Gateway	191
Mengelola disk lokal	192
Menentukan jumlah penyimpanan disk lokal	192
Optimalkan Kinerja	194
Mengukur buffer unggahan	194
Ukuran penyimpanan cache	196
Tambahkan buffer unggahan atau penyimpanan cache	196
Mengelola Bandwidth	197
Mengubah Bandwidth Throttling Menggunakan Storage Gateway Console	198
Penjadwalan Pelambatan Bandwidth	198
Menggunakan AWS SDK for Java	200
Menggunakan AWS SDK for .NET	202
Menggunakan AWS Tools for Windows PowerShell	204
Mengelola Pembaruan Gateway	205
Melakukan Tugas Pemeliharaan di Konsol Lokal	207
Melakukan Tugas di Konsol Lokal VM	207
Melakukan Tugas di Konsol Lokal EC2	225
Mengakses Konsol Lokal Gateway	231
Mengkonfigurasi Adaptor Jaringan untuk Gateway Anda	236
Menghapus Gateway Anda dan Menghapus Sumber Daya	241
Menghapus Gateway Anda dengan Menggunakan Storage Gateway Console	242
Menghapus Sumber Daya dari Gateway yang Diterapkan di Tempat	243
Menghapus Sumber Daya dari Gateway yang Diterapkan di Instans Amazon EC2	244
Performa	246
Panduan kinerja untuk Tape Gateways	246
Mengoptimalkan Kinerja Gateway	249
Konfigurasi yang Direkomendasikan	249
Tambahkan Sumber Daya ke Gateway Anda	250
Optimalkan Pengaturan iSCSI	253
Gunakan Ukuran Blok yang Lebih Besar untuk Tape Drives	253
Optimalkan Kinerja Virtual Tape Drive	254

Tambahkan Sumber Daya ke Lingkungan Aplikasi Anda	254
Menggunakan VMware Ketersediaan Tinggi dengan Storage Gateway	255
Konfigurasi Cluster VSphere VMware HA Anda	256
Unduh Image .ova dari konsol Storage Gateway	258
Menyebarkan Gateway	258
(Opsional) Tambahkan Opsi Override untuk VM Lain di Cluster Anda	258
Aktifkan Gateway Anda	259
Uji Konfigurasi Ketersediaan Tinggi VMware Anda	260
Keamanan	261
Perlindungan data	262
Enkripsi data	263
Manajemen Identitas dan Akses	264
Audiens	265
Mengautentikasi dengan identitas	266
Mengelola akses menggunakan kebijakan	269
Bagaimana AWS Storage Gateway bekerja dengan IAM	272
Contoh kebijakan berbasis identitas	279
Memecahkan masalah	283
Pencatatan dan Pemantauan	285
Informasi Storage Gateway di CloudTrail	285
Memahami Entri File Log Storage Gateway	286
Validasi kepatuhan	288
Ketangguhan	289
Keamanan Infrastruktur	289
AWS Praktik Terbaik Keamanan	290
Memecahkan masalah gateway	291
Pemecahan masalah: masalah offline gateway	291
Periksa firewall atau proxy terkait	292
Periksa SSL atau inspeksi paket mendalam yang sedang berlangsung dari lalu lintas gateway Anda	292
Periksa pemadaman listrik atau kegagalan perangkat keras pada host hypervisor	292
Periksa masalah dengan disk cache terkait	292
Pemecahan masalah: masalah aktivasi gateway	293
Mengatasi kesalahan saat mengaktifkan gateway Anda menggunakan titik akhir publik	294
Mengatasi kesalahan saat mengaktifkan gateway menggunakan endpoint Amazon VPC	297

Mengatasi kesalahan saat mengaktifkan gateway Anda menggunakan titik akhir publik dan ada titik akhir VPC Storage Gateway di VPC yang sama	301
Memecahkan masalah gateway lokal	301
Mengaktifkan AWS Support untuk membantu memecahkan masalah gateway Anda	306
Memecahkan masalah pengaturan Microsoft Hyper-V	307
Memecahkan masalah gateway Amazon EC2	311
Aktivasi gateway tidak terjadi setelah beberapa saat	312
Tidak dapat menemukan instance gateway EC2 dalam daftar instans	312
Tidak dapat melampirkan volume Amazon EBS ke instans gateway EC2	313
Tidak ada disk yang tersedia saat Anda mencoba menambahkan pesan volume penyimpanan	313
Cara menghapus disk yang dialokasikan sebagai ruang buffer unggah untuk mengurangi ruang buffer unggah	313
Throughput ke atau dari gateway EC2 turun ke nol	313
Mengaktifkan AWS Support untuk membantu memecahkan masalah gateway	314
Connect ke gateway Amazon EC2 Anda menggunakan konsol serial	316
Memecahkan masalah alat perangkat keras	316
Cara menentukan alamat IP layanan	316
Cara melakukan reset pabrik	316
Cara melakukan restart jarak jauh	316
Cara mendapatkan dukungan Dell iDRAC	317
Cara menemukan nomor seri alat perangkat keras	317
Cara mendapatkan dukungan alat perangkat keras	317
Memecahkan masalah rekaman virtual	318
Memulihkan Pita Virtual Dari Gateway yang Tidak Dapat Dipulihkan	318
Memecahkan Masalah Kaset yang Tidak Dapat Dipulihkan	322
Pemberitahuan Kesehatan Ketersediaan Tinggi	323
Memecahkan masalah ketersediaan tinggi	323
Pemberitahuan Kesehatan	324
Metrik	325
Memulihkan data Anda: praktik terbaik	325
Memulihkan dari shutdown VM yang tidak terduga	326
Memulihkan data dari gateway yang tidak berfungsi atau VM	327
Memulihkan data dari rekaman yang tidak dapat dipulihkan	327
Memulihkan data dari disk cache yang tidak berfungsi	327
Memulihkan data dari pusat data yang tidak dapat diakses	328

Sumber Daya Tambahan	329
Pengaturan Host	329
Mengkonfigurasi VMware untuk Storage Gateway	329
Menyinkronkan Waktu VM Gateway Anda	336
Menerapkan host Amazon EC2 untuk Tape Gateway	338
Terapkan Amazon EC2 dengan Pengaturan Default	342
Ubah opsi metadata instans Amazon EC2	345
Gerbang Pita	345
Menghapus Disk dari Gateway Anda	345
Volume EBS untuk Gerbang EC2	349
Bekerja dengan Perangkat VTL	350
Bekerja dengan Kaset	355
Mendapatkan Kunci Aktivasi	357
Linux (ikal)	358
Linux (bash/zsh)	359
Microsoft Windows PowerShell	360
Menggunakan konsol lokal Anda	360
Menghubungkan Inisiator iSCSI	361
Menghubungkan ke Perangkat VTL	362
Menghubungkan Volume atau Perangkat VTL Anda ke Klien Linux	368
Menyesuaikan Pengaturan iSCSI	370
Mengkonfigurasi Otentikasi CHAP	378
Menggunakan AWS Direct Connect dengan Storage Gateway	387
Persyaratan Pelabuhan	387
Menghubungkan ke Gateway Anda	394
Mendapatkan Alamat IP dari Host Amazon EC2	395
Memahami Sumber Daya dan ID Sumber Daya	396
Bekerja dengan ID Sumber Daya	396
Menandai Sumber Daya Anda	397
Bekerja dengan Tag	398
Komponen Sumber Terbuka	399
Kuota Storage Gateway	399
Kuota untuk kaset	400
Ukuran disk lokal yang direkomendasikan untuk gateway Anda	400
Referensi API	402
Header Permintaan yang Diperlukan	402

Menandatangani Permintaan	404
Contoh Perhitungan Tanda Tangan	405
Respons Kesalahan	407
Pengecualian	408
Kode Kesalahan Operasi	410
Respons Kesalahan	429
Operasi	431
Riwayat dokumen	432
Pembaruan sebelumnya	450
Catatan rilis	471

Dokumentasi Amazon S3 File Gateway telah dipindahkan ke [Apa itu Amazon S3 File Gateway?](#)

Dokumentasi Amazon FSx File Gateway telah dipindahkan ke [Apa itu Amazon FSx File Gateway?](#)

Dokumentasi Volume Gateway telah dipindahkan ke [Apa itu Volume Gateway?](#)

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.

Apa itu Tape Gateway?

AWS Storage Gateway menghubungkan perangkat lunak lokal dengan penyimpanan berbasis cloud untuk menyediakan integrasi tanpa batas dengan fitur keamanan data antara lingkungan TI lokal dan infrastruktur penyimpanan. AWS Anda dapat menggunakan layanan ini untuk menyimpan data di Amazon Web Services Cloud untuk penyimpanan yang terukur dan hemat biaya yang membantu menjaga keamanan data.

AWS Storage Gateway menawarkan File Gateway berbasis file (File Amazon S3 dan File Amazon FSx), berbasis volume (Cached dan Stored), dan solusi penyimpanan berbasis tape.

Topik

- [Gerbang Pita](#)
- [Apakah Anda pengguna Storage Gateway pertama kali?](#)
- [Cara kerja Tape Gateway \(arsitektur\)](#)
- [Harga Storage Gateway](#)
- [Rencanakan penyebaran Storage Gateway](#)

Gerbang Pita

Tape Gateway — Tape Gateway menyediakan penyimpanan pita virtual yang didukung cloud.

Dengan Tape Gateway, Anda dapat mengarsipkan data cadangan dengan hemat biaya dan tahan lama di S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive. Tape Gateway menyediakan infrastruktur rekaman virtual yang disesuaikan dengan kebutuhan bisnis Anda dan menghilangkan beban operasional penyediaan, penskalaan, dan pemeliharaan infrastruktur rekaman fisik.

Anda dapat menerapkan Storage Gateway baik lokal sebagai alat VM yang berjalan di VMware ESXi, KVM, atau hypervisor Microsoft Hyper-V, sebagai alat perangkat keras, atau sebagai instans Amazon EC2. AWS Anda menerapkan gateway Anda pada instans EC2 untuk menyediakan volume penyimpanan iSCSI di. AWS Anda dapat menggunakan gateway yang dihosting di instans EC2 untuk pemulihan bencana, pencerminan data, dan menyediakan penyimpanan untuk aplikasi yang dihosting di Amazon EC2.

Untuk ikhtisar arsitektur, lihat [Cara kerja Tape Gateway \(arsitektur\)](#). Untuk melihat berbagai kasus penggunaan yang AWS Storage Gateway membantu memungkinkan, lihat [AWS Storage Gateway](#).

Dokumentasi: Untuk dokumentasi Tape Gateway, lihat [Membuat Tape Gateway](#).

Apakah Anda pengguna Storage Gateway pertama kali?

Dalam dokumentasi berikut, Anda dapat menemukan bagian Memulai yang mencakup informasi penyiapan yang umum untuk semua gateway dan juga bagian pengaturan khusus gateway. Bagian Memulai menunjukkan cara menerapkan, mengaktifkan, dan mengonfigurasi penyimpanan untuk gateway. Bagian manajemen menunjukkan cara mengelola gateway dan sumber daya Anda:

- [Membuat Tape Gateway](#) memberikan petunjuk tentang cara membuat dan menggunakan Tape Gateway. Ini menunjukkan kepada Anda cara mencadangkan data ke kaset virtual dan mengarsipkan kaset.
- [Mengelola Gateway Anda](#) menjelaskan cara melakukan tugas manajemen untuk gateway Anda dan sumber dayanya.

Dalam panduan ini, Anda terutama dapat menemukan cara bekerja dengan operasi gateway dengan menggunakan AWS Management Console. Jika Anda ingin menjalankan operasi ini secara terprogram, lihat Referensi [AWS Storage Gateway API](#).

Cara kerja Tape Gateway (arsitektur)

Berikut ini, Anda dapat menemukan ikhtisar arsitektur dari solusi Tape Gateway .

Gerbang Pita

Tape Gateway menawarkan solusi yang tahan lama dan hemat biaya untuk mengarsipkan data Anda di Amazon Web Services Cloud. Dengan antarmuka pustaka pita virtual (VTL), Anda menggunakan infrastruktur cadangan berbasis tape yang ada untuk menyimpan data pada kartrid pita virtual yang Anda buat di Tape Gateway Anda. Setiap Tape Gateway telah dikonfigurasi sebelumnya dengan media changer dan tape drive. Ini tersedia untuk aplikasi cadangan klien Anda yang ada sebagai perangkat iSCSI. Anda menambahkan kartrid tape saat Anda perlu mengarsipkan data Anda.

Diagram berikut memberikan gambaran umum tentang penyebaran Tape Gateway.

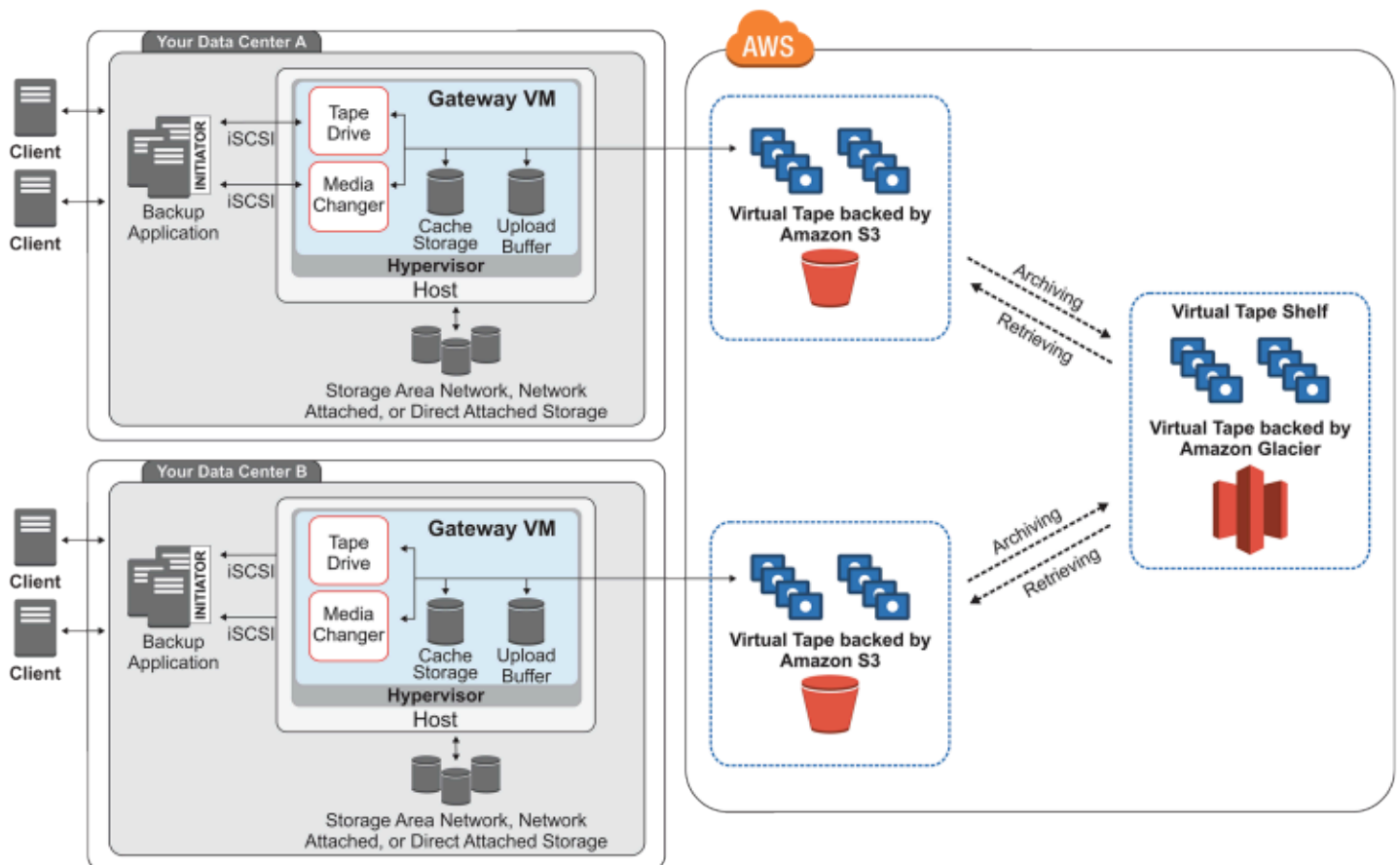


Diagram mengidentifikasi komponen Tape Gateway berikut:

- Pita virtual — Pita virtual seperti kartrid pita fisik. Namun, data pita virtual disimpan di Amazon Web Services Cloud. Seperti kaset fisik, kaset virtual bisa kosong atau dapat memiliki data tertulis di dalamnya. Anda dapat membuat kaset virtual baik dengan menggunakan konsol Storage Gateway atau secara terprogram dengan menggunakan Storage Gateway API. Setiap gateway dapat berisi hingga 1.500 kaset atau hingga 1 PiB dari total data rekaman sekaligus. Ukuran setiap pita virtual, yang dapat Anda konfigurasi saat membuat kaset, adalah antara 100 GiB dan 15 TiB.
- Virtual tape library (VTL) — VTL seperti perpustakaan rekaman fisik yang tersedia di tempat dengan lengan robot dan tape drive. VTL Anda mencakup koleksi kaset virtual yang disimpan. Setiap Tape Gateway dilengkapi dengan satu VTL.

Kaset virtual yang Anda buat muncul di VTL gateway Anda. Kaset di VTL didukung oleh Amazon S3. Saat perangkat lunak cadangan Anda menulis data ke gateway, gateway menyimpan data secara lokal dan kemudian mengunggahnya secara asinkron ke kaset virtual di VTL Anda—yaitu, Amazon S3.

- **Tape drive** — Sebuah VTL tape drive analog dengan tape drive fisik yang dapat melakukan I/O dan mencari operasi pada tape. Setiap VTL dilengkapi dengan satu set 10 tape drive, yang tersedia untuk aplikasi cadangan Anda sebagai perangkat iSCSI.
- **Media changer** — Pengubah media VTL analog dengan robot yang memindahkan kaset di sekitar slot penyimpanan dan tape drive perpustakaan rekaman fisik. Setiap VTL dilengkapi dengan satu media changer, yang tersedia untuk aplikasi cadangan Anda sebagai perangkat iSCSI.
- **Arsip** — Arsip analog dengan fasilitas penahan pita di luar kantor. Anda dapat mengarsipkan kaset dari VTL gateway Anda ke arsip. Jika diperlukan, Anda dapat mengambil kaset dari arsip kembali ke VTL gateway Anda.
- **Kaset pengarsipan** — Saat perangkat lunak cadangan mengeluarkan kaset, gateway Anda memindahkan kaset ke arsip untuk penyimpanan jangka panjang. Arsip terletak di AWS Wilayah tempat Anda mengaktifkan gateway. Kaset dalam arsip disimpan di rak pita virtual (VTS). VTS didukung oleh [S3 Glacier Flexible Retrieval](#) atau [S3 Glacier Deep Archive](#), [layanan penyimpanan berbiaya rendah untuk pengarsipan data, pencadangan](#), dan retensi data jangka panjang.
- **Mengambil kaset** — Anda tidak dapat membaca kaset yang diarsipkan secara langsung. Untuk membaca rekaman yang diarsipkan, Anda harus terlebih dahulu mengambilnya ke Tape Gateway dengan menggunakan konsol Storage Gateway atau Storage Gateway API.

Important

Jika Anda mengarsipkan kaset di S3 Glacier Flexible Retrieval, Anda dapat mengambil rekaman itu biasanya dalam waktu 3-5 jam. Jika Anda mengarsipkan rekaman di S3 Glacier Deep Archive, Anda dapat mengambilnya biasanya dalam waktu 12 jam.

Setelah menerapkan dan mengaktifkan Tape Gateway, Anda memasang drive tape virtual dan media changer di server aplikasi lokal sebagai perangkat iSCSI. Anda membuat kaset virtual sesuai kebutuhan. Kemudian Anda menggunakan aplikasi perangkat lunak cadangan yang ada untuk menulis data ke kaset virtual. Pengubah media memuat dan membongkar kaset virtual ke dalam drive pita virtual untuk operasi baca dan tulis.

Mengalokasikan disk lokal untuk gateway VM

VM gateway Anda memerlukan disk lokal, yang Anda alokasikan untuk tujuan berikut:

- Penyimpanan cache — Penyimpanan cache bertindak sebagai penyimpanan data yang tahan lama yang menunggu untuk diunggah ke Amazon S3 dari buffer unggahan.

Jika aplikasi Anda membaca data dari rekaman virtual, gateway menyimpan data ke penyimpanan cache. Gateway menyimpan data yang baru diakses di penyimpanan cache untuk akses latensi rendah. Jika aplikasi Anda meminta data tape, gateway terlebih dahulu memeriksa penyimpanan cache untuk data sebelum mengunduh data dari AWS.

- Buffer unggah - Buffer unggahan menyediakan area pementasan untuk gateway sebelum mengunggah data ke pita virtual. Buffer unggahan juga penting untuk membuat titik pemulihan yang dapat Anda gunakan untuk memulihkan kaset dari kegagalan yang tidak terduga. Untuk informasi selengkapnya, lihat [Anda Perlu Memulihkan Pita Virtual dari Gateway Tape yang Rusak](#).

Saat aplikasi cadangan Anda menulis data ke gateway Anda, gateway menyalin data ke penyimpanan cache dan buffer unggahan. Kemudian mengakui penyelesaian operasi tulis ke aplikasi cadangan Anda.

Untuk panduan tentang jumlah ruang disk yang akan dialokasikan untuk penyimpanan cache dan buffer unggahan, lihat [Menentukan jumlah penyimpanan disk lokal](#)

Harga Storage Gateway

Untuk informasi terkini tentang harga, lihat [Harga](#) di halaman AWS Storage Gateway detail.

Rencanakan penyebaran Storage Gateway

Dengan menggunakan perangkat lunak Storage Gateway, Anda dapat menghubungkan infrastruktur aplikasi lokal yang ada dengan penyimpanan AWS cloud yang dapat diskalakan dan hemat biaya yang menyediakan fitur keamanan data.

Untuk menerapkan Storage Gateway, pertama-tama Anda harus memutuskan dua hal berikut:

1. Jenis gateway Anda — panduan ini mencakup jenis gateway berikut:
 - Tape Gateway — Jika Anda mencari alternatif offsite yang hemat biaya, tahan lama, jangka panjang, untuk pengarsipan data, gunakan Tape Gateway. Dengan antarmuka perpustakaan pita virtual (VTL), Anda dapat menggunakan infrastruktur perangkat lunak cadangan berbasis pita yang ada untuk menyimpan data pada kartrid pita virtual yang Anda buat. Untuk informasi selengkapnya, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Saat Anda mengarsipkan kaset, Anda tidak perlu khawatir mengelola kaset di tempat Anda dan mengatur pengiriman kaset di luar lokasi. Untuk ikhtisar arsitektur, lihat [Cara kerja Tape Gateway \(arsitektur\)](#).

2. Opsi hosting - Anda dapat menjalankan Storage Gateway baik lokal sebagai alat VM atau perangkat keras, atau AWS sebagai instans Amazon EC2. Untuk informasi selengkapnya, lihat [Persyaratan](#). Jika pusat data Anda offline dan Anda tidak memiliki host yang tersedia, Anda dapat menerapkan gateway pada instans EC2. Storage Gateway menyediakan Amazon Machine Image (AMI) yang berisi image VM gateway.

Selain itu, saat Anda mengonfigurasi host untuk menyebarkan perangkat lunak gateway, Anda perlu mengalokasikan penyimpanan yang cukup untuk VM gateway.

Sebelum Anda melanjutkan ke langkah berikutnya, pastikan Anda telah melakukan hal berikut:

1. Untuk gateway yang digunakan di lokasi, pilih jenis host VM dan atur. Pilihan Anda adalah VMware ESXi Hypervisor, Microsoft Hyper-V, dan Linux Kernel-based Virtual Machine (KVM). Jika Anda menggunakan gateway di belakang firewall, pastikan port dapat diakses ke VM gateway. Untuk informasi selengkapnya, lihat [Persyaratan](#).
2. Instal perangkat lunak cadangan klien Anda. Untuk informasi selengkapnya, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Memulai

Di bagian ini, Anda dapat menemukan petunjuk tentang cara memulai dengan Storage Gateway. Untuk memulai, Anda mendaftar terlebih dahulu AWS. Jika Anda adalah pengguna pertama kali, kami sarankan Anda membaca bagian wilayah dan persyaratan.

Topik

- [Mendaftar untuk AWS Storage Gateway](#)
- [AWS Daerah](#)
- [Persyaratan](#)
- [Mengakses AWS Storage Gateway](#)

Mendaftar untuk AWS Storage Gateway

Untuk menggunakan Storage Gateway, Anda memerlukan akun Amazon Web Services yang memberi Anda akses ke semua AWS sumber daya, forum, dukungan, dan laporan penggunaan. Anda tidak dikenakan biaya untuk layanan apa pun kecuali jika Anda menggunakannya. Jika Anda sudah memiliki akun Amazon Web Services, Anda dapat melewati langkah ini.

Untuk mendaftar akun Amazon Web Services

1. Buka <https://portal.aws.amazon.com/billing/signup>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

Untuk informasi tentang harga, lihat [Harga](#) di halaman detail Storage Gateway.

AWS Daerah

Storage Gateway menyimpan volume, snapshot, tape, dan data file di AWS Wilayah tempat gateway Anda diaktifkan. Data file disimpan di AWS Wilayah tempat bucket Amazon S3 Anda berada. Anda memilih AWS Wilayah di kanan atas Storage Gateway Management Console sebelum mulai menerapkan gateway Anda.

- Gateway Penyimpanan—Untuk AWS Wilayah yang didukung dan daftar titik akhir AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat Titik [AWS Storage Gateway Akhir](#) dan Kuota di. Referensi Umum AWS
- Storage Gateway Hardware Appliance—Untuk AWS Wilayah yang didukung yang dapat Anda gunakan dengan perangkat keras, lihat Wilayah [Peralatan AWS Storage Gateway Perangkat Keras](#) di. Referensi Umum AWS

Persyaratan

Kecuali dinyatakan lain, persyaratan berikut ini umum untuk semua konfigurasi gateway.

Topik

- [Persyaratan perangkat keras dan penyimpanan](#)
- [Persyaratan jaringan dan firewall](#)
- [Hypervisor dan persyaratan host yang didukung](#)
- [Pemrakarsa iSCSI yang didukung](#)
- [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#)

Persyaratan perangkat keras dan penyimpanan

Bagian ini menjelaskan perangkat keras dan pengaturan minimum untuk gateway Anda dan jumlah minimum ruang disk yang akan dialokasikan untuk penyimpanan yang diperlukan.

Persyaratan perangkat keras untuk VM

Saat menerapkan gateway Anda, Anda harus memastikan bahwa perangkat keras yang mendasari tempat Anda menggunakan VM gateway dapat mendedikasikan sumber daya minimum berikut:

- Empat prosesor virtual ditugaskan ke VM.

- Untuk Tape Gateway, perangkat keras Anda harus mendedikasikan jumlah RAM berikut:
 - 16 GiB RAM cadangan untuk gateway dengan ukuran cache hingga 16 TiB
 - 32 GiB RAM cadangan untuk gateway dengan ukuran cache 16 TiB hingga 32 TiB
 - 48 GiB RAM cadangan untuk gateway dengan ukuran cache 32 TiB hingga 64 TiB
- 80 GiB ruang disk untuk pemasangan gambar VM dan data sistem.

Untuk informasi selengkapnya, lihat [Mengoptimalkan Kinerja Gateway](#). Untuk informasi tentang bagaimana perangkat keras Anda memengaruhi kinerja VM gateway, lihat [AWS Storage Gateway kuota](#).

Persyaratan untuk jenis instans Amazon EC2

Saat menerapkan gateway di Amazon Elastic Compute Cloud (Amazon EC2), ukuran instans minimal harus xlarge agar gateway berfungsi. Namun, untuk keluarga instance yang dioptimalkan komputasi, ukurannya harus minimal 2xlarge.

Untuk Tape Gateway, instans Amazon EC2 Anda harus mendedikasikan jumlah RAM berikut tergantung pada ukuran cache yang Anda rencanakan untuk digunakan untuk gateway Anda:

- 16 GiB RAM cadangan untuk gateway dengan ukuran cache hingga 16 TiB
- 32 GiB RAM cadangan untuk gateway dengan ukuran cache 16 TiB hingga 32 TiB
- 48 GiB RAM cadangan untuk gateway dengan ukuran cache 32 TiB hingga 64 TiB

Gunakan salah satu jenis contoh berikut yang direkomendasikan untuk jenis gateway Anda.

Direkomendasikan untuk volume cache dan tipe Tape Gateway

- Keluarga instance tujuan umum — tipe instans m4, m5, atau m6.

Note

Kami tidak menyarankan menggunakan tipe instance m4.16xlarge.

- Keluarga instans yang dioptimalkan komputasi — tipe instans c4, c5, atau c6. Pilih ukuran instans 2xlarge atau lebih tinggi untuk memenuhi persyaratan RAM yang diperlukan.
- Keluarga instans yang dioptimalkan untuk memori — tipe instans r3, r5, atau r6.

- Keluarga instans yang dioptimalkan untuk penyimpanan — tipe instans i3 atau i4.

Persyaratan penyimpanan

Selain ruang disk 80 GiB untuk VM, Anda juga memerlukan disk tambahan untuk gateway Anda.

Tabel berikut merekomendasikan ukuran untuk penyimpanan disk lokal untuk gateway yang Anda gunakan.

Jenis Gateway	Cache (Minimum)	Cache (Maksimum)	Unggah Buffer (Minimum)	Unggah Buffer (Maksimum)	Disk Lokal Lain yang Diperlukan
Gerbang Pita	150 GiB	64 TiB	150 GiB	2 TiB	—

Note

Anda dapat mengonfigurasi satu atau lebih drive lokal untuk cache Anda dan mengunggah buffer, hingga kapasitas maksimum.

Saat menambahkan cache atau mengunggah buffer ke gateway yang ada, penting untuk membuat disk baru di host Anda (hypervisor atau instans Amazon EC2). Jangan mengubah ukuran disk yang ada jika disk sebelumnya telah dialokasikan sebagai cache atau buffer unggahan.

Untuk informasi tentang kuota gateway, lihat [AWS Storage Gateway kuota](#).

Persyaratan jaringan dan firewall

Gateway Anda memerlukan akses ke internet, jaringan lokal, server Domain Name Service (DNS), firewall, router, dan sebagainya. Berikut ini, Anda dapat menemukan informasi tentang port yang diperlukan dan cara mengizinkan akses melalui firewall dan router.

Note

Dalam beberapa kasus, Anda dapat menerapkan Storage Gateway di Amazon EC2 atau menggunakan jenis penerapan lain (termasuk lokal) dengan kebijakan keamanan

jaringan yang AWS membatasi rentang alamat IP. Dalam kasus ini, gateway Anda mungkin mengalami masalah konektivitas layanan saat nilai rentang AWS IP berubah. Nilai rentang alamat AWS IP yang perlu Anda gunakan ada di subset layanan Amazon untuk AWS Wilayah tempat Anda mengaktifkan gateway Anda. Untuk nilai rentang IP saat ini, lihat [rentang alamat AWS IP](#) di Referensi Umum AWS.

Note

Persyaratan bandwidth jaringan bervariasi berdasarkan jumlah data yang diunggah dan diunduh oleh gateway. Minimal 100Mbps diperlukan untuk berhasil mengunduh, mengaktifkan, dan memperbarui gateway. Pola transfer data Anda akan menentukan bandwidth yang diperlukan untuk mendukung beban kerja Anda. Dalam beberapa kasus, Anda dapat menerapkan Storage Gateway di Amazon EC2 atau menggunakan jenis penerapan lainnya

Topik

- [Persyaratan pelabuhan](#)
- [Persyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance](#)
- [Mengizinkan AWS Storage Gateway akses melalui firewall dan router](#)
- [Mengonfigurasi grup keamanan untuk instans gateway Amazon EC2](#)

Persyaratan pelabuhan

Storage Gateway mengharuskan port tertentu diizinkan untuk operasinya. Ilustrasi berikut menunjukkan port yang diperlukan yang harus Anda izinkan untuk setiap jenis gateway. Beberapa port diperlukan oleh semua jenis gateway, dan yang lainnya diperlukan oleh jenis gateway tertentu. Untuk informasi selengkapnya tentang persyaratan port, lihat [Persyaratan Pelabuhan](#).

Port umum untuk semua jenis gateway

Port berikut umum untuk semua jenis gateway dan diperlukan oleh semua jenis gateway.

Protokol	Port	Arahan	Sumber	Tujuan	Bagaimana Digunakan
TCP	443 (HTTPS)	Ke luar	Storage Gateway	AWS	Untuk komunikasi dari Storage Gateway ke titik akhir AWS layanan. Untuk informasi tentang titik akhir layanan, lihat Mengizinkan AWS Storage Gateway akses melalui firewall dan router .
TCP	80 (HTTP)	Ke dalam	Host tempat Anda terhubung ke AWS Management Console.	Storage Gateway	Dengan sistem lokal untuk mendapatkan kunci aktivasi Storage Gateway. Port 80 hanya digunakan selama aktivasi alat

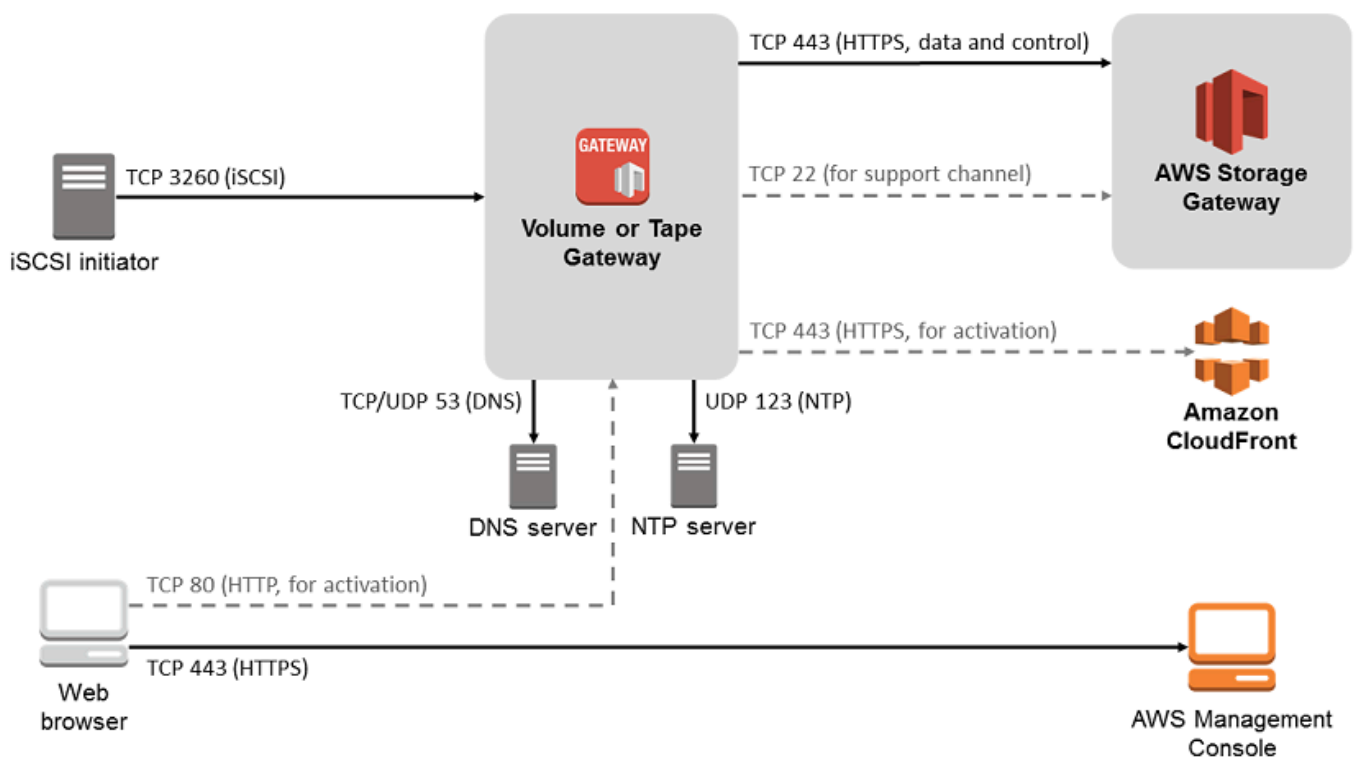
Protokol	Port	Arahan	Sumber	Tujuan	Bagaimana Digunakan
					<p>Storage Gateway.</p> <p>Storage Gateway tidak memerlukan port 80 untuk dapat diakses publik. Tingkat akses yang diperlukan ke port 80 tergantung pada konfigurasi jaringan Anda. Jika Anda mengaktifkan gateway dari Storage Gateway Management Console, host tempat Anda terhubung ke konsol harus memiliki akses ke port gateway 80 Anda.</p>

Protokol	Port	Arahan	Sumber	Tujuan	Bagaimana Digunakan
TCP/UDP	53 (DNS)	Ke luar	Storage Gateway	Server Domain Name Service (DNS)	Untuk komunikasi antara Storage Gateway dan server DNS.
TCP	22 (Saluran dukungan)	Ke luar	Storage Gateway	AWS Support	Memungkinkan AWS Support untuk mengakses gateway Anda untuk membantu Anda mengatasi masalah gateway. Anda tidak perlu port ini terbuka untuk operasi normal gateway Anda, tetapi diperlukan untuk pemecahan masalah.

Protokol	Port	Arahan	Sumber	Tujuan	Bagaimana Digunakan
UDP	123 (NTP)	Ke luar	Klien NTP	Server NTP	Digunakan oleh sistem lokal untuk menyinkronkan waktu VM ke waktu host.

Port untuk volume dan Tape Gateways

Ilustrasi berikut menunjukkan port yang akan dibuka untuk .



Selain port umum, Tape Gateway memerlukan port berikut.

Protokol	Port	Arahan	Sumber	Tujuan	Bagaimana Digunakan
TCP	3260 (iSCSI)	Ke dalam	Inisiator iSCSI	Storage Gateway	Dengan sistem lokal untuk terhubung ke target iSCSI yang diekspos oleh gateway.

Untuk informasi rinci tentang persyaratan port, lihat [Persyaratan Pelabuhan](#) di bagian Sumber daya Gateway Penyimpanan Tambahan.

Persyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance

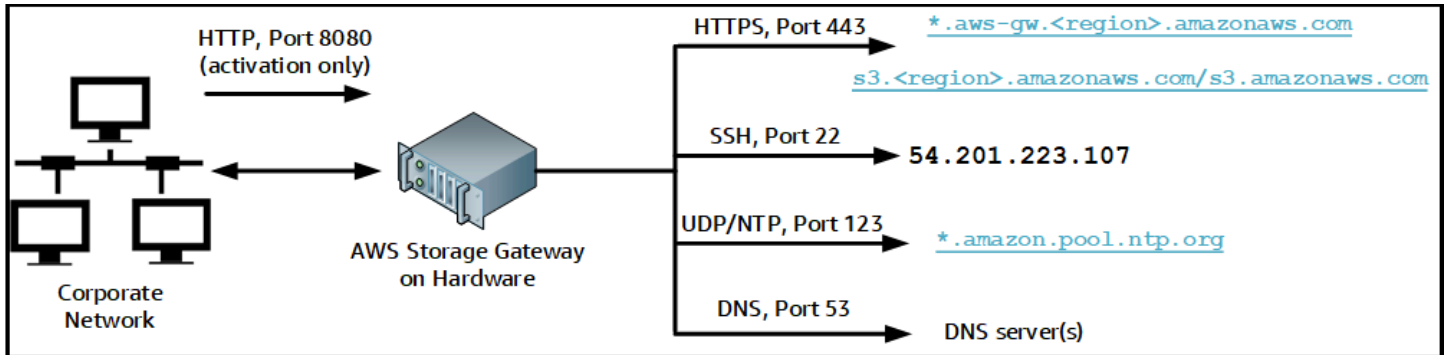
Setiap Storage Gateway Hardware Appliance memerlukan layanan jaringan berikut:

- Akses Internet — koneksi jaringan yang selalu aktif ke internet melalui antarmuka jaringan apa pun di server.
- Layanan DNS — Layanan DNS untuk komunikasi antara perangkat keras dan server DNS.
- Sinkronisasi waktu - layanan waktu Amazon NTP yang dikonfigurasi secara otomatis harus dapat dijangkau.
- Alamat IP — Alamat DHCP atau IPv4 statis yang ditetapkan. Anda tidak dapat menetapkan alamat IPv6.

Ada lima port jaringan fisik di bagian belakang server Dell PowerEdge R640. Dari kiri ke kanan (menghadap ke belakang server) port ini adalah sebagai berikut:

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

Anda dapat menggunakan port IDRac untuk manajemen server jarak jauh.



Alat perangkat keras membutuhkan port berikut untuk beroperasi.

Protokol	Port	Arahan	Sumber	Tujuan	Bagaimana Digunakan
SSH	22	Ke luar	Alat perangkat keras	54.201.223.107	Saluran dukungan
DNS	53	Ke luar	Alat perangkat keras	Server DNS	Resolusi nama
UDP/NTP	123	Ke luar	Alat perangkat keras	*.amazon.pool.ntp.org	Sinkronisasi waktu
HTTPS	443	Ke luar	Alat perangkat keras	*.amazonaws.com	Transfer data
HTTP	8080	Ke dalam	AWS	Alat perangkat keras	Aktivasi (hanya sebentar)

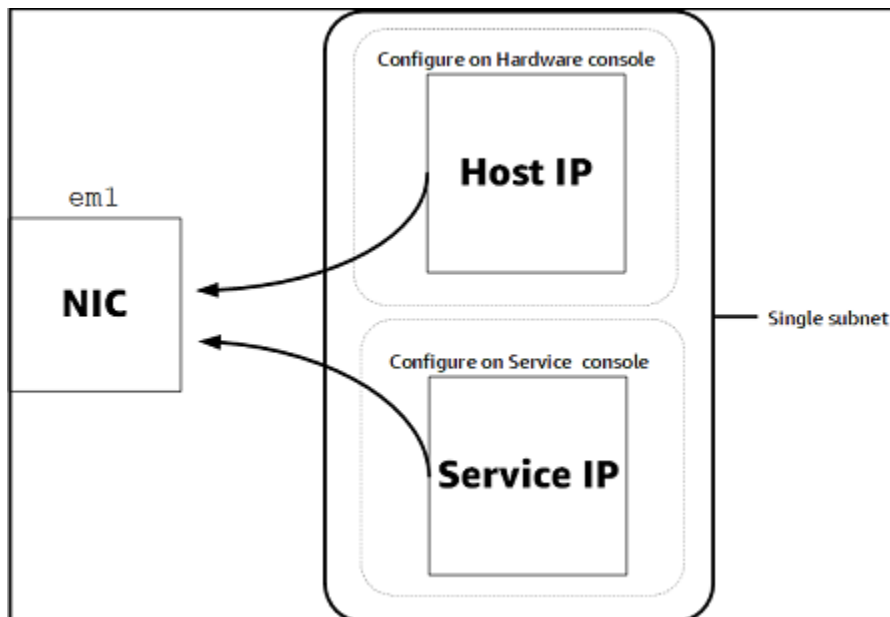
Untuk melakukan seperti yang dirancang, alat perangkat keras memerlukan pengaturan jaringan dan firewall sebagai berikut:

- Konfigurasi semua antarmuka jaringan yang terhubung di konsol perangkat keras.
- Pastikan bahwa setiap antarmuka jaringan berada pada subnet yang unik.
- Sediakan semua antarmuka jaringan yang terhubung dengan akses keluar ke titik akhir yang tercantum dalam diagram sebelumnya.
- Konfigurasi setidaknya satu antarmuka jaringan untuk mendukung alat perangkat keras. Untuk informasi selengkapnya, lihat [Mengkonfigurasi parameter jaringan](#).

Note

Untuk ilustrasi yang menunjukkan bagian belakang server dengan port-portnya, lihat [Memasang rak alat perangkat keras Anda dan menghubungkannya ke daya](#)

Semua alamat IP pada antarmuka jaringan yang sama (NIC), baik untuk gateway atau host, harus berada di subnet yang sama. Ilustrasi berikut menunjukkan skema pengalamatan.



Untuk informasi selengkapnya tentang mengaktifkan dan mengonfigurasi perangkat keras, lihat [Menggunakan Storage Gateway Hardware Appliance](#)

Mengizinkan AWS Storage Gateway akses melalui firewall dan router

Gateway Anda memerlukan akses ke titik akhir layanan berikut untuk berkomunikasi AWS. Jika Anda menggunakan firewall atau router untuk memfilter atau membatasi lalu lintas jaringan, Anda harus

mengonfigurasi firewall dan router Anda untuk mengizinkan titik akhir layanan ini untuk komunikasi keluar. AWS

Note

Jika Anda mengonfigurasi titik akhir VPC pribadi untuk Storage Gateway Anda untuk digunakan untuk koneksi dan transfer data ke dan dari AWS, gateway Anda tidak memerlukan akses ke internet publik. Untuk informasi selengkapnya, lihat [Mengaktifkan gateway di cloud pribadi virtual](#).

Important

Bergantung pada AWS Wilayah gateway Anda, ganti *wilayah* di titik akhir layanan dengan string wilayah yang benar.

Titik akhir layanan berikut diperlukan oleh semua gateway untuk operasi head-bucket.

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

Titik akhir layanan berikut diperlukan oleh semua gateway untuk operasi jalur kontrol (anon-cp, client-cp, proxy-app) dan jalur data (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
```

Titik akhir layanan gateway berikut diperlukan untuk melakukan panggilan API.

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

Contoh berikut adalah titik akhir layanan gateway di Wilayah AS Barat (Oregon) (us-west-2).

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

Titik akhir layanan Amazon S3, yang ditunjukkan berikut, hanya digunakan oleh File Gateways. File Gateway memerlukan titik akhir ini untuk mengakses bucket S3 tempat file berbagi peta.

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

Contoh berikut adalah titik akhir layanan S3 di Wilayah AS Timur (Ohio) (). us-east-2

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

Note

Jika gateway Anda tidak dapat menentukan AWS Wilayah tempat bucket S3 Anda berada, titik akhir layanan ini akan menjadi default. `s3.us-east-1.amazonaws.com` Kami menyarankan Anda mengizinkan akses ke Wilayah AS Timur (Virginia Utara) (us-east-1) selain AWS Wilayah tempat gateway Anda diaktifkan, dan di mana bucket S3 Anda berada.

Berikut ini adalah titik akhir layanan S3 untuk AWS GovCloud (US) Wilayah.

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

Contoh berikut adalah endpoint layanan FIPS untuk bucket S3 di Wilayah AWS GovCloud (AS-Barat).

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

VM Storage Gateway dikonfigurasi untuk menggunakan server NTP berikut.

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

- Gateway Penyimpanan—Untuk AWS Wilayah yang didukung dan daftar titik akhir AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat titik [AWS Storage Gateway akhir](#) dan kuota di Referensi Umum AWS

- Storage Gateway Hardware Appliance—Untuk AWS Wilayah yang didukung yang dapat Anda gunakan dengan [alat perangkat keras, lihat wilayah perangkat keras Storage Gateway](#) di Referensi Umum AWS

Mengonfigurasi grup keamanan untuk instans gateway Amazon EC2

Grup keamanan mengontrol lalu lintas ke instans gateway Amazon EC2 Anda. Saat Anda mengonfigurasi grup keamanan, kami merekomendasikan hal berikut:

- Kelompok keamanan tidak boleh mengizinkan koneksi masuk dari internet luar. Seharusnya hanya mengizinkan instance dalam grup keamanan gateway untuk berkomunikasi dengan gateway. Jika Anda perlu mengizinkan instance untuk terhubung ke gateway dari luar grup keamanannya, kami sarankan Anda mengizinkan koneksi hanya pada port 3260 (untuk koneksi iSCSI) dan 80 (untuk aktivasi).
- Jika Anda ingin mengaktifkan gateway Anda dari host Amazon EC2 di luar grup keamanan gateway, izinkan koneksi masuk pada port 80 dari alamat IP host tersebut. Jika Anda tidak dapat menentukan alamat IP host pengaktif, Anda dapat membuka port 80, mengaktifkan gateway Anda, dan kemudian menutup akses pada port 80 setelah menyelesaikan aktivasi.
- Izinkan akses port 22 hanya jika Anda menggunakan AWS Support untuk tujuan pemecahan masalah. Untuk informasi selengkapnya, lihat [Anda AWS Support ingin membantu memecahkan masalah gateway EC2 Anda](#).

Dalam beberapa kasus, Anda mungkin menggunakan instans Amazon EC2 sebagai inisiator (yaitu, untuk menyambung ke target iSCSI pada gateway yang Anda gunakan di Amazon EC2. Dalam kasus seperti itu, kami merekomendasikan pendekatan dua langkah:

1. Anda harus meluncurkan instance inisiator dalam grup keamanan yang sama dengan gateway Anda.
2. Anda harus mengkonfigurasi akses sehingga inisiator dapat berkomunikasi dengan gateway Anda.

Untuk informasi tentang port yang akan dibuka untuk gateway Anda, lihat [Persyaratan Pelabuhan](#).

Hypervisor dan persyaratan host yang didukung

Anda dapat menjalankan Storage Gateway lokal sebagai alat mesin virtual (VM), atau alat perangkat keras fisik, atau AWS sebagai instans Amazon EC2.

Note

Ketika produsen mengakhiri dukungan umum untuk versi hypervisor, Storage Gateway juga mengakhiri dukungan untuk versi hypervisor tersebut. Untuk informasi rinci tentang dukungan untuk versi hypervisor tertentu, lihat dokumentasi pabrikan.

Storage Gateway mendukung versi dan host hypervisor berikut:

- [VMware ESXi Hypervisor \(versi 7.0 atau 8.0\) - Versi gratis VMware tersedia di situs web VMware.](#) Untuk pengaturan ini, Anda juga memerlukan klien VMware vSphere untuk terhubung ke host.
- [Microsoft Hyper-V Hypervisor \(versi 2012 R2, 2016, 2019, atau 2022\) — Hyper-V versi mandiri gratis tersedia di Microsoft Download Center.](#) Untuk penyiapan ini, Anda memerlukan Microsoft Hyper-V Manager pada komputer klien Microsoft Windows untuk terhubung ke host.
- Mesin Virtual berbasis Kernel Linux (KVM) – Sebuah teknologi virtualisasi gratis, sumber terbuka. KVM disertakan dalam semua versi Linux versi 2.6.20 dan yang lebih baru. Storage Gateway diuji dan didukung untuk distribusi CentOS/RHEL 7.7, Ubuntu 16.04 LTS, dan Ubuntu 18.04 LTS. Distribusi Linux modern lainnya dapat berfungsi, tetapi fungsi atau kinerja tidak dijamin. Kami merekomendasikan opsi ini jika Anda sudah memiliki lingkungan KVM yang aktif dan berjalan dan Anda sudah terbiasa dengan cara kerja KVM.
- Instans Amazon EC2 — Storage Gateway menyediakan Amazon Machine Image (AMI) yang berisi image VM gateway. Hanya jenis file, volume cache, dan Tape Gateway yang dapat digunakan di Amazon EC2. Untuk informasi tentang cara menerapkan gateway di Amazon EC2, lihat [Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway](#)
- Storage Gateway Hardware Appliance — Storage Gateway menyediakan perangkat keras fisik sebagai opsi penyebaran lokal untuk lokasi dengan infrastruktur mesin virtual terbatas.

Note

Storage Gateway tidak mendukung pemulihan gateway dari VM yang dibuat dari snapshot atau klon VM gateway lain atau dari Amazon EC2 AMI Anda. Jika VM gateway Anda tidak berfungsi, aktifkan gateway baru dan pulihkan data Anda ke gateway itu. Untuk informasi selengkapnya, lihat [Memulihkan dari shutdown mesin virtual yang tidak terduga.](#) Storage Gateway tidak mendukung memori dinamis dan balon memori virtual.

Pemrakarsa iSCSI yang didukung

Saat Anda menggunakan Tape Gateway, gateway sudah dikonfigurasi sebelumnya dengan satu media changer dan 10 tape drive. Tape drive dan media changer ini tersedia untuk aplikasi cadangan klien Anda yang ada sebagai perangkat iSCSI.

Untuk terhubung ke perangkat iSCSI ini, Storage Gateway mendukung inisiator iSCSI berikut:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Perusahaan Topi Merah Linux 5
- Perusahaan Topi Merah Linux 6
- Red Hat Enterprise Linux 7
- VMware ESX Initiator, yang menyediakan alternatif untuk menggunakan inisiator dalam sistem operasi tamu VM Anda

Important


Storage Gateway tidak mendukung Microsoft Multipath I/O (MPIO) dari klien Windows. Storage Gateway mendukung menghubungkan beberapa host ke volume yang sama jika host mengoordinasikan akses dengan menggunakan Windows Server Failover Clustering (WSFC). Namun, Anda tidak dapat menghubungkan beberapa host ke volume yang sama (misalnya, berbagi sistem file NTFS/Ext4 yang tidak dikelompokkan) tanpa menggunakan WSFC.

Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway

Anda menggunakan aplikasi cadangan untuk membaca, menulis, dan mengelola kaset dengan Tape Gateway. Aplikasi cadangan pihak ketiga berikut didukung untuk bekerja dengan Tape Gateways.

Jenis medium changer yang Anda pilih tergantung pada aplikasi cadangan yang Anda rencanakan untuk digunakan. Tabel berikut mencantumkan aplikasi cadangan pihak ketiga yang telah diuji dan

ditemukan kompatibel dengan Tape Gateways. Tabel ini mencakup tipe medium changer yang direkomendasikan untuk setiap aplikasi backup.

Aplikasi Backup	Jenis Pengubah Sedang
Cadangan Arcserve	AWS-Gateway-VTL
Bacula Perusahaan V10.x	AWS-Gateway-VTL atau STK-L700
Commvault V11	STK-L700
Dell EMC 19,5 NetWorker	AWS-Gateway-VTL
IBM Spectrum Melindungi v8.1.10	IBM-03584L32-0402
Pelindung Data Fokus Mikro (HPE) 9 atau 11.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 atau 2016 Manajer Perlindungan Data	STK-L700
NovaStor DataCenter/Jaringan 6.4 atau 7.1	STK-L700
NetVault Cadangan Quest 12.4 atau 13.x	STK-L700
Cadangan & Replikasi Veeam 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014 atau 15 atau 16 atau 20 atau 22.x	AWS-Gateway-VTL
Eksekutif Cadangan Veritas 2012	STK-L700
<div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note Veritas telah mengakhiri dukungan untuk Backup Exec 2012.</p> </div>	
Veritas NetBackup Versi 7.x atau 8.x	AWS-Gateway-VTL

⚠ Important

Kami sangat menyarankan Anda memilih medium changer yang terdaftar untuk aplikasi backup Anda. Pengubah media lainnya mungkin tidak berfungsi dengan baik. Anda dapat memilih medium changer yang berbeda setelah gateway diaktifkan. Untuk informasi selengkapnya, lihat [Memilih Pengubah Medium Setelah Aktivasi Gateway](#).

Mengakses AWS Storage Gateway

Anda dapat menggunakan [Storage Gateway Management Console](#) untuk melakukan berbagai konfigurasi gateway dan tugas manajemen. Bagian Memulai dan berbagai bagian lain dari panduan ini menggunakan konsol untuk menggambarkan fungsionalitas gateway.

Untuk mengizinkan akses browser ke konsol Storage Gateway, pastikan browser Anda memiliki akses ke titik akhir Storage Gateway API. Untuk informasi selengkapnya, lihat [titik akhir dan kuota Storage Gateway di Referensi AWS](#) Umum.

Selain itu, Anda dapat menggunakan AWS Storage Gateway API untuk mengonfigurasi dan mengelola gateway secara terprogram. Untuk informasi selengkapnya tentang API, lihat [Referensi API untuk Storage Gateway](#).

Anda juga dapat menggunakan AWS SDK untuk mengembangkan aplikasi yang berinteraksi dengan Storage Gateway. AWS SDK untuk Java, .NET, dan PHP membungkus Storage Gateway API yang mendasarinya untuk menyederhanakan tugas pemrograman Anda. Untuk informasi tentang mengunduh pustaka SDK, lihat [Pustaka Kode Contoh](#).

Menggunakan Storage Gateway Hardware Appliance

Storage Gateway Hardware Appliance adalah perangkat keras fisik dengan perangkat lunak Storage Gateway yang sudah diinstal sebelumnya pada konfigurasi server yang divalidasi. Anda dapat mengelola peralatan perangkat keras Anda dari halaman ikhtisar alat perangkat keras di AWS Storage Gateway konsol.

Perangkat perangkat keras adalah server 1U berkinerja tinggi yang dapat Anda gunakan di pusat data, atau lokal di dalam firewall perusahaan Anda. Saat Anda membeli dan mengaktifkan perangkat keras, proses aktivasi mengaitkan perangkat keras Anda dengan akun Amazon Web Services Anda. Setelah aktivasi, perangkat keras Anda muncul di konsol sebagai gateway di halaman ikhtisar perangkat keras. Anda dapat mengonfigurasi perangkat keras Anda sebagai tipe File Gateway, Tape Gateway, atau Volume Gateway. Prosedur yang Anda gunakan untuk menyebarkan dan mengaktifkan jenis gateway ini pada alat perangkat keras sama dengan pada platform virtual.

Di bagian berikut, Anda dapat menemukan petunjuk tentang cara memesan, mengatur, mengonfigurasi, mengaktifkan, meluncurkan, dan menggunakan Storage Gateway Hardware Appliance.

Topik

- [Informasi Pemesanan](#)
- [AWS Wilayah yang didukung](#)
- [Menyiapkan alat perangkat keras Anda](#)
- [Memasang rak alat perangkat keras Anda dan menghubungkannya ke daya](#)
- [Mengkonfigurasi parameter jaringan](#)
- [Mengaktifkan alat perangkat keras Anda](#)
- [Membuat gateway](#)
- [Mengkonfigurasi alamat IP untuk gateway](#)
- [Mengkonfigurasi gateway Anda](#)
- [Menghapus gateway dari alat perangkat keras](#)
- [Menghapus alat perangkat keras Anda](#)

Informasi Pemesanan

Alat AWS Storage Gateway perangkat keras tersedia secara eksklusif melalui pengecer. Silakan hubungi reseller pilihan Anda untuk informasi pembelian dan untuk meminta penawaran.

AWS Wilayah yang didukung

Untuk daftar yang didukung Wilayah AWS di mana Storage Gateway Hardware Appliance tersedia untuk aktivasi dan penggunaan, lihat [Storage Gateway Hardware Appliance Regions](#) di Referensi Umum AWS.

Menyiapkan alat perangkat keras Anda

Setelah menerima Storage Gateway Hardware Appliance, Anda menggunakan konsol perangkat keras untuk mengonfigurasi jaringan guna menyediakan koneksi yang selalu aktif AWS dan mengaktifkan alat Anda. Aktivasi mengaitkan perangkat Anda dengan akun Amazon Web Services yang digunakan selama proses aktivasi. Setelah alat diaktifkan, Anda dapat meluncurkan file, volume, atau Tape Gateway dari konsol Storage Gateway.

Note

Ini adalah tanggung jawab Anda untuk memastikan firmware alat perangkat keras up-to-date.

Untuk menginstal dan mengkonfigurasi alat perangkat keras Anda

1. Pasang alat di rak, dan colokkan koneksi daya dan jaringan. Untuk informasi selengkapnya, lihat [Memasang rak alat perangkat keras Anda dan menghubungkannya ke daya](#).
2. Atur alamat Internet Protocol versi 4 (IPv4) untuk perangkat keras (host) dan Storage Gateway (layanan). Untuk informasi selengkapnya, lihat [Mengkonfigurasi parameter jaringan](#).
3. Aktifkan alat perangkat keras di halaman ikhtisar alat perangkat keras konsol di AWS Wilayah pilihan Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan alat perangkat keras Anda](#).
4. Instal Storage Gateway di perangkat perangkat keras Anda. Untuk informasi selengkapnya, lihat [Mengkonfigurasi gateway Anda](#).

Anda mengatur gateway pada perangkat keras Anda dengan cara yang sama seperti Anda mengatur gateway di VMware ESXi, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), atau Amazon EC2.

Meningkatkan penyimpanan cache yang dapat digunakan

Anda dapat meningkatkan penyimpanan yang dapat digunakan pada alat perangkat keras dari 5 TB menjadi 12 TB. Melakukan hal ini menyediakan cache yang lebih besar untuk akses latensi rendah ke data di AWS. Jika Anda memesan model 5 TB, Anda dapat meningkatkan penyimpanan yang dapat digunakan menjadi 12 TB dengan membeli lima SSD 1,92 TB (solid state drive).

Anda kemudian dapat menambahkannya ke alat perangkat keras sebelum Anda mengaktifkannya. Jika Anda telah mengaktifkan alat perangkat keras dan ingin meningkatkan penyimpanan yang dapat digunakan pada alat menjadi 12 TB, lakukan hal berikut:

1. Setel ulang alat perangkat keras ke pengaturan pabriknya. Hubungi Amazon Web Services Support untuk petunjuk tentang cara melakukannya.
2. Tambahkan lima SSD 1,92 TB ke alat.

Opsi kartu antarmuka jaringan

Tergantung pada model alat yang Anda pesan, mungkin dilengkapi dengan kartu jaringan tembaga 10G-Base-T atau kartu jaringan 10G DA/SFP+.

- Konfigurasi NIC 10G-Base-T:
 - Gunakan kabel CAT6 untuk 10G atau CAT5 (e) untuk 1G
- Konfigurasi 10G DA/SFP+NIC:
 - Gunakan Kabel Twinax tembaga Direct Attach hingga 5 meter
 - Modul optik SFP+ yang kompatibel dengan Dell/Intel (SR atau LR)
 - Transceiver tembaga SFP/SFP+ untuk 1G-Base-T atau 10G-Base-T

Memasang rak alat perangkat keras Anda dan menghubungkannya ke daya

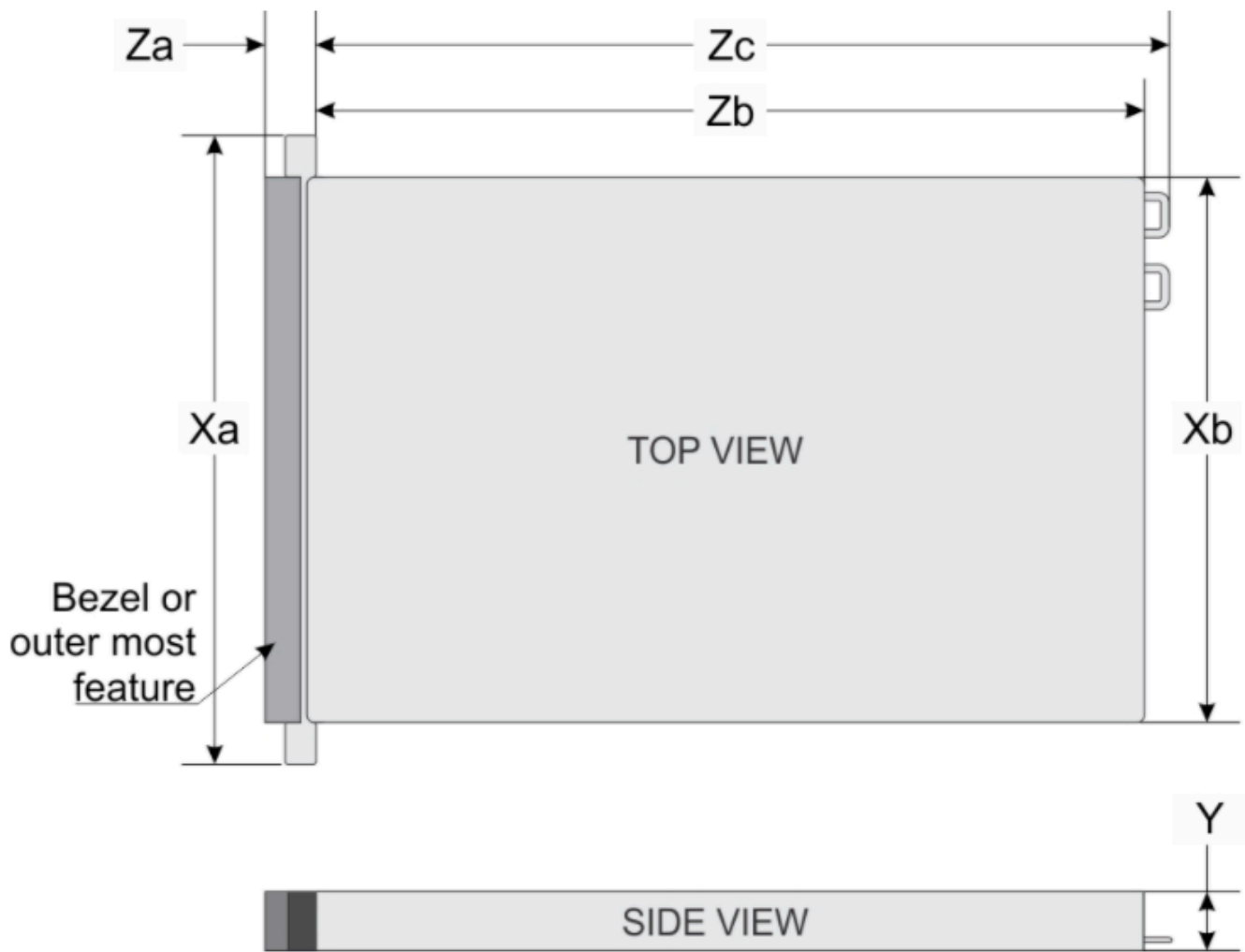
Setelah membuka kotak Storage Gateway Hardware Appliance, ikuti petunjuk yang terdapat di kotak untuk memasang rak server. Alat Anda memiliki faktor bentuk 1U dan cocok dengan rak 19 inci yang sesuai dengan Komisi Elektroteknik Internasional (IEC) standar.

Untuk menginstal alat perangkat keras Anda, Anda memerlukan komponen berikut:

- Kabel daya: satu diperlukan, dua direkomendasikan.
- Kabel jaringan yang didukung (tergantung pada Kartu Antarmuka Jaringan (NIC) yang disertakan dalam alat perangkat keras). Twinax Copper DAC, modul optik SFP+(kompatibel dengan Intel) atau transceiver tembaga SFP ke Base-T.
- Keyboard dan monitor, atau solusi sakelar keyboard, video, dan mouse (KVM).

Dimensi alat perangkat keras

dimensi alat perangkat keras termasuk braket pemasangan dan bezel.



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

dimensi alat perangkat keras termasuk braket pemasangan dan bezel.

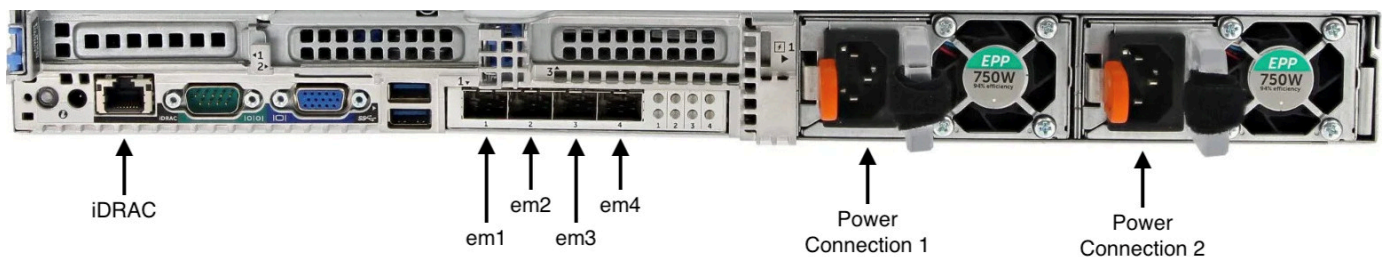
Untuk menghubungkan alat perangkat keras ke daya

Note

Sebelum Anda melakukan prosedur berikut, pastikan bahwa Anda memenuhi semua persyaratan untuk Storage Gateway Hardware Appliance seperti yang dijelaskan dalam [Persyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance](#).

1. Colokkan sambungan daya ke masing-masing dari dua catu daya. Dimungkinkan untuk menghubungkan hanya ke satu koneksi daya, tetapi kami merekomendasikan koneksi daya ke kedua catu daya.

Pada gambar berikut, Anda dapat melihat alat perangkat keras dengan koneksi yang berbeda. alat perangkat keras belakang dengan label konektor jaringan dan daya.



alat perangkat keras belakang dengan label konektor jaringan dan daya.

2. Colokkan kabel Ethernet ke em1 port untuk menyediakan koneksi internet yang selalu aktif. em1Port adalah yang pertama dari empat port jaringan fisik di belakang, dari kiri ke kanan.

Note

Alat perangkat keras tidak mendukung trunking VLAN. Siapkan port sakelar tempat Anda menghubungkan alat perangkat keras sebagai port VLAN non-trunked.

3. Colokkan keyboard dan monitor.
4. Nyalakan server dengan menekan tombol Power di panel depan, seperti yang ditunjukkan pada gambar berikut.
bagian depan alat perangkat keras dengan label tombol daya.



bagian depan alat perangkat keras dengan label tombol daya.

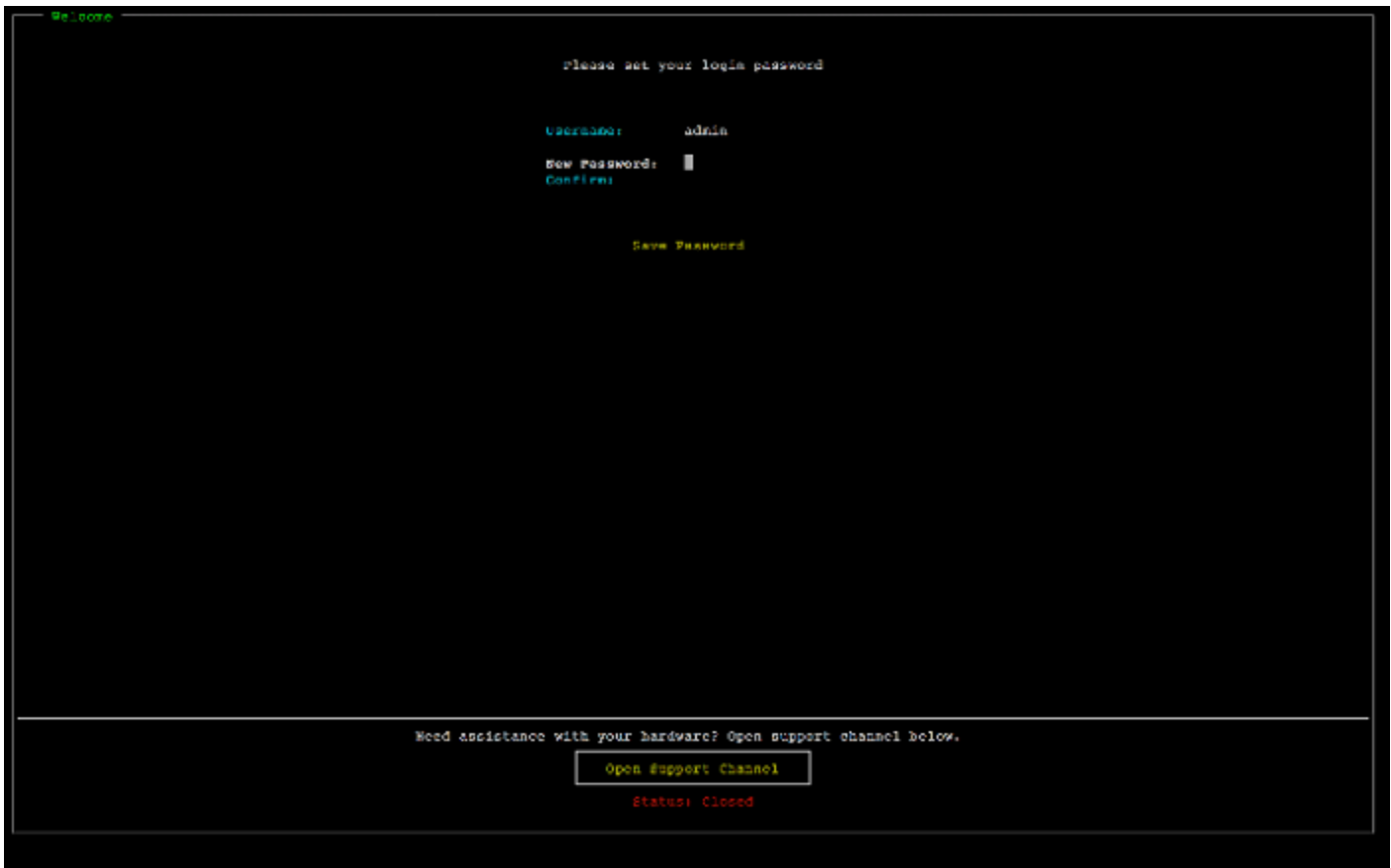
Setelah server boot, konsol perangkat keras muncul di monitor. Konsol perangkat keras menyajikan antarmuka pengguna khusus AWS yang dapat Anda gunakan untuk mengonfigurasi parameter jaringan awal. Anda mengonfigurasi parameter ini untuk menghubungkan alat AWS dan membuka saluran dukungan untuk pemecahan masalah oleh Amazon Web Services Support.

Untuk bekerja dengan konsol perangkat keras, masukkan teks dari keyboard dan gunakan Up,, DownRight, dan Left Arrow tombol untuk bergerak di sekitar layar ke arah yang ditunjukkan. Gunakan Tab tombol untuk bergerak maju secara berurutan melalui item di layar. Pada beberapa pengaturan, Anda dapat menggunakan Shift+Tab penekanan tombol untuk bergerak mundur secara berurutan. Gunakan Enter tombol untuk menyimpan pilihan, atau untuk memilih tombol di layar.

Untuk mengatur kata sandi untuk pertama kalinya

1. Untuk Atur Kata Sandi, masukkan kata sandi, lalu tekan Down arrow.
2. Untuk Konfirmasi, masukkan kembali kata sandi Anda, lalu pilih Simpan Kata Sandi.

konsol alat perangkat keras mengatur layar dialog kata sandi.



konsol alat perangkat keras mengatur layar dialog kata sandi.

Pada titik ini, Anda berada di konsol perangkat keras, ditunjukkan berikut.
menu utama konsol alat perangkat keras yang menunjukkan koneksi dan opsi menu.



menu utama konsol alat perangkat keras yang menunjukkan koneksi dan opsi menu.

Langkah selanjutnya

[Mengkonfigurasi parameter jaringan](#)

Mengkonfigurasi parameter jaringan

Setelah server boot, Anda dapat memasukkan kata sandi pertama Anda di konsol perangkat keras seperti yang dijelaskan dalam [Memasang rak alat perangkat keras Anda dan menghubungkannya ke daya](#).

Selanjutnya, pada konsol perangkat keras, ambil langkah-langkah berikut untuk mengonfigurasi parameter jaringan sehingga alat perangkat keras Anda dapat terhubung AWS.

Untuk mengatur alamat jaringan

1. Pilih Konfigurasi Jaringan dan tekan Enter tombol. Layar Konfigurasi Jaringan yang ditampilkan berikut muncul.
konsol alat perangkat keras mengkonfigurasi layar jaringan.



konsol alat perangkat keras mengkonfigurasi layar jaringan.

2. Untuk Alamat IP, masukkan alamat IPv4 yang valid dari salah satu sumber berikut:

- Gunakan alamat IPv4 yang ditetapkan oleh server Dynamic Host Configuration Protocol (DHCP) Anda ke port jaringan fisik Anda.

Jika Anda melakukannya, perhatikan alamat IPv4 ini untuk digunakan nanti dalam langkah aktivasi.

- Tetapkan alamat IPv4 statis. Untuk melakukannya, pilih Statis di em1 bagian dan tekan Enter untuk melihat layar Konfigurasi IP Statis yang ditunjukkan berikut.

em1Bagian ini ada di bagian kiri atas dalam kelompok pengaturan port.

Setelah Anda memasukkan alamat IPv4 yang valid, tekan tombol atau. Down arrow Tab

Note

Jika Anda mengonfigurasi antarmuka lain, itu harus menyediakan koneksi selalu aktif yang sama ke AWS titik akhir yang tercantum dalam persyaratan.

konsol alat perangkat keras mengkonfigurasi NIC ke layar IP statis.



konsol alat perangkat keras mengkonfigurasi NIC ke layar IP statis.

3. Untuk Subnet, masukkan subnet mask yang valid, lalu tekan. Down arrow
4. Untuk Gateway, masukkan alamat IPv4 gateway jaringan Anda, lalu tekan. Down arrow
5. Untuk DNS1, masukkan alamat IPv4 untuk server Domain Name Service (DNS) Anda, lalu tekan. Down arrow
6. (Opsional) Untuk DNS2, masukkan alamat IPv4 kedua, lalu tekan. Down arrow Penetapan server DNS kedua akan memberikan redundansi tambahan jika server DNS pertama menjadi tidak tersedia.

7. Pilih Simpan dan kemudian tekan Enter untuk menyimpan pengaturan alamat IPv4 statis Anda untuk alat.

Untuk keluar dari konsol perangkat keras

1. Pilih Kembali untuk kembali ke layar Utama.
2. Pilih Logout untuk kembali ke layar Login.

Langkah selanjutnya

[Mengaktifkan alat perangkat keras Anda](#)

Mengaktifkan alat perangkat keras Anda

Setelah mengonfigurasi alamat IP Anda, Anda memasukkan alamat IP ini di halaman Perangkat Keras AWS Storage Gateway konsol untuk mengaktifkan alat perangkat keras Anda. Proses aktivasi memvalidasi bahwa perangkat keras Anda memiliki kredensial keamanan yang sesuai dan mendaftarkan alat ke akun Anda. AWS

Anda dapat memilih untuk mengaktifkan alat perangkat keras Anda di salah satu yang didukung Wilayah AWS. Untuk daftar yang didukung Wilayah AWS, lihat [Storage Gateway Hardware Appliance Regions](#) di Referensi Umum AWS.

Untuk mengaktifkan Storage Gateway Hardware Appliance Anda

1. Buka [Konsol AWS Storage Gateway Manajemen](#) dan masuk dengan kredensial akun yang ingin Anda gunakan untuk mengaktifkan perangkat keras Anda.

Note

Untuk aktivasi saja, berikut ini harus benar:

- Browser Anda harus berada di jaringan yang sama dengan perangkat keras Anda.
- Firewall Anda harus mengizinkan akses HTTP pada port 8080 ke alat untuk lalu lintas masuk.

2. Pilih Hardware dari menu navigasi di sisi kiri halaman.
3. Pilih Aktifkan alat.

4. Untuk Alamat IP, masukkan alamat IP yang Anda konfigurasi untuk perangkat keras Anda, lalu pilih Connect.

Untuk informasi selengkapnya tentang mengonfigurasi alamat IP, lihat [Mengonfigurasi parameter jaringan parameter jaringan](#).

5. Untuk Nama, masukkan nama untuk perangkat keras Anda. Nama dapat mencapai 255 karakter dan tidak dapat menyertakan karakter garis miring.
6. Untuk zona waktu perangkat keras, masukkan zona waktu lokal tempat sebagian besar beban kerja untuk gateway akan dihasilkan., lalu pilih Berikutnya.

Zona waktu mengontrol saat pembaruan perangkat keras berlangsung, dengan jam 2 pagi digunakan sebagai waktu terjadwal default untuk melakukan pembaruan. Idealnya, jika zona waktu diatur dengan benar, pembaruan akan dilakukan di luar jendela hari kerja lokal secara default.

7. Tinjau parameter aktivasi di bagian detail alat perangkat keras. Anda dapat memilih Sebelumnya untuk kembali dan membuat perubahan jika perlu. Jika tidak, pilih Aktifkan untuk menyelesaikan aktivasi.

Spanduk muncul di halaman ikhtisar alat perangkat keras, yang menunjukkan bahwa alat perangkat keras telah berhasil diaktifkan.

Pada titik ini, alat dikaitkan dengan akun Anda. Langkah selanjutnya adalah mengkonfigurasi dan meluncurkan S3 File Gateway, FSx File Gateway, Tape Gateway, atau Volume Gateway pada alat baru.

Langkah selanjutnya

[Membuat gateway](#)

Membuat gateway

Anda dapat membuat Gateway File S3, FSx File Gateway, Tape Gateway, atau Volume Gateway pada perangkat keras.

Untuk membuat gateway pada perangkat keras Anda

1. Masuk ke AWS Management Console dan buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.

2. Pilih Perangkat Keras.
3. Pilih perangkat keras yang diaktifkan di mana Anda ingin membuat gateway Anda, lalu pilih Buat Gateway.
4. Ikuti prosedur yang dijelaskan dalam [Membuat Gateway Anda](#) untuk menyiapkan, menghubungkan, dan mengonfigurasi jenis gateway yang Anda pilih.

Ketika Anda selesai membuat gateway Anda di konsol Storage Gateway, perangkat lunak Storage Gateway secara otomatis mulai menginstal pada perangkat keras. Diperlukan waktu 5-10 menit agar gateway ditampilkan sebagai online di konsol.

Untuk menetapkan alamat IP statis ke gateway yang diinstal, Anda selanjutnya mengonfigurasi antarmuka jaringan gateway sehingga aplikasi Anda dapat menggunakannya.

Langkah selanjutnya

[Mengkonfigurasi alamat IP untuk gateway](#)

Mengkonfigurasi alamat IP untuk gateway

Sebelum Anda mengaktifkan perangkat keras Anda, Anda menetapkan alamat IP ke antarmuka jaringan fisiknya. Sekarang setelah Anda mengaktifkan alat dan meluncurkan Storage Gateway Anda di atasnya, Anda perlu menetapkan alamat IP lain ke mesin virtual Storage Gateway yang berjalan pada perangkat keras. Untuk menetapkan alamat IP statis ke gateway yang diinstal pada perangkat keras Anda, konfigurasi alamat IP dari konsol lokal untuk gateway itu. Aplikasi Anda (seperti klien NFS atau SMB Anda, inisiator iSCSI Anda, dan sebagainya) terhubung ke alamat IP ini. Anda dapat mengakses konsol lokal gateway dari konsol alat perangkat keras.

Untuk mengonfigurasi alamat IP pada alat Anda agar berfungsi dengan aplikasi

1. Pada konsol perangkat keras, pilih Open Service Console untuk membuka layar login untuk konsol lokal gateway.
2. Masukkan kata sandi login localhost, lalu tekan. Enter
Akun default adalah admin dan kata sandi default adalahpassword.
3. Ubah kata sandi default. Pilih Tindakan lalu Atur Kata Sandi Lokal dan masukkan kredensial baru Anda di kotak dialog Set Local Password.
4. (Opsional) Konfigurasi pengaturan proxy Anda. Lihat [the section called “Mengatur Kata Sandi Konsol Lokal dari Storage Gateway Console”](#) untuk instruksi.

- Arahkan ke halaman Pengaturan Jaringan konsol lokal gateway seperti yang ditunjukkan berikut. halaman konfigurasi konsol lokal gateway yang menampilkan opsi termasuk konfigurasi jaringan.

```

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

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

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _

```

halaman konfigurasi konsol lokal gateway yang menampilkan opsi termasuk konfigurasi jaringan.

- Ketik 2 untuk pergi ke halaman Konfigurasi Jaringan yang ditunjukkan berikut. gateway halaman konfigurasi jaringan konsol lokal dengan DHCP dan opsi IP statis.

```

AWS Storage Gateway Network Configuration

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

Press "x" to exit

Enter command: _

```

gateway halaman konfigurasi jaringan konsol lokal dengan DHCP dan opsi IP statis.

- Konfigurasi alamat IP statis atau DHCP untuk port jaringan pada perangkat keras Anda untuk menyajikan file, volume, dan Tape Gateway untuk aplikasi. Alamat IP ini harus berada di subnet yang sama dengan alamat IP yang digunakan selama aktivasi perangkat keras.

Untuk keluar dari konsol lokal gateway

- Tekan penekanan tombol `Ctrl+]` (tutup braket). Konsol perangkat keras muncul.

Note

Keystroke sebelumnya adalah satu-satunya cara untuk keluar dari konsol lokal gateway.

Langkah selanjutnya

[Mengkonfigurasi gateway Anda](#)

Mengkonfigurasi gateway Anda

Setelah perangkat keras Anda diaktifkan dan dikonfigurasi, alat Anda muncul di konsol. Sekarang Anda dapat membuat jenis gateway yang Anda inginkan. Lanjutkan penginstalan pada halaman Configure gateway untuk jenis gateway Anda. Untuk petunjuk, lihat [Mengonfigurasi Gateway Tape Anda Mengkonfigurasi Gateway](#) .

Menghapus gateway dari alat perangkat keras

Untuk menghapus perangkat lunak gateway dari perangkat keras Anda, gunakan prosedur berikut. Setelah Anda melakukannya, perangkat lunak gateway dihapus dari perangkat keras Anda.

Untuk menghapus gateway dari alat perangkat keras

1. Pada halaman Hardware konsol Storage Gateway, pilih perangkat keras yang ingin Anda hapus.
2. Untuk Tindakan, pilih Hapus Gateway. Kotak dialog konfirmasi muncul.
3. Verifikasi bahwa Anda ingin menghapus perangkat lunak gateway dari perangkat keras tertentu, lalu ketik kata hapus di kotak konfirmasi dan pilih Hapus.

Note

Setelah Anda menghapus perangkat lunak gateway, Anda tidak dapat membatalkan tindakan. Untuk jenis gateway tertentu, Anda dapat kehilangan data saat penghapusan, terutama data yang di-cache. Untuk informasi selengkapnya tentang menghapus gateway, lihat [Menghapus Gateway Anda dengan Menggunakan AWS Storage Gateway Konsol dan Menghapus Sumber Daya Terkait](#).

Menghapus gateway tidak menghapus alat perangkat keras dari konsol. Alat perangkat keras tetap untuk penerapan gateway masa depan.

Menghapus alat perangkat keras Anda

Jika Anda tidak lagi memerlukan Storage Gateway Hardware Appliance yang telah diaktifkan, Anda dapat menghapus perangkat sepenuhnya dari AWS akun Anda.

Note

Untuk memindahkan alat Anda ke AWS akun lain atau Wilayah AWS, Anda harus menghapusnya terlebih dahulu menggunakan prosedur berikut, lalu buka saluran dukungan gateway dan hubungi AWS Support untuk melakukan soft reset. Untuk informasi selengkapnya, lihat [Mengaktifkan AWS Support akses untuk membantu memecahkan masalah gateway yang dihosting di tempat](#) tempat.

Untuk menghapus alat perangkat keras Anda

1. Jika Anda telah menginstal gateway pada alat perangkat keras, Anda harus terlebih dahulu menghapus gateway sebelum Anda dapat menghapus alat. Untuk petunjuk tentang cara menghapus gateway dari perangkat keras Anda, lihat [Menghapus gateway dari alat perangkat keras](#).
2. Pada halaman Hardware konsol Storage Gateway, pilih perangkat keras yang ingin Anda hapus.
3. Untuk Tindakan, pilih Hapus Alat. Kotak dialog konfirmasi muncul.
4. Verifikasi bahwa Anda ingin menghapus perangkat keras yang ditentukan, lalu ketik kata hapus di kotak konfirmasi dan pilih Hapus.

Saat Anda menghapus alat perangkat keras, semua sumber daya yang terkait dengan gateway yang diinstal pada alat dihapus, tetapi data pada alat perangkat keras itu sendiri tidak dihapus.

Membuat Gateway Anda

Topik ikhtisar di halaman ini memberikan sinopsis tingkat tinggi tentang cara kerja proses pembuatan Storage Gateway. Untuk step-by-step prosedur untuk membuat jenis gateway tertentu menggunakan konsol Storage Gateway, lihat [Membuat Gateway Tape Membuat Gateway](#).

Ikhtisar - Aktivasi Gateway

Aktivasi gateway melibatkan pengaturan gateway Anda, menghubungkannya AWS, lalu meninjau pengaturan Anda dan mengaktifkannya.

Siapkan gateway

Untuk mengatur Storage Gateway Anda, pertama-tama Anda memilih jenis gateway yang ingin Anda buat dan platform host tempat Anda akan menjalankan alat virtual gateway. Anda kemudian mengunduh template alat virtual gateway untuk platform pilihan Anda dan menerapkannya di lingkungan lokal Anda. Anda juga dapat menerapkan Storage Gateway sebagai perangkat keras fisik yang Anda pesan dari pengecer pilihan Anda, atau sebagai instans Amazon EC2 di AWS lingkungan cloud Anda. Saat Anda menerapkan alat gateway, Anda mengalokasikan ruang disk fisik lokal pada host virtualisasi.

Connect ke AWS

Langkah selanjutnya adalah menghubungkan gateway Anda ke AWS. Untuk melakukan ini, pertama-tama Anda memilih jenis titik akhir layanan yang ingin Anda gunakan untuk komunikasi antara alat virtual gateway dan AWS layanan di cloud. Titik akhir ini dapat diakses dari internet publik, atau hanya dari dalam VPC Amazon Anda, di mana Anda memiliki kontrol penuh atas konfigurasi keamanan jaringan. Anda kemudian menentukan alamat IP gateway atau kunci aktivasi, yang dapat Anda peroleh dengan menghubungkan ke konsol lokal pada alat gateway.

Tinjau dan aktifkan

Pada titik ini, Anda akan memiliki kesempatan untuk meninjau gateway dan opsi koneksi yang Anda pilih, dan membuat perubahan jika perlu. Ketika semuanya diatur seperti yang Anda inginkan, Anda dapat mengaktifkan gateway. Sebelum Anda dapat mulai menggunakan gateway yang diaktifkan, Anda perlu mengonfigurasi beberapa pengaturan tambahan dan membuat sumber daya penyimpanan Anda.

Ikhtisar - Konfigurasi Gateway

Setelah mengaktifkan Storage Gateway, Anda perlu melakukan beberapa konfigurasi tambahan. Pada langkah ini, Anda mengalokasikan penyimpanan fisik yang Anda sediakan di platform host gateway untuk digunakan sebagai cache atau buffer unggahan oleh alat gateway. Anda kemudian mengonfigurasi pengaturan untuk membantu memantau kesehatan gateway Anda menggunakan CloudWatch Log Amazon dan CloudWatch alarm, dan menambahkan tag untuk membantu mengidentifikasi gateway, jika diinginkan. Sebelum Anda dapat mulai menggunakan gateway yang diaktifkan dan dikonfigurasi, Anda harus membuat sumber daya penyimpanan Anda.

Ikhtisar - Sumber Daya Penyimpanan

Setelah mengaktifkan dan mengonfigurasi Storage Gateway, Anda perlu membuat sumber daya penyimpanan cloud agar dapat digunakan. Bergantung pada jenis gateway yang Anda buat, Anda akan menggunakan konsol Storage Gateway untuk membuat Volume, Kaset, atau file Amazon S3 atau Amazon FSx untuk diasosiasikan dengannya. Setiap jenis gateway menggunakan sumber dayanya masing-masing untuk meniru jenis infrastruktur penyimpanan jaringan terkait, dan mentransfer data yang Anda tulis ke AWS cloud.

Membuat Tape Gateway

Di bagian ini, Anda dapat menemukan petunjuk tentang cara membuat dan menggunakan Tape Gateway di AWS Storage Gateway.

Topik

- [Membuat Gateway](#)
- [Membuat Kolam Tape Kustom](#)
- [Membuat Kaset](#)
- [Menggunakan Tape Gateway Anda](#)

Membuat Gateway

Di bagian ini, Anda dapat menemukan petunjuk tentang cara mengunduh, menyebarkan, dan mengaktifkan Tape Gateway standar.

Topik

- [Siapkan Tape Gateway](#)
- [Hubungkan Tape Gateway Anda ke AWS](#)
- [Tinjau pengaturan dan aktifkan Tape Gateway Anda](#)
- [Konfigurasi Tape Gateway Anda](#)

Siapkan Tape Gateway

Untuk menyiapkan Tape Gateway baru

1. Buka AWS Management Console di <https://console.aws.amazon.com/storagegateway/home/>, dan pilih Wilayah AWS tempat Anda ingin membuat gateway Anda.
2. Pilih Buat gateway untuk membuka halaman Mengatur gateway.
3. Di bagian Pengaturan Gateway, lakukan hal berikut:
 - a. Untuk nama Gateway, masukkan nama untuk gateway Anda. Anda dapat mencari nama ini untuk menemukan gateway Anda di halaman daftar di konsol Storage Gateway.
 - b. Untuk zona waktu Gateway, pilih zona waktu lokal untuk bagian dunia tempat Anda ingin menggunakan gateway Anda.
4. Di bagian opsi Gateway, untuk tipe Gateway, pilih Tape Gateway.
5. Di bagian Opsi platform, lakukan hal berikut:
 - a. Untuk platform Host, pilih platform tempat Anda ingin menerapkan gateway Anda, lalu ikuti instruksi khusus platform yang ditampilkan di halaman konsol Storage Gateway untuk menyiapkan platform host Anda. Anda dapat memilih dari opsi berikut:
 - VMware ESXi - Unduh, gunakan, dan konfigurasi mesin virtual gateway menggunakan VMware ESXi.
 - Microsoft Hyper-V - Unduh, gunakan, dan konfigurasi mesin virtual gateway menggunakan Microsoft Hyper-V.
 - Linux KVM - Unduh, gunakan, dan konfigurasi mesin virtual gateway menggunakan Linux KVM.
 - Amazon EC2 - Konfigurasi dan luncurkan instans Amazon EC2 untuk meng-host gateway Anda. Opsi ini tidak tersedia untuk gateway volume Tersimpan.
 - Alat perangkat keras - Pesan alat perangkat keras fisik khusus dari AWS untuk meng-host gateway Anda.

- b. Untuk Konfirmasi pengaturan gateway, pilih kotak centang untuk mengonfirmasi bahwa Anda melakukan langkah penerapan untuk platform host yang Anda pilih. Langkah ini tidak berlaku untuk platform host alat Perangkat Keras.
6. Di bagian Pengaturan aplikasi Backup, untuk aplikasi Backup, pilih aplikasi yang ingin Anda gunakan untuk mencadangkan data tape Anda ke kaset virtual yang terkait dengan Tape Gateway Anda.
7. Pilih Berikutnya untuk melanjutkan.

Sekarang gateway Anda sudah diatur, Anda harus memilih bagaimana Anda ingin terhubung dan berkomunikasi dengannya AWS. Untuk petunjuk, lihat [Connect Tape Gateway Anda ke AWS](#).

Hubungkan Tape Gateway Anda ke AWS

Untuk menghubungkan Tape Gateway baru ke AWS

1. Selesaikan prosedur yang dijelaskan di [Siapkan Tape Gateway](#) jika Anda belum melakukannya. Setelah selesai, pilih Berikutnya untuk membuka AWS halaman Connect to di konsol Storage Gateway.
2. Di bagian opsi Endpoint, untuk titik akhir Layanan, pilih jenis titik akhir yang akan digunakan gateway Anda untuk berkomunikasi. AWS Anda dapat memilih dari opsi berikut:
 - Dapat diakses publik - Gateway Anda berkomunikasi AWS melalui internet publik. Jika Anda memilih opsi ini, gunakan kotak centang titik akhir yang diaktifkan FIPS untuk menentukan apakah koneksi harus mematuhi Standar Pemrosesan Informasi Federal (FIPS).

Note

Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir yang sesuai dengan FIPS. Untuk informasi selengkapnya, lihat [Federal Information Processing Standard \(FIPS\) 140-2](#).

Titik akhir layanan FIPS hanya tersedia di beberapa AWS Wilayah. Untuk informasi selengkapnya, lihat [titik akhir dan kuota Storage Gateway](#) di Referensi Umum AWS

- VPC Hosted - Gateway Anda berkomunikasi dengan AWS melalui koneksi pribadi dengan VPC Anda, memungkinkan Anda untuk mengontrol pengaturan jaringan Anda. Jika Anda memilih opsi ini, Anda harus menentukan titik akhir VPC yang ada dengan memilih ID titik

akhir VPC dari menu tarik-turun, atau dengan memberikan nama DNS titik akhir VPC atau alamat IP.

3. Di bagian Opsi koneksi Gateway, untuk opsi Koneksi, pilih cara mengidentifikasi gateway Anda AWS. Anda dapat memilih dari opsi berikut:

- Alamat IP - Berikan alamat IP gateway Anda di bidang yang sesuai. Alamat IP ini harus bersifat publik atau dapat diakses dari dalam jaringan Anda saat ini, dan Anda harus dapat menghubungkannya dari browser web Anda.

Anda dapat memperoleh alamat IP gateway dengan masuk ke konsol lokal gateway dari klien hypervisor Anda, atau dengan menyalinnya dari halaman detail instans Amazon EC2 Anda.

- Kunci aktivasi - Berikan kunci aktivasi untuk gateway Anda di bidang yang sesuai. Anda dapat membuat kunci aktivasi menggunakan konsol lokal gateway. Pilih opsi ini jika alamat IP gateway Anda tidak tersedia.

4. Pilih Berikutnya untuk melanjutkan.

Sekarang Anda telah memilih bagaimana Anda ingin gateway Anda terhubung AWS, Anda perlu mengaktifkan gateway. Untuk petunjuk, lihat [Meninjau pengaturan dan mengaktifkan Tape Gateway Anda](#).

Tinjau pengaturan dan aktifkan Tape Gateway Anda

Untuk mengaktifkan Tape Gateway baru

1. Lengkapi prosedur yang dijelaskan dalam topik berikut jika Anda belum melakukannya:
 - [Siapkan Tape Gateway](#)
 - [Hubungkan Tape Gateway Anda ke AWS](#)

Setelah selesai, pilih Berikutnya untuk membuka halaman Ulasan dan mengaktifkan di konsol Storage Gateway.

2. Tinjau detail gateway awal untuk setiap bagian di halaman.
3. Jika bagian berisi kesalahan, pilih Edit untuk kembali ke halaman pengaturan yang sesuai dan membuat perubahan.

Note

Anda tidak dapat mengubah opsi gateway atau pengaturan koneksi setelah gateway Anda diaktifkan.

4. Pilih Aktifkan gateway untuk melanjutkan.

Sekarang setelah Anda mengaktifkan gateway Anda, Anda perlu melakukan konfigurasi pertama kali untuk mengalokasikan disk penyimpanan lokal dan mengonfigurasi logging. Untuk petunjuk, lihat [Mengkonfigurasi Gateway Tape Anda](#).

Konfigurasi Tape Gateway Anda


Untuk melakukan konfigurasi pertama kali pada Tape Gateway baru

1. Lengkapi prosedur yang dijelaskan dalam topik berikut jika Anda belum melakukannya:
 - [Siapkan Tape Gateway](#)
 - [Hubungkan Tape Gateway Anda ke AWS](#)
 - [Tinjau pengaturan dan aktifkan Tape Gateway Anda](#)

Setelah selesai, pilih Berikutnya untuk membuka halaman Configure gateway di konsol Storage Gateway.

2. Di bagian Configure storage, gunakan menu drop-down untuk mengalokasikan setidaknya satu disk dengan kapasitas minimal 165 GiB untuk CACHE STORAGE, dan setidaknya satu disk dengan kapasitas minimal 150 GiB untuk UPLOAD BUFFER. Disk lokal yang tercantum di bagian ini sesuai dengan penyimpanan fisik yang Anda sediakan di platform host Anda.
3. Di bagian grup CloudWatch log, pilih cara mengatur CloudWatch Log Amazon untuk memantau kesehatan gateway Anda. Anda dapat memilih dari opsi berikut:
 - Buat grup log baru - Siapkan grup log baru untuk memantau gateway Anda.
 - Gunakan grup log yang ada - Pilih grup log yang ada dari menu drop-down yang sesuai.
 - Nonaktifkan logging - Jangan gunakan Amazon CloudWatch Logs untuk memantau gateway Anda.

4. Di bagian CloudWatch alarm, pilih cara mengatur CloudWatch alarm Amazon untuk memberi tahu Anda saat metrik gateway menyimpang dari batas yang ditentukan. Anda dapat memilih dari opsi berikut:
 - Buat alarm yang direkomendasikan oleh Storage Gateway — Buat semua CloudWatch alarm yang direkomendasikan secara otomatis saat gateway dibuat. Untuk informasi selengkapnya tentang alarm yang direkomendasikan, lihat [Memahami CloudWatch alarm](#).

 Note

Fitur ini memerlukan izin CloudWatch kebijakan, yang tidak secara otomatis diberikan sebagai bagian dari kebijakan akses penuh Storage Gateway yang telah dikonfigurasi sebelumnya. Pastikan kebijakan keamanan Anda memberikan izin berikut sebelum Anda mencoba membuat alarm yang direkomendasikan CloudWatch :

- `cloudwatch:PutMetricAlarm`- buat alarm
 - `cloudwatch:DisableAlarmActions`- matikan tindakan alarm
 - `cloudwatch:EnableAlarmActions`- Aktifkan tindakan alarm
 - `cloudwatch>DeleteAlarms`- Hapus alarm
- Buat alarm khusus — Konfigurasi CloudWatch alarm baru untuk memberi tahu Anda tentang metrik gateway Anda. Pilih Buat alarm untuk menentukan metrik dan menentukan tindakan alarm di CloudWatch konsol Amazon. Untuk petunjuk, lihat [Menggunakan CloudWatch alarm Amazon](#) di Panduan CloudWatch Pengguna Amazon.
 - Tanpa alarm — Jangan menerima CloudWatch pemberitahuan tentang metrik gateway Anda.
5. (Opsional) Di bagian Tag, pilih Tambahkan tag baru, lalu masukkan pasangan nilai kunci peka huruf besar/kecil untuk membantu Anda mencari dan memfilter gateway Anda pada halaman daftar di konsol Storage Gateway. Ulangi langkah ini untuk menambahkan tag sebanyak yang Anda butuhkan.
 6. Pilih Konfigurasi untuk menyelesaikan pembuatan gateway Anda.

Untuk memeriksa status gateway baru Anda, cari di halaman ikhtisar Gateway di Storage Gateway.

Sekarang Anda telah membuat gateway Anda, Anda perlu membuat kaset virtual untuk digunakan. Untuk petunjuk, lihat [Membuat Kaset](#).

Membuat Kolam Tape Kustom

Bagian ini menjelaskan cara membuat kumpulan pita kustom baru di AWS Storage Gateway.

Topik

- [Memilih Jenis Tape Pool](#)
- [Menggunakan Tape Retention Lock](#)
- [Membuat Kolam Tape Kustom](#)

Memilih Jenis Tape Pool

AWS Storage Gateway menggunakan tape pool untuk menentukan kelas penyimpanan tempat Anda ingin kaset diarsipkan saat dikeluarkan. Storage Gateway menyediakan dua tape pool standar:

- **Glacier Pool** — Mengarsipkan rekaman di kelas penyimpanan S3 Glacier Flexible Retrieval. Ketika perangkat lunak cadangan Anda mengeluarkan rekaman, itu secara otomatis diarsipkan dalam S3 Glacier Flexible Retrieval. Anda menggunakan S3 Glacier Flexible Retrieval untuk arsip yang lebih aktif, di mana Anda dapat mengambil kaset biasanya dalam waktu 3-5 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- **Deep Archive Pool** — Mengarsipkan rekaman di kelas penyimpanan S3 Glacier Deep Archive. Saat perangkat lunak cadangan Anda mengeluarkan kaset, rekaman itu secara otomatis diarsipkan di S3 Glacier Deep Archive. Anda menggunakan S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital, di mana data diakses sekali atau dua kali setahun. Anda dapat mengambil kaset yang diarsipkan di S3 Glacier Deep Archive biasanya dalam waktu 12 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Jika Anda mengarsipkan kaset di S3 Glacier Flexible Retrieval, Anda dapat memindahkannya ke S3 Glacier Deep Archive nanti. Untuk informasi selengkapnya, lihat [Memindahkan Tape Anda dari Pengambilan Fleksibel Gletser S3 ke Kelas Penyimpanan S3 Glacier Deep Archive](#).

Storage Gateway juga mendukung pembuatan kumpulan pita khusus, yang memungkinkan Anda mengaktifkan kunci retensi pita untuk mencegah kaset yang diarsipkan dihapus atau dipindahkan ke kolam lain untuk jangka waktu yang tetap, hingga 100 tahun. Ini termasuk mengunci kontrol izin pada siapa yang dapat menghapus kaset atau mengubah pengaturan retensi.

Menggunakan Tape Retention Lock

Dengan kunci retensi pita, Anda dapat mengunci kaset yang diarsipkan. Kunci retensi pita adalah opsi untuk kaset di kolam pita khusus. Kaset yang mengaktifkan kunci retensi pita tidak dapat dihapus atau dipindahkan ke kumpulan lain untuk jangka waktu yang tetap, hingga 100 tahun.

Anda dapat mengonfigurasi kunci retensi pita dalam salah satu dari dua mode:

- **Mode tata kelola** — Saat dikonfigurasi dalam mode tata kelola, hanya pengguna AWS Identity and Access Management (IAM) dengan izin untuk melakukan yang `storagegateway:BypassGovernanceRetention` dapat menghapus kaset dari kumpulan. Jika Anda menggunakan AWS Storage Gateway API untuk menghapus rekaman, Anda juga harus menyetel `BypassGovernanceRetention` ke `true`.
- **Mode kepatuhan** — Ketika dikonfigurasi dalam mode kepatuhan, perlindungan tidak dapat dihapus oleh pengguna mana pun, termasuk root Akun AWS.

Ketika tape dikunci dalam mode kepatuhan, jenis kunci retensi tidak dapat diubah, dan periode retensi tidak dapat dipersingkat. Jenis kunci mode kepatuhan membantu memastikan bahwa rekaman tidak dapat ditimpa atau dihapus selama periode retensi.

Important

Konfigurasi kumpulan kustom tidak dapat diubah setelah dibuat.

Anda dapat mengaktifkan kunci retensi pita saat Anda membuat kumpulan pita khusus. Setiap kaset baru yang dilampirkan ke kumpulan kustom mewarisi jenis kunci retensi, periode, dan kelas penyimpanan untuk kumpulan itu.

Anda juga dapat mengaktifkan kunci retensi pita pada kaset yang diarsipkan sebelum rilis fitur ini dengan memindahkan kaset antara kumpulan default dan kumpulan kustom yang Anda buat. Jika kaset diarsipkan, kunci retensi pita segera efektif.

Note

Jika Anda memindahkan kaset yang diarsipkan antara kelas penyimpanan S3 Glacier Flexible Retrieval dan S3 Glacier Deep Archive, Anda dikenakan biaya untuk memindahkan

kaset. Tidak ada biaya tambahan untuk memindahkan kaset dari kolam default ke kolam khusus jika kelas penyimpanan tetap sama.

Membuat Kolam Tape Kustom

Gunakan langkah-langkah berikut untuk membuat kumpulan kaset khusus menggunakan AWS Storage Gateway konsol.

Untuk membuat kolam tape kustom

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi kiri, pilih tab Tape Library, lalu pilih tab Pools.
3. Pilih Create pool untuk membuka panel Create pool.
4. Untuk Nama, masukkan nama unik untuk mengidentifikasi kumpulan pita kustom Anda. Panjang nama pool harus antara 2 dan 100 karakter.
5. Untuk kelas Penyimpanan, pilih Glacier atau Glacier Deep Archive.
6. Untuk jenis kunci Retensi, pilih Tidak Ada, Kepatuhan, atau Tata Kelola.

Note

Jika Anda memilih Kepatuhan, kunci retensi pita tidak dapat dihapus oleh pengguna mana pun, termasuk root Akun AWS.

7. Jika Anda memilih jenis kunci retensi pita, masukkan periode Retensi dalam beberapa hari. Periode retensi maksimum adalah 36.500 hari (100 tahun).
8. (Opsional) Untuk Tag, pilih Tambahkan tag baru untuk menambahkan tag ke kumpulan pita kustom Anda. Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengelola, memfilter, dan mencari kumpulan pita kustom Anda.

Masukkan Kunci, dan secara opsional, Nilai untuk tag Anda. Anda dapat menambahkan hingga 50 tag ke kolam kaset.

9. Pilih Buat kolam untuk membuat kumpulan pita kustom baru Anda.

Membuat Kaset

Bagian ini menjelaskan cara membuat kaset virtual baru menggunakan AWS Storage Gateway. Anda dapat membuat kaset virtual baru secara manual menggunakan AWS Storage Gateway konsol atau Storage Gateway API. Anda juga dapat mengonfigurasi Tape Gateway untuk membuatnya secara otomatis, yang membantu mengurangi kebutuhan akan manajemen rekaman manual, membuat penerapan besar Anda lebih sederhana, dan membantu menskalakan kebutuhan penyimpanan lokal dan arsip.

Tape Gateway mendukung penulisan sekali, baca banyak (WORM) dan kunci retensi pita pada kaset virtual. Kaset virtual yang diaktifkan cacing membantu memastikan bahwa data pada kaset aktif di pustaka rekaman virtual Anda tidak dapat ditimpa atau dihapus. Untuk informasi selengkapnya tentang perlindungan WORM untuk kaset virtual, lihat bagian berikut, [the section called “Perlindungan Pita WORM”](#).

Dengan kunci retensi pita, Anda dapat menentukan mode dan periode retensi pada kaset virtual yang diarsipkan, mencegahnya dihapus untuk jangka waktu tetap hingga 100 tahun. Ini termasuk kontrol izin tentang siapa yang dapat menghapus kaset atau memodifikasi pengaturan retensi. Untuk informasi selengkapnya tentang kunci retensi pita, lihat [the section called “Kunci Retensi Pita”](#).

Note

Anda hanya dikenakan biaya untuk jumlah data yang Anda tulis ke rekaman itu, bukan kapasitas rekaman.

Anda dapat menggunakan AWS Key Management Service (AWS KMS) untuk mengenkripsi data yang ditulis ke pita virtual yang disimpan di Amazon Simple Storage Service (Amazon S3). Saat ini, Anda dapat melakukan ini dengan menggunakan AWS Storage Gateway API atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat [CreateTapes](#) atau [buat-kaset](#).

Topik

- [Tulis Sekali, Baca Banyak \(WORM\) Tape Protection](#)
- [Membuat Kaset Secara Manual](#)
- [Mengizinkan Pembuatan Pita Otomatis](#)

Tulis Sekali, Baca Banyak (WORM) Tape Protection

Anda dapat mencegah kaset virtual ditimpa atau dihapus dengan mengaktifkan perlindungan WORM untuk kaset virtual. AWS Storage Gateway Perlindungan WORM untuk kaset virtual diaktifkan saat membuat kaset.

Data yang ditulis ke kaset virtual WORM tidak dapat ditimpa. Hanya data baru yang dapat ditambahkan ke kaset virtual WORM, dan data yang ada tidak dapat dihapus. Mengaktifkan perlindungan WORM untuk kaset virtual membantu melindungi kaset tersebut saat sedang digunakan secara aktif, sebelum dikeluarkan dan diarsipkan.

Konfigurasi WORM hanya dapat diatur ketika kaset dibuat, dan konfigurasi itu tidak dapat diubah setelah kaset dibuat.

Membuat Kaset Secara Manual

Anda dapat membuat kaset virtual baru secara manual menggunakan AWS Storage Gateway konsol atau Storage Gateway API. Konsol ini menawarkan antarmuka yang nyaman untuk pembuatan pita dengan fleksibilitas untuk menentukan awalan untuk barcode pita yang dihasilkan secara acak. Jika Anda perlu sepenuhnya menyesuaikan barcode tape Anda (misalnya, untuk mencocokkan nomor seri pita fisik yang sesuai), Anda harus menggunakan API. Untuk informasi selengkapnya tentang membuat kaset menggunakan Storage Gateway API, lihat [CreateTapeWithBarcode](#) di Storage Gateway API Reference.

Untuk membuat kaset virtual secara manual menggunakan konsol Storage Gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih tab Gateways.
3. Pilih Buat kaset untuk membuka panel Buat kaset.
4. Untuk Gateway, pilih gateway. Rekaman itu dibuat untuk gateway ini.
5. Untuk jenis Tape, pilih Standar untuk membuat kaset virtual standar. Pilih WORM untuk membuat tulis setelah membaca banyak kaset virtual (WORM).
6. Untuk Jumlah kaset, pilih jumlah kaset yang ingin Anda buat. Untuk informasi lebih lanjut tentang kuota kaset, lihat [AWS Storage Gateway kuota](#).
7. Untuk Kapasitas, masukkan ukuran pita virtual yang ingin Anda buat. Kaset harus lebih besar dari 100 GiB. Untuk informasi tentang kuota kapasitas, lihat [AWS Storage Gateway kuota](#).
8. Untuk awalan Barcode, masukkan awalan yang ingin Anda tambahkan ke barcode kaset virtual Anda.

Note

Kaset virtual diidentifikasi secara unik oleh kode batang, dan Anda dapat menambahkan awalan ke kode batang. Anda dapat menggunakan awalan untuk membantu mengidentifikasi kaset virtual Anda. Awalan harus huruf besar (A—Z) dan panjangnya harus satu hingga empat karakter.

9. Untuk Pool, pilih Glacier Pool, Deep Archive Pool, atau kolam khusus yang telah Anda buat. Pool menentukan kelas penyimpanan tempat rekaman Anda disimpan saat dikeluarkan oleh perangkat lunak cadangan Anda.
 - Pilih Glacier Pool jika Anda ingin mengarsipkan rekaman di kelas penyimpanan S3 Glacier Flexible Retrieval. Ketika perangkat lunak cadangan Anda mengeluarkan rekaman, itu secara otomatis diarsipkan dalam S3 Glacier Flexible Retrieval. Anda menggunakan S3 Glacier Flexible Retrieval untuk arsip yang lebih aktif, di mana Anda dapat mengambil kaset biasanya dalam waktu 3-5 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
 - Pilih Deep Archive Pool jika Anda ingin mengarsipkan rekaman di kelas penyimpanan S3 Glacier Deep Archive. Saat perangkat lunak cadangan Anda mengeluarkan kaset, rekaman itu secara otomatis diarsipkan di S3 Glacier Deep Archive. Anda menggunakan S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital, di mana data diakses sekali atau dua kali setahun. Anda dapat mengambil rekaman yang diarsipkan di S3 Glacier Deep Archive biasanya dalam waktu 12 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
 - Pilih kolam khusus, jika ada yang tersedia. Anda mengonfigurasi kumpulan pita khusus untuk menggunakan Deep Archive Pool atau Glacier Pool. Kaset diarsipkan ke kelas penyimpanan yang dikonfigurasi saat dikeluarkan oleh perangkat lunak cadangan Anda.

Jika Anda mengarsipkan kaset di S3 Glacier Flexible Retrieval, Anda dapat memindahkannya ke S3 Glacier Deep Archive nanti. Untuk informasi selengkapnya, lihat [Memindahkan Tape Anda dari Pengambilan Fleksibel Gletser S3 ke Kelas Penyimpanan S3 Glacier Deep Archive](#).

Note

Kaset yang dibuat sebelum 27 Maret 2019, diarsipkan langsung di S3 Glacier Flexible Retrieval saat perangkat lunak cadangan Anda mengeluarkannya.

10. (Opsional) Untuk Tag, pilih Tambahkan tag baru dan masukkan kunci dan nilai untuk menambahkan tag ke rekaman Anda. Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengelola, memfilter, dan mencari kaset Anda.
11. Pilih Buat kaset.
12. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.

Status kaset virtual awalnya diatur ke CREATING ketika kaset virtual sedang dibuat. Setelah kaset dibuat, statusnya berubah menjadi TERSEDIA. Untuk informasi selengkapnya, lihat [Mengelola Tape Gateway Anda](#).

Mengizinkan Pembuatan Pita Otomatis

Tape Gateway dapat secara otomatis membuat kaset virtual baru untuk mempertahankan jumlah minimum kaset yang tersedia yang Anda konfigurasi. Kemudian membuat kaset baru ini tersedia untuk diimpor oleh aplikasi cadangan sehingga pekerjaan cadangan Anda dapat berjalan tanpa gangguan. Mengizinkan pembuatan pita otomatis menghilangkan kebutuhan akan skrip khusus selain proses manual membuat kaset virtual baru.

Tape Gateway memunculkan kaset baru secara otomatis ketika memiliki kaset lebih sedikit daripada jumlah minimum kaset yang tersedia yang ditentukan untuk pembuatan pita otomatis. Rekaman baru muncul ketika:

- Kaset diimpor dari slot impor/ekspor.
- Kaset diimpor ke tape drive.

Gateway mempertahankan jumlah minimum kaset dengan awalan barcode yang ditentukan dalam kebijakan pembuatan pita otomatis. Jika ada lebih sedikit kaset daripada jumlah minimum kaset dengan awalan barcode, gateway secara otomatis membuat kaset baru yang cukup untuk menyamai jumlah minimum kaset yang ditentukan dalam kebijakan pembuatan pita otomatis.

Ketika Anda mengeluarkan kaset dan masuk ke slot impor/ekspor, pita itu tidak dihitung terhadap jumlah minimum kaset yang ditentukan dalam kebijakan pembuatan pita otomatis Anda. Hanya kaset di slot impor/ekspor yang dihitung sebagai “tersedia.” Mengekspor kaset tidak memulai pembuatan pita otomatis. Hanya impor yang memengaruhi jumlah kaset yang tersedia.

Memindahkan kaset dari slot impor/ekspor ke tape drive atau slot penyimpanan mengurangi jumlah kaset di slot impor/ekspor dengan awalan barcode yang sama. Gateway membuat kaset baru untuk mempertahankan jumlah minimum kaset yang tersedia untuk awalan barcode tersebut.

Untuk memungkinkan pembuatan pita otomatis

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih tab Gateways.
3. Pilih gateway yang ingin Anda buat kaset secara otomatis.
4. Di menu Actions, pilih Configure tape auto-create.

Halaman pembuatan otomatis Tape muncul. Anda dapat menambahkan, mengubah, atau menghapus opsi pembuatan otomatis tape di sini.

5. Untuk mengizinkan pembuatan pita otomatis, pilih Tambahkan item baru lalu konfigurasi pengaturan untuk pembuatan pita otomatis.
6. Untuk jenis Tape, pilih Standar untuk membuat kaset virtual standar. Pilih WORM untuk membuat kaset virtual write-once-read-many(WORM).
7. Untuk jumlah minimum kaset, masukkan jumlah minimum kaset virtual yang harus tersedia di Tape Gateway setiap saat. Rentang yang valid untuk nilai ini adalah minimal 1 dan maksimum 10.
8. Untuk Kapasitas, masukkan ukuran, dalam byte, dari kapasitas pita virtual. Rentang yang valid adalah minimal 100 GiB dan maksimum 15 TiB.
9. Untuk awalan Barcode, masukkan awalan yang ingin Anda tambahkan ke barcode kaset virtual Anda.

Note

Kaset virtual diidentifikasi secara unik oleh kode batang, dan Anda dapat menambahkan awalan ke kode batang. Awalan adalah opsional, tetapi Anda dapat menggunakannya untuk membantu mengidentifikasi kaset virtual Anda. Awalan harus huruf besar (A—Z) dan panjangnya harus satu hingga empat karakter.

10. Untuk Pool, pilih Glacier Pool, Deep Archive Pool, atau kolam khusus yang telah Anda buat. Pool menentukan kelas penyimpanan tempat rekaman Anda disimpan saat dikeluarkan oleh perangkat lunak cadangan Anda.
 - Pilih Glacier Pool jika Anda ingin mengarsipkan rekaman di kelas penyimpanan S3 Glacier Flexible Retrieval. Ketika perangkat lunak cadangan Anda mengeluarkan rekaman, itu secara otomatis diarsipkan dalam S3 Glacier Flexible Retrieval. Anda menggunakan S3 Glacier Flexible Retrieval untuk arsip yang lebih aktif, di mana Anda dapat mengambil kaset biasanya dalam waktu 3-5 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
 - Pilih Deep Archive Pool jika Anda ingin mengarsipkan rekaman di kelas penyimpanan S3 Glacier Deep Archive. Saat perangkat lunak cadangan Anda mengeluarkan kaset, rekaman itu secara otomatis diarsipkan di S3 Glacier Deep Archive. Anda menggunakan S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital, di mana data diakses sekali atau dua kali setahun. Anda dapat mengambil rekaman yang diarsipkan di S3 Glacier Deep Archive biasanya dalam waktu 12 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
 - Pilih kolam khusus, jika ada yang tersedia. Anda mengonfigurasi kumpulan pita khusus untuk menggunakan Deep Archive Pool atau Glacier Pool. Kaset diarsipkan ke kelas penyimpanan yang dikonfigurasi saat dikeluarkan oleh perangkat lunak cadangan Anda.

Jika Anda mengarsipkan kaset di S3 Glacier Flexible Retrieval, Anda dapat memindahkannya ke S3 Glacier Deep Archive nanti. Untuk informasi selengkapnya, lihat [Memindahkan Tape Anda dari Pengambilan Fleksibel Gletser S3 ke Kelas Penyimpanan S3 Glacier Deep Archive](#).

Note

Kaset yang dibuat sebelum 27 Maret 2019, diarsipkan langsung di S3 Glacier Flexible Retrieval saat perangkat lunak cadangan Anda mengeluarkannya.

11. Setelah selesai mengonfigurasi pengaturan, pilih Simpan perubahan.
12. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.

Status kaset virtual yang tersedia awalnya diatur ke CREATING ketika kaset sedang dibuat. Setelah kaset dibuat, statusnya berubah menjadi TERSEDIA. Untuk informasi selengkapnya, lihat [Mengelola Tape Gateway Anda](#).

Untuk informasi selengkapnya tentang mengubah kebijakan pembuatan tape otomatis, atau menghapus pembuatan tape otomatis dari Tape Gateway, lihat [Mengelola Pembuatan Pita Otomatis](#).

Langkah Selanjutnya

[Menggunakan Tape Gateway Anda](#)

Menggunakan Tape Gateway Anda

Berikut ini, Anda dapat menemukan petunjuk tentang cara menggunakan Tape Gateway Anda.

Topik

- [Menghubungkan Perangkat VTL Anda](#)
- [Menggunakan Perangkat Lunak Cadangan Anda untuk Menguji Pengaturan Gateway Anda](#)
- [Apa Langkah Berikutnya?](#)

Menghubungkan Perangkat VTL Anda

Berikut ini, Anda dapat menemukan petunjuk tentang cara menghubungkan perangkat pustaka pita virtual (VTL) Anda ke klien Microsoft Windows atau Red Hat Enterprise Linux (RHEL) Anda.

Topik

- [Menghubungkan ke Klien Microsoft Windows](#)
- [Menghubungkan ke Klien Linux](#)

Menghubungkan ke Klien Microsoft Windows

Prosedur berikut menunjukkan ringkasan langkah-langkah yang Anda ikuti untuk terhubung ke klien Windows.

Untuk menghubungkan perangkat VTL Anda ke klien Windows

1. Mulai `iscsicpl.exe`.

Note

Anda harus memiliki hak administrator pada komputer klien untuk menjalankan inisiator iSCSI.

2. Mulai layanan inisiator Microsoft iSCSI.
3. Di kotak dialog iSCSI Initiator Properties, pilih tab Discovery, lalu pilih Discover Portal.
4. Berikan alamat IP Tape Gateway Anda untuk alamat IP atau nama DNS.
5. Pilih tab Target, lalu pilih Refresh. Semua 10 tape drive dan medium changer muncul di kotak Target Ditemukan. Status target tidak aktif.
6. Pilih perangkat pertama dan hubungkan. Anda menghubungkan perangkat satu per satu.
7. Connect semua target.

Pada klien Windows, penyedia driver untuk tape drive harus Microsoft. Gunakan prosedur berikut untuk memverifikasi penyedia driver, dan perbarui driver dan penyedia jika perlu:

Untuk memverifikasi dan memperbarui driver dan penyedia

1. Pada klien Windows Anda, mulai Device Manager.

2. Perluas drive Tape, buka menu konteks (klik kanan) untuk tape drive, dan pilih Properties.
3. Di tab Driver pada kotak dialog Properti Perangkat, verifikasi Penyedia Driver adalah Microsoft.
4. Jika Penyedia Driver bukan Microsoft, tetapkan nilainya sebagai berikut:
 - a. Pilih Perbarui Driver.
 - b. Dalam kotak dialog Perbarui Perangkat Lunak Driver, pilih Jelajahi komputer saya untuk perangkat lunak driver.
 - c. Dalam kotak dialog Perbarui Perangkat Lunak Driver, pilih Biarkan saya memilih dari daftar driver perangkat di komputer saya.
 - d. Pilih LTO Tape drive dan pilih Berikutnya.
5. Pilih Tutup untuk menutup jendela Perbarui Perangkat Lunak Driver, dan verifikasi bahwa nilai Penyedia Driver sekarang diatur ke Microsoft.
6. Ulangi langkah-langkah untuk memperbarui driver dan penyedia untuk semua tape drive.

Menghubungkan ke Klien Linux

Prosedur berikut menunjukkan ringkasan langkah-langkah yang Anda ikuti untuk terhubung ke klien RHEL.

Untuk menghubungkan klien Linux ke perangkat VTL

1. Instal paket `iscsi-initiator-utils` RPM.

Anda dapat menggunakan perintah berikut untuk menginstal paket.

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

2. Pastikan daemon iSCSI sedang berjalan.

Untuk RHEL 5 atau 6, gunakan perintah berikut.

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

Untuk RHEL 7, gunakan perintah berikut.

```
sudo service iscsid status
```

3. Temukan volume atau target perangkat VTL yang ditentukan untuk gateway. Gunakan perintah penemuan berikut.

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

Output dari perintah penemuan terlihat seperti contoh output berikut.

Untuk Gerbang Volume: [GATEWAY_IP]:3260, 1 iqn.1997-05.com.amazon:myvolume

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

4. Connect ke target.

Pastikan untuk menentukan [GATEWAY_IP] dan IQN yang benar dalam perintah connect.

Gunakan perintah berikut ini.

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

5. Verifikasi bahwa volume terpasang ke mesin klien (inisiator). Untuk melakukannya, gunakan perintah berikut.

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

Output dari perintah akan terlihat seperti contoh output berikut.

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

Untuk Volume Gateways, kami sangat menyarankan bahwa setelah Anda mengatur inisiator Anda, Anda menyesuaikan pengaturan iSCSI Anda seperti yang dibahas dalam [Menyesuaikan Pengaturan iSCSI Linux Anda](#)

Verifikasi bahwa perangkat VTL terpasang ke mesin klien (inisiator). Untuk melakukannya, gunakan perintah berikut.

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

Output dari perintah akan terlihat seperti contoh output berikut.


```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
```

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

Langkah Selanjutnya

[Menggunakan Perangkat Lunak Cadangan Anda untuk Menguji Pengaturan Gateway Anda](#)

Menggunakan Perangkat Lunak Cadangan Anda untuk Menguji Pengaturan Gateway Anda

Anda menguji penyiapan Tape Gateway Anda dengan melakukan tugas-tugas berikut menggunakan aplikasi cadangan Anda:

1. Konfigurasi aplikasi cadangan untuk mendeteksi perangkat penyimpanan Anda.

Note

Untuk meningkatkan kinerja I/O, sebaiknya atur ukuran blok drive tape di aplikasi cadangan Anda ke 1 MB Untuk informasi lebih lanjut, lihat [Gunakan Ukuran Blok yang Lebih Besar untuk Tape Drives](#).

2. Cadangkan data ke kaset.
3. Arsipkan rekaman itu.
4. Ambil rekaman dari arsip.
5. Kembalikan data dari rekaman itu.

Untuk menguji penyiapan Anda, gunakan aplikasi cadangan yang kompatibel, seperti yang dijelaskan berikut.

Note

Kecuali dinyatakan lain, semua aplikasi cadangan memenuhi syarat di Microsoft Windows.

Topik

- [Menguji Pengaturan Anda dengan Menggunakan Arcserve Backup r17.0](#)
- [Menguji Pengaturan Anda dengan Menggunakan Bacula Enterprise](#)
- [Menguji Pengaturan Anda dengan Menggunakan Commvault](#)
- [Menguji Pengaturan Anda dengan Menggunakan Dell EMC NetWorker](#)
- [Menguji Pengaturan Anda dengan Menggunakan IBM Spectrum Protect](#)
- [Menguji Pengaturan Anda dengan Menggunakan Pelindung Data Micro Focus \(HPE\)](#)
- [Menguji Pengaturan Anda dengan Menggunakan Microsoft System Center Data Protection Manager](#)
- [Menguji Pengaturan Anda dengan NovaStor DataCenter Menggunakan/Jaringan](#)
- [Menguji Pengaturan Anda dengan Menggunakan Quest NetVault Backup](#)
- [Menguji Pengaturan Anda dengan Menggunakan Cadangan & Replikasi Veeam](#)
- [Menguji Pengaturan Anda dengan Menggunakan Veritas Backup Exec](#)

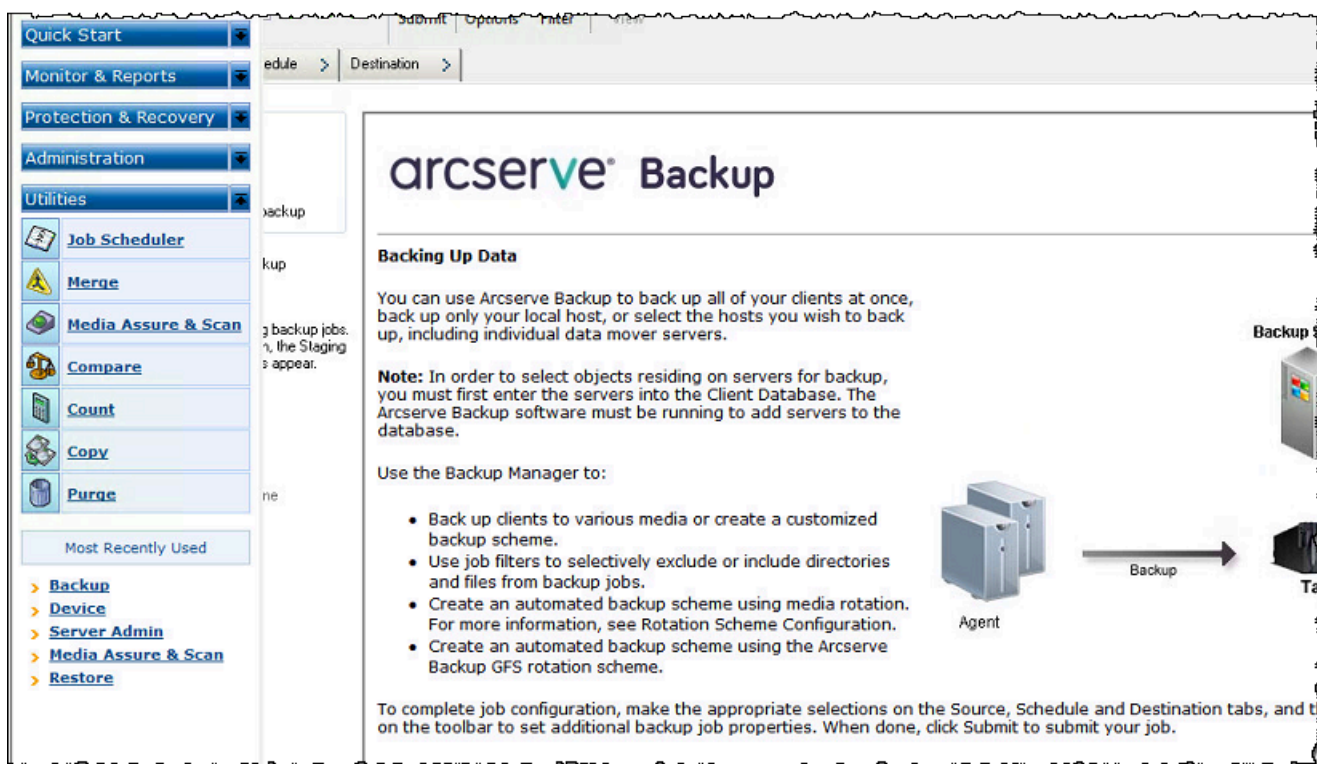
- [Menguji Pengaturan Anda dengan Menggunakan Veritas NetBackup](#)

Untuk informasi selengkapnya tentang aplikasi cadangan yang kompatibel, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Menguji Pengaturan Anda dengan Menggunakan Arcserve Backup r17.0

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Arcserve Backup r17.0. Dalam topik ini, Anda dapat menemukan dokumentasi dasar untuk mengonfigurasi Arcserve Backup dengan Tape Gateway dan melakukan operasi pencadangan dan pemulihan. Untuk informasi rinci tentang penggunaan Arcserve Backup r17.0, lihat [dokumentasi Arcserve Backup r17](#) di Panduan Administrasi Arcserve.

Screen shot berikut menunjukkan menu Arcserve.



Topik

- [Mengkonfigurasi Arcserve untuk Bekerja dengan Perangkat VTL](#)
- [Memuat Kaset ke Media Pool](#)
- [Mencadangkan Data ke Tape](#)

- [Mengarsipkan Pita](#)
- [Memulihkan Data dari Tape](#)

Mengkonfigurasi Arcserve untuk Bekerja dengan Perangkat VTL

Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) Anda ke klien Anda, Anda memindai perangkat Anda.

Untuk memindai perangkat VTL

1. Di Arcserve Backup Manager, pilih menu Utilities.
2. Pilih Media Assure dan Scan.

Memuat Kaset ke Media Pool

Ketika perangkat lunak Arcserve terhubung ke gateway Anda dan kaset Anda tersedia, Arcserve secara otomatis memuat kaset Anda. Jika gateway Anda tidak ditemukan di perangkat lunak Arcserve, coba mulai ulang mesin tape di Arcserve.

Untuk me-restart mesin tape

1. Pilih Mulai Cepat, pilih Administrasi, lalu pilih Perangkat.
2. Pada menu navigasi, buka menu konteks (klik kanan) untuk gateway Anda dan pilih slot impor/ekspor.
3. Pilih Impor Cepat dan tetapkan kaset Anda ke slot kosong.
4. Buka menu konteks (klik kanan) untuk gateway Anda dan pilih Inventaris/Slot Offline.
5. Pilih Quick Inventory untuk mengambil informasi media dari database.

Jika Anda menambahkan kaset baru, Anda perlu memindai gateway Anda agar rekaman baru itu muncul di Arcserve. Jika kaset baru tidak muncul, Anda harus mengimpor kaset.

Untuk mengimpor kaset

1. Pilih menu Mulai Cepat, pilih Cadangan, lalu pilih Tujuan ketuk.
2. Pilih gateway Anda, buka menu konteks (klik kanan) untuk satu kaset, lalu pilih Impor/Ekspor Slot.
3. Buka menu konteks (klik kanan) untuk setiap rekaman baru dan pilih Inventaris.

4. Buka menu konteks (klik kanan) untuk setiap rekaman baru dan pilih Format.

Barcode setiap tape sekarang muncul di konsol Storage Gateway Anda, dan setiap tape siap digunakan.

Mencadangkan Data ke Tape

Ketika kaset Anda telah dimuat ke Arcserve, Anda dapat mencadangkan data. Proses pencadangan sama dengan membuat cadangan kaset fisik.

Untuk mencadangkan data ke kaset

1. Dari menu Mulai Cepat, buka sesi pemulihan cadangan.
2. Pilih tab Sumber, lalu pilih sistem file atau sistem database yang ingin Anda cadangkan.
3. Pilih tab Jadwal dan pilih metode pengulangan yang ingin Anda gunakan.
4. Pilih tab Tujuan dan kemudian pilih rekaman yang ingin Anda gunakan. Jika data yang Anda cadangkan lebih besar dari yang dapat ditahan oleh kaset, Arcserve meminta Anda untuk memasang kaset baru.
5. Pilih Kirim untuk mencadangkan data Anda.

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan mungkin gagal. Untuk menyelesaikan pekerjaan pencadangan yang gagal, Anda harus mengirimkannya kembali.

Mengarsipkan Pita

Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka kaset ke penyimpanan offline. Sebelum Anda mengeluarkan dan mengarsipkan rekaman, Anda mungkin ingin memeriksa konten di dalamnya.

Untuk mengarsipkan kaset

1. Dari menu Mulai Cepat, buka sesi pemulihan cadangan.
2. Pilih tab Sumber, lalu pilih sistem file atau sistem basis data yang ingin Anda cadangkan.

3. Pilih tab Jadwal dan pilih metode pengulangan yang ingin Anda gunakan.
4. Pilih gateway Anda, buka menu konteks (klik kanan) untuk satu kaset, lalu pilih Impor/Ekspor Slot.
5. Tetapkan slot surat untuk memuat kaset. Status di konsol Storage Gateway berubah menjadi Arsip. Proses arsip mungkin memakan waktu lama.

Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman itu muncul sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Ketika pengarsipan selesai, rekaman tidak lagi terdaftar di VTL tetapi diarsipkan dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive.

Memulihkan Data dari Tape

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Gunakan Arcserve untuk memulihkan data. Proses ini sama dengan memulihkan data dari kaset fisik. Untuk petunjuknya, lihat dokumentasi [Arcserve Backup r17](#).

Untuk memulihkan data dari kaset, gunakan prosedur berikut.

Untuk memulihkan data dari kaset

1. Dari menu Mulai Cepat, buka sesi pemulihan pemulihan.
2. Pilih tab Sumber, lalu pilih sistem file atau sistem basis data yang ingin Anda pulihkan.
3. Pilih tab Tujuan dan terima pengaturan default.
4. Pilih tab Jadwal, pilih metode pengulangan yang ingin Anda gunakan, lalu pilih Kirim.

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan Menggunakan Bacula Enterprise

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Bacula Enterprise versi 10. Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi aplikasi cadangan Bacula versi 10 untuk Tape Gateway dan melakukan operasi pencadangan dan pemulihan. Untuk informasi rinci tentang cara menggunakan Bacula versi 10, lihat [Manual dan Dokumentasi Sistem Bacula](#) atau hubungi Sistem Bacula.

Note

Bacula hanya didukung di Linux.

Menyiapkan Bacula Enterprise

Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) Anda ke klien Linux Anda, Anda mengonfigurasi perangkat lunak Bacula untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Anda, lihat [Menghubungkan Perangkat VTL Anda](#)

Untuk mengatur Bacula

1. Dapatkan salinan berlisensi perangkat lunak cadangan Bacula Enterprise dari Bacula Systems.
2. Instal perangkat lunak Bacula Enterprise di komputer lokal atau di cloud Anda.

Untuk informasi tentang cara mendapatkan perangkat lunak penginstalan, lihat [Cadangan Perusahaan untuk Amazon S3 dan Storage Gateway](#). Untuk panduan penginstalan tambahan, lihat whitepaper Bacula [Menggunakan Layanan Cloud dan Penyimpanan Objek dengan Bacula Enterprise Edition](#).

Mengkonfigurasi Bacula untuk Bekerja dengan Perangkat VTL

Selanjutnya, konfigurasi Bacula untuk bekerja dengan perangkat VTL Anda. Berikut ini, Anda dapat menemukan langkah-langkah konfigurasi dasar.

Untuk mengkonfigurasi Bacula

1. Instal Direktori Bacula dan daemon Penyimpanan Bacula. Untuk petunjuk, lihat Bab 7 dari [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#) Bacula white paper.

2. Connect ke sistem yang menjalankan Bacula Director dan konfigurasi inisiator iSCSI. Untuk melakukannya, gunakan skrip yang disediakan pada langkah 7.4 di whitepaper [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#) Bacula.
3. Konfigurasi perangkat penyimpanan. Gunakan skrip yang disediakan di whitepaper Bacula yang dibahas sebelumnya.
4. Konfigurasi Direktur Bacula lokal, tambahkan target penyimpanan, dan tentukan kumpulan media untuk kaset Anda. Gunakan skrip yang disediakan di whitepaper Bacula yang dibahas sebelumnya.

Mencadangkan Data ke Tape

1. Buat kaset di konsol Storage Gateway. Untuk informasi tentang cara membuat kaset, lihat [Membuat Kaset](#).
2. Transfer kaset dari slot I/E ke slot penyimpanan dengan menggunakan perintah berikut.

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

Misalnya, perintah berikut mentransfer kaset dari slot I/E 1601 ke slot penyimpanan 1.

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

3. Luncurkan konsol Bacula dengan menggunakan perintah berikut.

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

Note

Saat Anda membuat dan mentransfer kaset ke Bacula, gunakan perintah Bacula console (bconsole) `update slots storage=VTL` sehingga Bacula tahu tentang kaset baru yang Anda buat.

4. Beri label pita dengan barcode sebagai nama volume atau label dengan menggunakan perintah bconsole berikut.

```
label storage=VTL pool=pool.VTL barcodes === label the tapes with the  
barcode as the volume name / label
```

5. Pasang kaset dengan menggunakan perintah berikut.

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

6. Buat pekerjaan cadangan yang menggunakan kumpulan media yang Anda buat, lalu tulis data ke rekaman virtual dengan menggunakan prosedur yang sama dengan yang Anda lakukan dengan kaset fisik.
7. Lepaskan kaset dari konsol Bacula dengan menggunakan perintah berikut.

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

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan gagal, dan status rekaman di Bacula Enterprise akan berubah menjadi PENUH. Jika Anda tahu rekaman itu belum sepenuhnya digunakan, Anda dapat secara manual mengubah status rekaman kembali ke APPEND dan melanjutkan pekerjaan pencadangan menggunakan pita yang sama. Anda juga dapat melanjutkan pekerjaan pada rekaman yang berbeda jika kaset lain dalam status APPEND tersedia.

Mengarsipkan Pita

Ketika semua pekerjaan cadangan untuk rekaman tertentu selesai dan Anda dapat mengarsipkan rekaman itu, gunakan skrip `mtx-changer` untuk memindahkan pita dari slot penyimpanan ke slot I/E. Tindakan ini mirip dengan aksi `eject` di aplikasi cadangan lainnya.

Untuk mengarsipkan kaset

1. Pindahkan kaset dari slot penyimpanan ke slot I/E dengan menggunakan `/opt/bacula/scripts/mtx-changer` perintah.

Misalnya, perintah berikut mentransfer kaset dari slot penyimpanan 1 ke slot I/E 1601.

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

2. Verifikasi bahwa rekaman itu diarsipkan dalam penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive) dan rekaman tersebut memiliki status Diarsipkan.

Memulihkan Data dari Pita yang Diarsipkan dan Diambil

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan dari arsip ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Kembalikan data Anda dengan menggunakan perangkat lunak Bacula:
 - a. Impor kaset ke dalam slot penyimpanan dengan menggunakan `/opt/bacula/scripts/mtx-changer` perintah untuk mentransfer kaset dari slot I/E.

Misalnya, perintah berikut mentransfer kaset dari slot I/E 1601 ke slot penyimpanan 1.

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

- b. Gunakan konsol Bacula untuk memperbarui slot, lalu pasang kaset.
- c. Jalankan perintah restore untuk memulihkan data Anda. Untuk instruksi, lihat dokumentasi Bacula.

Menguji Pengaturan Anda dengan Menggunakan Commvault

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Commvault versi 11. Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengonfigurasi aplikasi cadangan Commvault untuk Tape Gateway, melakukan arsip cadangan, dan mengambil data Anda dari kaset yang diarsipkan. Untuk informasi terperinci tentang cara menggunakan Commvault, lihat [Panduan Memulai Cepat Commvault](#) di situs web Commvault.

Topik

- [Mengkonfigurasi Commvault untuk Bekerja dengan Perangkat VTL](#)
- [Membuat Kebijakan Penyimpanan dan Subklien](#)
- [Mencadangkan Data ke Tape di Commvault](#)
- [Mengarsipkan Tape di Commvault](#)
- [Memulihkan Data dari Tape](#)

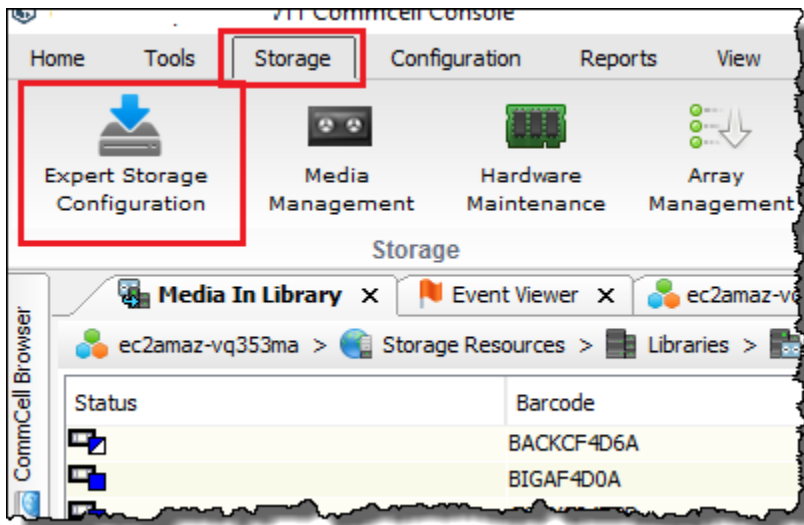
Mengkonfigurasi Commvault untuk Bekerja dengan Perangkat VTL

Setelah Anda menghubungkan perangkat VTL ke klien Windows, Anda mengonfigurasi Commvault untuk mengenalinya. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows, lihat. [Menghubungkan Perangkat VTL Anda ke klien Windows](#)

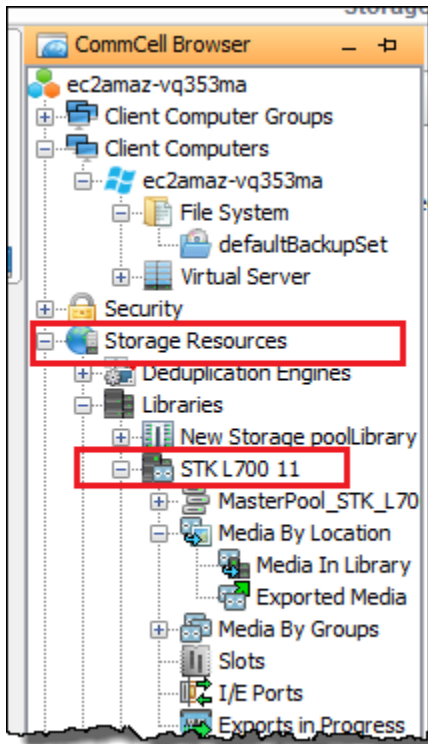
Aplikasi cadangan Commvault tidak secara otomatis mengenali perangkat VTL. Anda harus menambahkan perangkat secara manual untuk mengeksposnya ke aplikasi cadangan Commvault dan kemudian menemukan perangkat.

Untuk mengkonfigurasi Commvault

1. Di menu utama CommCell konsol, pilih Storage, lalu pilih Expert Storage Configuration untuk membuka kotak MediaAgents dialog Select.



2. Pilih agen media yang tersedia yang ingin Anda gunakan, pilih Tambah, lalu pilih OK.
3. Di kotak dialog Expert Storage Configuration, pilih Mulai, lalu pilih Deteksi/Konfigurasi Perangkat.
4. Biarkan opsi Jenis Perangkat dipilih, pilih Deteksi Lengkap, lalu pilih OK.
5. Di kotak Konfirmasi Deteksi Lengkap, pilih Ya.
6. Di kotak dialog Pemilihan Perangkat, pilih perpustakaan Anda dan semua drive-nya, lalu pilih OK. Tunggu perangkat Anda terdeteksi, lalu pilih Tutup untuk menutup laporan log.
7. Klik kanan perpustakaan Anda, pilih Konfigurasi, lalu pilih Ya. Tutup kotak dialog konfigurasi.
8. Di Apakah perpustakaan ini memiliki pembaca kode batang? kotak dialog, pilih Ya, dan kemudian untuk jenis perangkat, pilih IBM ULTRIUM V5.
9. Di CommCell browser, pilih Sumber Daya Penyimpanan, lalu pilih Pustaka untuk melihat pustaka rekaman Anda.



10. Untuk melihat kaset di pustaka, buka menu konteks (klik kanan) untuk pustaka Anda, lalu pilih Temukan Media, Lokasi media, Perpustakaan Media.
11. Untuk memasang kaset Anda, buka menu konteks (klik kanan) untuk media Anda, lalu pilih Muat.

Membuat Kebijakan Penyimpanan dan Subklien

Setiap pekerjaan pencadangan dan pemulihan dikaitkan dengan kebijakan penyimpanan dan kebijakan subklien.

Kebijakan penyimpanan memetakan lokasi asli data ke media Anda.

Untuk membuat kebijakan penyimpanan

1. Di CommCell browser, pilih Kebijakan.
2. Buka menu konteks (klik kanan) untuk Kebijakan Penyimpanan, lalu pilih Kebijakan Penyimpanan Baru.
3. Di wizard Buat Kebijakan Penyimpanan, pilih Perlindungan Data dan Pengarsipan, lalu pilih Berikutnya.

4. Ketik nama untuk Nama Kebijakan Penyimpanan, lalu pilih Kebijakan Penyimpanan Tambahan. Untuk mengaitkan kebijakan penyimpanan ini dengan beban tambahan, pilih salah satu opsi. Jika tidak, biarkan opsi tidak dicentang, lalu pilih Berikutnya.
5. Dalam Apakah Anda ingin menggunakan kebijakan deduplikasi global? kotak dialog, pilih preferensi Deduplikasi Anda, lalu pilih Berikutnya.
6. Dari Library for Primary Copy, pilih library VTL Anda, lalu pilih Next.
7. Verifikasi bahwa pengaturan agen media Anda sudah benar, lalu pilih Berikutnya.
8. Verifikasi bahwa pengaturan kumpulan goresan Anda sudah benar, lalu pilih Berikutnya.
9. Konfigurasi kebijakan penyimpanan Anda di data Backup Agen iData, lalu pilih Berikutnya.
10. Tinjau pengaturan enkripsi, lalu pilih Berikutnya.
11. Untuk melihat kebijakan penyimpanan Anda, pilih Kebijakan Penyimpanan.

Anda membuat kebijakan subklien dan mengaitkannya dengan kebijakan penyimpanan Anda. Kebijakan subklien memungkinkan Anda mengonfigurasi klien sistem file serupa dari templat pusat, sehingga Anda tidak perlu menyiapkan banyak sistem file serupa secara manual.

Untuk membuat kebijakan subklien

1. Di CommCell browser, pilih Komputer Klien, lalu pilih komputer klien Anda. Pilih File System, lalu pilih defaultBackupSet.
2. Klik kanan defaultBackupSet, pilih Semua Tugas, lalu pilih Subklien Baru.
3. Di kotak properti Subclient, ketikkan nama di SubClient Nama, lalu pilih OK.
4. Pilih Browse, navigasikan ke file yang ingin Anda cadangkan, pilih Tambah, lalu tutup kotak dialog.
5. Di kotak properti Subklien, pilih tab Perangkat Penyimpanan, pilih kebijakan penyimpanan dari kebijakan Penyimpanan, lalu pilih OK.
6. Di jendela Jadwal Cadangan yang muncul, kaitkan subklien baru dengan jadwal cadangan.
7. Pilih Jangan Jadwalkan untuk satu kali atau cadangan sesuai permintaan, lalu pilih OK.

Anda sekarang harus melihat subklien Anda di defaultBackupSettab.

Mencadangkan Data ke Tape di Commvault

Anda membuat pekerjaan cadangan dan menulis data ke rekaman virtual dengan menggunakan prosedur yang sama yang Anda gunakan dengan kaset fisik. Untuk informasi selengkapnya, lihat dokumentasi [Commvault](#).

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan mungkin gagal. Dalam beberapa kasus, Anda dapat memilih opsi untuk melanjutkan pekerjaan yang gagal. Jika tidak, Anda harus mengirimkan pekerjaan baru. Jika Commvault menandai rekaman itu sebagai tidak dapat digunakan setelah pekerjaan gagal, Anda harus memuat ulang rekaman ke drive untuk terus menulis ke sana. Jika beberapa kaset tersedia, Commvault mungkin melanjutkan pekerjaan pencadangan yang gagal pada rekaman yang berbeda.

Mengarsipkan Tape di Commvault

Anda memulai proses pengarsipan dengan mengeluarkan rekaman itu. Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka kaset ke penyimpanan offline. Sebelum Anda mengeluarkan dan mengarsipkan kaset, Anda mungkin ingin terlebih dahulu memeriksa konten pada rekaman itu.

Untuk mengarsipkan kaset

1. Di CommCell browser, pilih Sumber Daya Penyimpanan, Pustaka, lalu pilih Perpustakaan Anda. Pilih Media Berdasarkan Lokasi, lalu pilih Media Di Perpustakaan.
2. Buka menu konteks (klik kanan) untuk rekaman yang ingin Anda arsipkan, pilih Semua Tugas, pilih Ekspor, lalu pilih OK.

Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman itu muncul sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Saat pengarsipan selesai, rekaman itu tidak lagi tercantum dalam VTL.

Dalam perangkat lunak Commvault, verifikasi bahwa rekaman itu tidak lagi ada di slot penyimpanan.

Di panel navigasi konsol Storage Gateway, pilih Tapes. Verifikasi bahwa status rekaman arsip Anda DIARSIPKAN.

Memulihkan Data dari Tape

Anda dapat memulihkan data dari rekaman yang belum pernah diarsipkan dan diambil, atau dari rekaman yang telah diarsipkan dan diambil. Untuk kaset yang belum pernah diarsipkan dan diambil (kaset yang tidak diambil), Anda memiliki dua opsi untuk memulihkan data:

- Pulihkan oleh subklien
- Pulihkan dengan ID pekerjaan

Untuk memulihkan data dari rekaman yang tidak diambil oleh subklien

1. Di CommCell browser, pilih Komputer Klien, lalu pilih komputer klien Anda. Pilih File System, lalu pilih defaultBackupSet.
2. Buka menu konteks (klik kanan) untuk subklien Anda, pilih Jelajahi dan Pulihkan, lalu pilih Lihat Konten.
3. Pilih file yang ingin Anda pulihkan, lalu pilih Recover All Selected.
4. Pilih Home, lalu pilih Job Controller untuk memantau status pekerjaan pemulihan Anda.

Untuk memulihkan data dari rekaman yang tidak diambil oleh ID pekerjaan

1. Di CommCell browser, pilih Komputer Klien, lalu pilih komputer klien Anda. Klik kanan File System, pilih View, lalu pilih Backup History.
2. Dalam kategori Jenis Cadangan, pilih jenis pekerjaan cadangan yang Anda inginkan, lalu pilih OK. Tab dengan riwayat pekerjaan cadangan muncul.
3. Temukan Job ID yang ingin Anda pulihkan, klik kanan, lalu pilih Browse and Restore.
4. Dalam kotak dialog Browse and Restore Options, pilih Lihat Konten.
5. Pilih file yang ingin Anda pulihkan, lalu pilih Recover All Selected.
6. Pilih Home, lalu pilih Job Controller untuk memantau status pekerjaan pemulihan Anda.

Untuk memulihkan data dari rekaman yang diarsipkan dan diambil

1. Di CommCell browser, pilih Sumber Daya Penyimpanan, pilih Pustaka, lalu pilih Perpustakaan Anda. Pilih Media Berdasarkan Lokasi, lalu pilih Media Di Perpustakaan.
2. Klik kanan rekaman yang diambil, pilih Semua Tugas, lalu pilih Katalog.
3. Di kotak dialog Catalog Media, pilih Katalog saja, lalu pilih OK.

4. Pilih CommCell Home, lalu pilih Job Controller untuk memantau status pekerjaan pemulihan Anda.
5. Setelah pekerjaan berhasil, buka menu konteks (klik kanan) untuk rekaman Anda, pilih Lihat, lalu pilih Lihat Konten Katalog. Perhatikan nilai Job ID untuk digunakan nanti.
6. Pilih Recatalog/Merge. Pastikan bahwa Merge hanya dipilih di kotak dialog Catalog Media.
7. Pilih Home, lalu pilih Job Controller untuk memantau status pekerjaan pemulihan Anda.
8. Setelah pekerjaan berhasil, pilih CommCell Home, pilih Control Panel, dan kemudian pilih Browse/Search/Recovery.
9. Pilih Tampilkan data lama selama penelusuran dan pemulihan, pilih OK, lalu tutup Control Panel.
10. Di CommCell browser, klik kanan Komputer Klien, lalu pilih komputer klien Anda. Pilih Lihat, lalu pilih Job History.
11. Di kotak dialog Filter Riwayat Pekerjaan, pilih Advanced.
12. Pilih Sertakan Data Berusia, lalu pilih OK.
13. Di kotak dialog Job History, pilih OK untuk membuka tab riwayat pekerjaan.
14. Temukan pekerjaan yang ingin Anda pulihkan, buka menu konteks (klik kanan) untuknya, lalu pilih Browse and Restore.
15. Dalam kotak dialog Browse and Restore, pilih Lihat Konten.
16. Pilih file yang ingin Anda pulihkan, lalu pilih Recover All Selected.
17. Pilih Home, lalu pilih Job Controller untuk memantau status pekerjaan pemulihan Anda.

Menguji Pengaturan Anda dengan Menggunakan Dell EMC NetWorker

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Dell EMC 19.5. NetWorker Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi NetWorker perangkat lunak Dell EMC untuk bekerja dengan Tape Gateway dan melakukan pencadangan, termasuk cara mengonfigurasi perangkat penyimpanan, menulis data ke kaset, mengarsipkan kaset, dan mengembalikan data dari kaset.

Untuk informasi rinci tentang cara menginstal dan menggunakan NetWorker perangkat lunak Dell EMC, lihat Panduan [Administrasi](#).

Untuk informasi selengkapnya tentang aplikasi cadangan yang kompatibel, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Topik


- [Mengkonfigurasi untuk Bekerja dengan Perangkat VTL](#)
- [Mengizinkan Impor Kaset WORM ke Dell EMC NetWorker](#)
- [Mencadangkan Data ke Tape di Dell EMC NetWorker](#)
- [Mengarsipkan Tape di Dell EMC NetWorker](#)
- [Memulihkan Data dari Pita yang Diarsipkan di Dell EMC NetWorker](#)

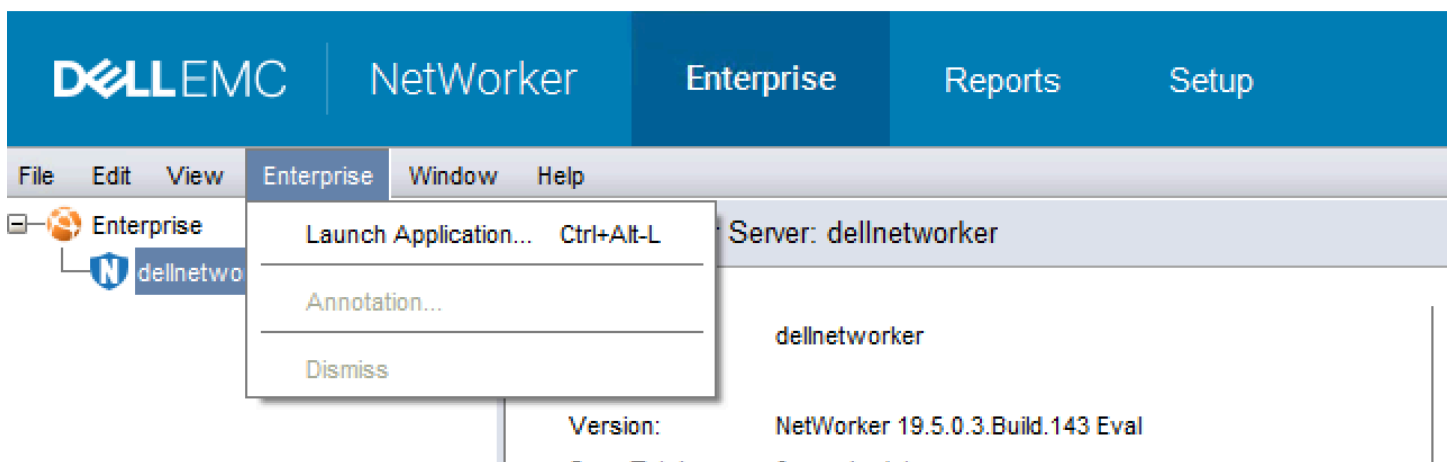
Mengkonfigurasi untuk Bekerja dengan Perangkat VTL

Setelah menghubungkan perangkat pustaka pita virtual (VTL) ke klien Microsoft Windows, Anda mengonfigurasi untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows, lihat [Menghubungkan Perangkat VTL Anda](#)

tidak secara otomatis mengenali perangkat Tape Gateway. Untuk mengekspos perangkat VTL Anda ke perangkat NetWorker lunak dan mendapatkan perangkat lunak untuk menemukannya, Anda secara manual mengkonfigurasi perangkat lunak. Berikut ini, kami berasumsi bahwa Anda telah menginstal perangkat lunak dengan benar dan bahwa Anda terbiasa dengan Konsol Manajemen. Untuk informasi selengkapnya tentang Management Console, lihat bagian antarmuka NetWorker Management Console pada Panduan [NetWorker Administrasi EMC Dell](#).

Screen shot berikut menunjukkan Dell EMC 19.5 NetWorker .

 NetWorker Management Console V19.5.0.3 - localhost



Untuk mengkonfigurasi perangkat lunak Dell EMC untuk NetWorker perangkat VTL

1. Mulai aplikasi Dell EMC NetWorker Management Console, pilih Enterprise dari menu, lalu pilih localhost dari panel kiri.

2. Buka menu konteks (klik kanan) untuk localhost, lalu pilih Luncurkan Aplikasi.
3. Pilih tab Perangkat, buka menu konteks (klik kanan) untuk Pustaka, lalu pilih Pindai Perangkat.
4. Di wizard Pindai Perangkat, pilih Mulai Pindai, lalu pilih OK dari kotak dialog yang muncul.
5. Perluas pohon folder Libraries untuk melihat semua pustaka Anda dan tekan F5 untuk menyegarkan. Proses ini mungkin memakan waktu beberapa detik untuk memuat perangkat ke perpustakaan.
6. Buka jendela perintah (CMD.exe) dengan hak istimewa admin dan jalankan utilitas “jbconfig” yang diinstal dengan Dell EMC 19.5. NetWorker

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

C:\Users\Administrator>jbconfig

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

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

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

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

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

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

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

```

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

Jukebox has been added successfully

The following configuration options have been set:

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

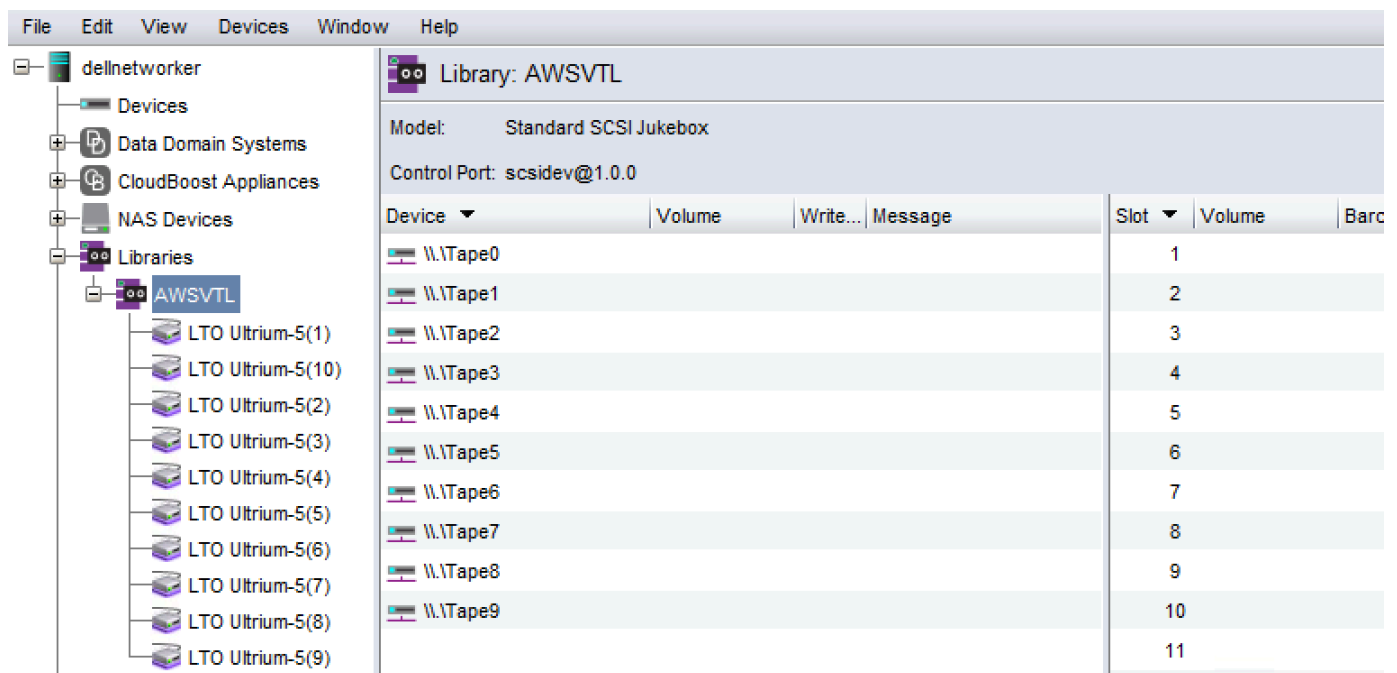
You can review and change the characteristics of the autochanger and its
associated devices using the NetWorker Management Console.

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

C:\Users\Administrator>_

```

7. Saat “jbconfig” selesai, kembali ke GUI NetWorker dan tekan F5 untuk menyegarkan.
8. Pilih perpustakaan Anda untuk melihat kaset Anda di panel kiri dan daftar slot volume kosong yang sesuai di panel kanan. Dalam tangkapan layar ini, perpustakaan AWSVTL "" dipilih.



9. Dalam daftar volume, pilih volume yang ingin Anda aktifkan (volume yang dipilih disorot), buka menu konteks (klik kanan) untuk volume yang dipilih, lalu pilih Deposit. Tindakan ini memindahkan pita dari slot I/E ke slot volume.

10. Di kotak dialog yang muncul, pilih Ya, dan kemudian di kotak dialog Muat Kartrid ke dalam, pilih Ya.
11. Jika Anda tidak memiliki kaset lagi untuk disetor, pilih Tidak atau Abaikan. Jika tidak, pilih Ya untuk menyettor kaset tambahan.

Mengizinkan Impor Kaset WORM ke Dell EMC NetWorker

Anda sekarang siap untuk mengimpor kaset dari Tape Gateway Anda ke perpustakaan Dell NetWorker EMC.

Kaset virtual ditulis setelah membaca banyak kaset (WORM), tetapi Dell EMC NetWorker mengharapkan kaset Non-worm. Agar Dell EMC NetWorker dapat bekerja dengan kaset virtual Anda, Anda harus mengaktifkan impor kaset ke kolam media non-worm.

Untuk memungkinkan impor kaset WORM ke kolam media non-worm

1. Di NetWorker Console, pilih Media, buka menu konteks (klik kanan) untuk localhost, lalu pilih Properties.
2. Di jendela NetWorker Sever Properties, pilih tab Configuration.
3. Di bagian penanganan pita Worm, kosongkan kaset WORM hanya di kotak kolam WORM, lalu pilih OK.

Mencadangkan Data ke Tape di Dell EMC NetWorker

Mencadangkan data ke kaset adalah proses dua langkah.

1. Beri label pada kaset yang ingin Anda buat cadangan data, buat kumpulan media target, dan tambahkan kaset ke kolam.

Anda membuat kumpulan media dan menulis data ke rekaman virtual dengan menggunakan prosedur yang sama dengan kaset fisik. Untuk informasi lebih lanjut, lihat bagian Backing Up Data dari Panduan Administrasi [Dell EMC NetWorker](#).

2. Tulis data ke rekaman itu. Anda mencadangkan data dengan menggunakan aplikasi NetWorker Pengguna Dell EMC alih-alih Konsol Manajemen NetWorker EMC Dell. Aplikasi NetWorker Pengguna Dell EMC diinstal sebagai bagian dari instalasi. NetWorker

Note

Anda menggunakan aplikasi NetWorker Pengguna Dell EMC untuk melakukan pencadangan, tetapi Anda melihat status pencadangan dan pemulihan pekerjaan di EMC Management Console. Untuk melihat status, pilih menu Perangkat dan lihat status di jendela Log.

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan ditangguhkan, dan status rekaman di Dell EMC NetWorker akan berubah menjadi Write Protected. Anda dapat mengarsipkan rekaman atau terus membaca data darinya. Anda dapat melanjutkan pekerjaan cadangan yang ditangguhkan pada rekaman yang berbeda.

Mengarsipkan Tape di Dell EMC NetWorker

Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka NetWorker pita Dell EMC ke penyimpanan offline. Anda memulai arsip rekaman dengan mengeluarkan selotip dari tape drive ke slot penyimpanan. Anda kemudian menarik kaset dari slot ke arsip dengan menggunakan aplikasi cadangan Anda — yaitu, perangkat lunak Dell EMC. NetWorker

Untuk mengarsipkan rekaman dengan menggunakan Dell EMC NetWorker

1. Pada tab Devices di jendela NetWorker Administrasi, pilih localhost atau server EMC Anda, lalu pilih Libraries.
2. Pilih perpustakaan yang Anda impor dari pustaka rekaman virtual Anda.
3. Dari daftar kaset yang telah Anda tulis datanya, buka menu konteks (klik kanan) untuk rekaman yang ingin Anda arsipkan, lalu pilih Eject/Withdraw.
4. Di kotak konfirmasi yang muncul, pilih OK.

Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman itu muncul sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Saat pengarsipan selesai, rekaman itu tidak lagi tercantum dalam VTL.

Dalam NetWorker perangkat lunak Dell EMC, verifikasi bahwa rekaman itu tidak lagi ada di slot penyimpanan.

Di panel navigasi konsol Storage Gateway, pilih Tapes. Verifikasi bahwa status rekaman arsip Anda DIARSIPKAN.

Memulihkan Data dari Pita yang Diarsipkan di Dell EMC NetWorker

Memulihkan data yang diarsipkan adalah proses dua langkah:

1. Ambil rekaman yang diarsipkan dari Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Gunakan perangkat NetWorker lunak Dell EMC untuk memulihkan data. Anda melakukan ini dengan membuat memulihkan file folder, seperti yang Anda lakukan saat memulihkan data dari kaset fisik. Untuk petunjuk, lihat bagian Menggunakan program NetWorker Pengguna dari Panduan [NetWorker Administrasi Dell EMC](#).

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan Menggunakan IBM Spectrum Protect

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan IBM Spectrum Protect with. AWS Storage Gateway (IBM Spectrum Protect sebelumnya dikenal sebagai Tivoli Storage Manager.)

Topik ini berisi informasi dasar tentang cara mengkonfigurasi perangkat lunak cadangan IBM Spectrum Protect versi 8.1.10 untuk Tape Gateway. Ini juga mencakup informasi dasar tentang melakukan operasi pencadangan dan pemulihan dengan IBM Spectrum Protect. Untuk informasi selengkapnya tentang cara mengelola perangkat lunak cadangan IBM Spectrum Protect, lihat [Ikhtisar tugas administrasi](#) IBM untuk IBM Spectrum Protect.

Perangkat lunak cadangan IBM Spectrum Protect mendukung AWS Storage Gateway pada sistem operasi berikut.

- Microsoft Windows Server
- Topi Merah Linux

Untuk informasi tentang perangkat yang didukung IBM Spectrum Protect untuk Windows, lihat Perangkat yang [Didukung IBM Spectrum Protect \(sebelumnya Tivoli Storage Manager\) untuk AIX, HP-UX, Solaris](#), dan Windows.

Untuk informasi tentang perangkat yang didukung IBM Spectrum Protect untuk Linux, lihat Perangkat yang Didukung [IBM Spectrum Protect \(sebelumnya Tivoli Storage Manager\)](#) untuk Linux.

Topik

- [Menyiapkan IBM Spectrum Protect](#)
- [Mengkonfigurasi IBM Spectrum Protect untuk Bekerja dengan Perangkat VTL](#)
- [Menulis Data ke Pita di IBM Spectrum Protect](#)
- [Memulihkan Data dari Tape yang Diarsipkan di IBM Spectrum Protect](#)

Menyiapkan IBM Spectrum Protect

Setelah Anda menghubungkan perangkat VTL Anda ke klien Anda, Anda mengonfigurasi perangkat lunak IBM Spectrum Protect versi 8.1.10 untuk mengenalinya. Untuk informasi selengkapnya tentang menghubungkan perangkat VTL ke klien Anda, lihat [Menghubungkan Perangkat VTL Anda](#)

Untuk mengatur IBM Spectrum Protect

1. Dapatkan salinan berlisensi perangkat lunak IBM Spectrum Protect versi 8.1.10 dari IBM.
2. Instal perangkat lunak IBM Spectrum Protect di lingkungan lokal atau instans Amazon EC2 di cloud. Untuk informasi selengkapnya, lihat dokumentasi [Instalasi dan peningkatan IBM untuk IBM Spectrum Protect](#).

Untuk informasi selengkapnya tentang mengonfigurasi perangkat lunak IBM Spectrum Protect, lihat [Mengonfigurasi pustaka AWS pita virtual Tape Gateway untuk server IBM Spectrum Protect](#).

Mengkonfigurasi IBM Spectrum Protect untuk Bekerja dengan Perangkat VTL

Selanjutnya, konfigurasikan IBM Spectrum Protect untuk bekerja dengan perangkat VTL Anda. Anda dapat mengonfigurasi IBM Spectrum Protect untuk bekerja dengan perangkat VTL di Microsoft Windows Server atau Red Hat Linux.

Mengkonfigurasi IBM Spectrum Protect untuk Windows

Untuk petunjuk lengkap tentang cara mengkonfigurasi IBM Spectrum Protect pada Windows, lihat [Tape Device Driver-W12 6266 untuk Windows 2012](#) di situs web Lenovo. Berikut ini adalah dokumentasi dasar tentang proses tersebut.

Untuk mengkonfigurasi IBM Spectrum Protect untuk Microsoft Windows

1. Dapatkan paket driver yang tepat untuk media changer Anda. Untuk driver perangkat pita, IBM Spectrum Protect memerlukan versi W12 6266 untuk Windows 2012. Untuk petunjuk tentang cara mendapatkan driver, lihat [Tape Device Driver-W12 6266 untuk Windows 2012](#) di situs web Lenovo.

Note

Pastikan Anda menginstal set driver “non-eksklusif”.

2. Di komputer Anda, buka Manajemen Komputer, perluas perangkat Media Changer, dan verifikasi bahwa jenis media changer terdaftar sebagai IBM 3584 Tape Library.
3. Pastikan kode batang untuk rekaman apa pun di pustaka pita virtual adalah delapan karakter atau kurang. Jika Anda mencoba menetapkan kode batang pita Anda yang lebih panjang dari delapan karakter, Anda mendapatkan pesan kesalahan ini: "Tape barcode is too long for media changer".
4. Pastikan semua tape drive dan media changer Anda muncul di IBM Spectrum Protect. Untuk melakukannya, gunakan perintah berikut: `\Tivoli\TSM\server>tsmdlst.exe`

Konfigurasi IBM Spectrum Protect untuk Linux

Berikut ini adalah dokumentasi dasar tentang mengkonfigurasi IBM Spectrum untuk bekerja dengan perangkat VTL di Linux.

Untuk mengkonfigurasi IBM Spectrum Protect untuk Linux

1. Buka [IBM Fix Central](#) di situs web IBM Support, dan pilih Pilih produk.
2. Untuk Grup Produk, pilih Penyimpanan Sistem.
3. Untuk Pilih dari Penyimpanan Sistem, pilih Sistem pita.
4. Untuk sistem Tape, pilih driver dan perangkat lunak Tape.
5. Untuk Pilih dari driver dan perangkat lunak Tape, pilih driver perangkat Tape.

6. Untuk Platform, pilih sistem operasi Anda dan pilih Lanjutkan.
7. Pilih versi driver perangkat yang ingin Anda unduh. Kemudian ikuti instruksi pada halaman unduhan Fix Central untuk mengunduh dan mengkonfigurasi IBM Spectrum Protect.
8. Pastikan kode batang untuk rekaman apa pun di pustaka pita virtual adalah delapan karakter atau kurang. Jika Anda mencoba menetapkan kode batang pita Anda yang lebih panjang dari delapan karakter, Anda mendapatkan pesan kesalahan ini: "Tape barcode is too long for media changer".

Menulis Data ke Pita di IBM Spectrum Protect

Anda menulis data ke pita virtual Tape Gateway dengan menggunakan prosedur dan kebijakan cadangan yang sama yang Anda lakukan dengan kaset fisik. Buat konfigurasi yang diperlukan untuk pencadangan dan pemulihan pekerjaan. Untuk informasi selengkapnya tentang mengonfigurasi IBM Spectrum Protect, lihat [Ikhtisar tugas administrasi](#) untuk IBM Spectrum Protect.

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan mungkin gagal. Jika pekerjaan pencadangan gagal, status rekaman di IBM Spectrum Protect berubah menjadi ReadOnly. Jika Anda tahu rekaman itu belum sepenuhnya digunakan, Anda dapat secara manual mengubah status rekaman kembali ReadWrite, dan melanjutkan atau mengirim ulang pekerjaan cadangan menggunakan rekaman yang sama. IBM Spectrum Protect mungkin melanjutkan pekerjaan pencadangan yang gagal pada rekaman yang berbeda jika kaset lain dalam ReadWrite status tersedia.

Memulihkan Data dari Tape yang Diarsipkan di IBM Spectrum Protect

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan dari arsip ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Kembalikan data dengan menggunakan perangkat lunak cadangan IBM Spectrum Protect. Anda melakukan ini dengan membuat titik pemulihan, seperti yang Anda lakukan saat memulihkan

data dari kaset fisik. Untuk informasi selengkapnya tentang mengonfigurasi IBM Spectrum Protect, lihat [Ikhtisar tugas administrasi](#) untuk IBM Spectrum Protect.

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan Menggunakan Pelindung Data Micro Focus (HPE)

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Pelindung Data Micro Focus (HPE) v9.x. Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi perangkat lunak Pelindung Data Micro Focus (HPE) untuk Tape Gateway dan melakukan operasi pencadangan dan pemulihan. Untuk informasi rinci tentang cara menggunakan perangkat lunak Pelindung Data Micro Focus (HPE), lihat dokumentasi Hewlett Packard. Untuk informasi selengkapnya tentang aplikasi cadangan yang kompatibel, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Topik

- [Mengkonfigurasi Pelindung Data Fokus Mikro \(HPE\) untuk Bekerja dengan Perangkat VTL](#)
- [Mempersiapkan Kaset Virtual untuk Digunakan dengan HPE Data Protector](#)
- [Memuat Kaset ke Media Pool](#)
- [Mencadangkan Data ke Tape](#)
- [Mengarsipkan Pita](#)
- [Memulihkan Data dari Tape](#)

Mengkonfigurasi Pelindung Data Fokus Mikro (HPE) untuk Bekerja dengan Perangkat VTL

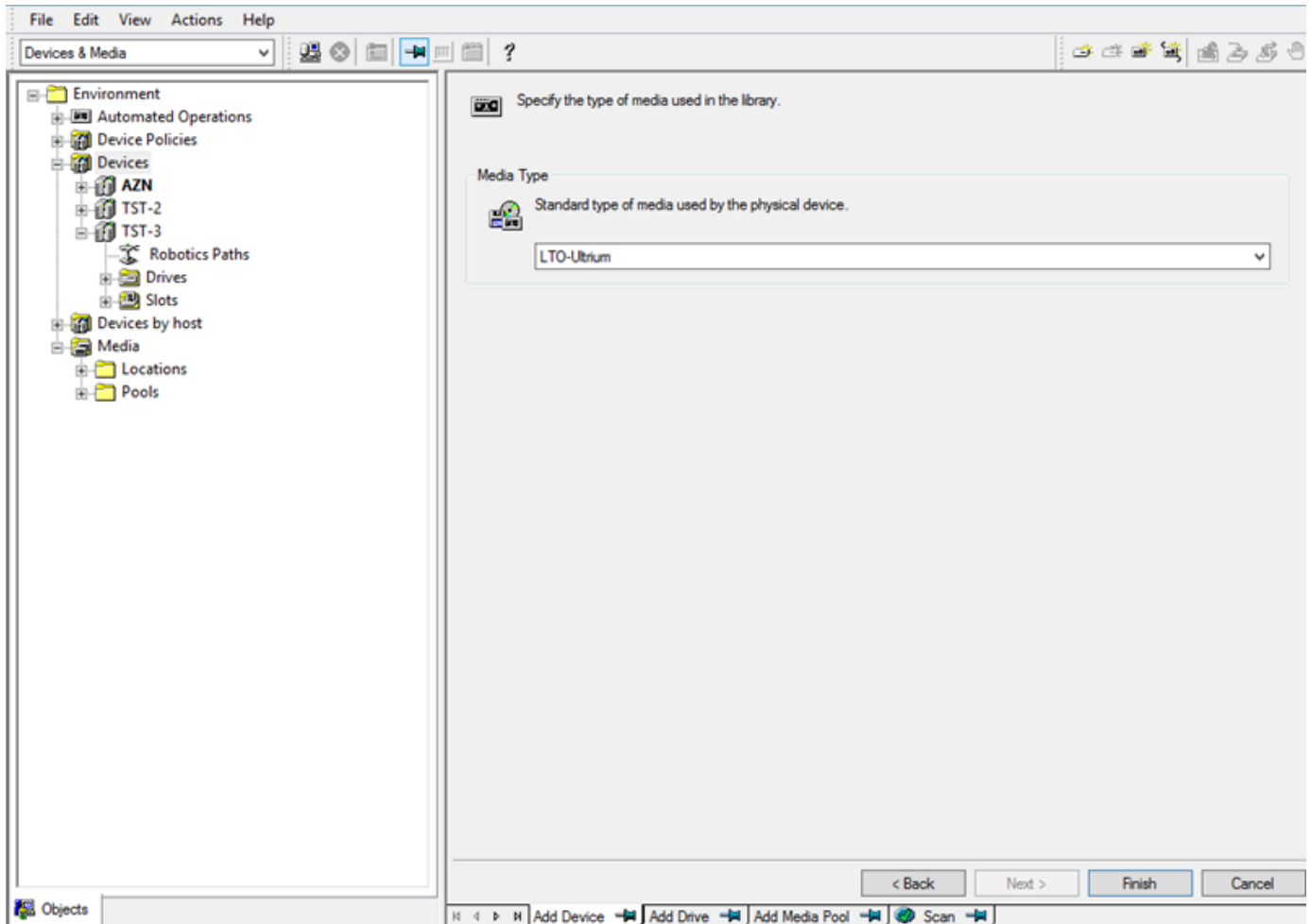
Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) ke klien, Anda mengonfigurasi Pelindung Data Micro Focus (HPE) untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien, lihat [Menghubungkan Perangkat VTL Anda](#)

Perangkat lunak Pelindung Data Micro Focus (HPE) tidak secara otomatis mengenali perangkat Tape Gateway. Agar perangkat lunak mengenali perangkat ini, tambahkan perangkat secara manual dan kemudian temukan perangkat VTL, seperti yang dijelaskan berikut.

Untuk menambahkan perangkat VTL

1. Di jendela utama Pelindung Data Fokus Mikro (HPE), pilih rak Perangkat & Media dalam daftar di kiri atas.

Buka menu konteks (klik kanan) untuk Perangkat, dan pilih Tambah Perangkat.



2. Pada tab Tambah Perangkat, ketikkan nilai untuk Nama Perangkat. Untuk Jenis Perangkat, pilih Perpustakaan SCSI, lalu pilih Berikutnya.
3. Pada layar berikutnya, lakukan hal berikut:
 - a. Untuk alamat SCSI robot perpustakaan, pilih alamat spesifik Anda.
 - b. Untuk Pilih tindakan apa yang harus dilakukan Pelindung Data jika drive sibuk, pilih “Batalan” atau tindakan pilihan Anda.
 - c. Pilih untuk mengaktifkan opsi ini:
 - Dukungan pembaca barcode

- Secara otomatis menemukan alamat SCSI yang diubah
 - Cadangan/Rilis SCSI (kontrol robot)
- d. Biarkan Gunakan barcode sebagai label media pada inisialisasi yang jelas (tidak dicentang), kecuali sistem Anda memerlukannya.
 - e. Pilih Next untuk melanjutkan.
4. Pada layar berikutnya, tentukan slot yang ingin Anda gunakan dengan HP Data Protector. Gunakan tanda hubung (“-”) di antara angka untuk menunjukkan rentang slot, misalnya 1-6. Ketika Anda telah menentukan slot untuk digunakan, pilih Berikutnya.
 5. Untuk jenis media standar yang digunakan oleh perangkat fisik, pilih LTO_Ultrium, lalu pilih Selesai untuk menyelesaikan pengaturan.

Pustaka rekaman Anda sekarang siap digunakan. Untuk memuat kaset ke dalamnya, lihat bagian selanjutnya.

Mempersiapkan Kaset Virtual untuk Digunakan dengan HPE Data Protector

Sebelum Anda dapat mencadangkan data ke kaset virtual, Anda perlu menyiapkan rekaman untuk digunakan. Melakukan hal ini melibatkan tindakan berikut:

- Muat kaset virtual ke perpustakaan kaset
- Muat kaset virtual ke dalam slot
- Buat kolam media
- Muat kaset virtual ke kolam media

Di bagian berikut, Anda dapat menemukan langkah-langkah untuk memandu Anda melalui proses ini.

Memuat Kaset Virtual ke Perpustakaan Tape

Pustaka rekaman Anda sekarang harus terdaftar di bawah Perangkat. Jika Anda tidak melihatnya, tekan F5 untuk menyegarkan layar. Ketika perpustakaan Anda terdaftar, Anda dapat memuat kaset virtual ke dalam perpustakaan.

Untuk memuat kaset virtual ke perpustakaan kaset Anda

1. Pilih tanda plus di sebelah pustaka kaset Anda untuk menampilkan node untuk jalur robotika, drive, dan slot.

2. Buka menu konteks (klik kanan) untuk Drive, pilih Tambah Drive, ketik nama untuk rekaman Anda, lalu pilih Berikutnya untuk melanjutkan.
3. Pilih tape drive yang ingin Anda tambahkan untuk alamat SCSI drive data, pilih Secara otomatis menemukan alamat SCSI yang diubah, lalu pilih Berikutnya.
4. Pada layar berikut, pilih Advanced. Layar pop-up Opsi Lanjutan muncul.
 - a. Pada tab Pengaturan, Anda harus mempertimbangkan opsi berikut:
 - CRC Check (untuk mendeteksi perubahan data yang tidak disengaja)
 - Deteksi drive kotor (untuk memastikan drive bersih sebelum cadangan)
 - SCSI Reserve/Release (drive) (untuk menghindari pertengkaran tape)
 - b. Untuk tujuan pengujian, Anda dapat membiarkan opsi ini dinonaktifkan (tidak dicentang).
 - c. Pada tab Ukuran, atur ukuran Blok (kB) ke Default (256).
 - c. Pilih OK untuk menutup layar opsi lanjutan, lalu pilih Berikutnya untuk melanjutkan.
5. Pada layar berikutnya, pilih opsi ini di bawah Kebijakan Perangkat:
 - Perangkat dapat digunakan untuk memulihkan
 - Perangkat dapat digunakan sebagai perangkat sumber untuk salinan objek
6. Pilih Selesai untuk menyelesaikan menambahkan tape drive Anda ke perpustakaan kaset Anda.

Memuat Kaset Virtual ke Slot

Sekarang setelah Anda memiliki tape drive di perpustakaan kaset Anda, Anda dapat memuat kaset virtual ke dalam slot.

Untuk memuat kaset ke dalam slot

1. Di node pohon pustaka tape, buka simpul berlabel Slots. Setiap slot memiliki status yang diwakili oleh ikon:
 - Pita hijau berarti selotip sudah dimuat ke dalam slot.
 - Slot abu-abu berarti slotnya kosong.
 - Tanda tanya cyan berarti rekaman di slot itu tidak diformat.
2. Untuk slot kosong, buka menu konteks (klik kanan), lalu pilih Enter. Jika Anda memiliki kaset yang ada, pilih satu untuk dimuat ke dalam slot itu.

Membuat Media Pool

Media pool adalah grup logis yang digunakan untuk mengatur kaset Anda. Untuk mengatur cadangan tape, Anda membuat kumpulan media.

Untuk membuat kolam media

1. Di rak Perangkat & Media, buka simpul pohon untuk Media, buka menu konteks (klik kanan) untuk node Pools, lalu pilih Add Media Pool.
2. Untuk nama Pool, ketikkan nama.
3. Untuk Jenis Media, pilih LTO_Ultrium, lalu pilih Berikutnya.
4. Pada layar berikut, terima nilai default, lalu pilih Berikutnya.
5. Pilih Selesai untuk menyelesaikan pembuatan kumpulan media.

Memuat Kaset ke Media Pool

Sebelum Anda dapat mencadangkan data ke kaset Anda, Anda harus memuat kaset ke kolam media yang Anda buat.

Untuk memuat rekaman virtual ke kolam media

1. Pada node pohon pustaka tape Anda, pilih node Slots.
2. Pilih pita yang dimuat, yang memiliki ikon hijau yang menunjukkan pita yang dimuat. Buka menu konteks (klik kanan) dan pilih Format, lalu pilih Berikutnya.
3. Pilih kumpulan media yang Anda buat, lalu pilih Berikutnya.
4. Untuk Deskripsi Sedang, pilih Gunakan kode batang, lalu pilih Berikutnya.
5. Untuk Options, pilih Force Operation, lalu pilih Finish.

Anda sekarang akan melihat perubahan slot yang Anda pilih dari status tidak ditetapkan (abu-abu) ke status pita yang disisipkan (hijau). Serangkaian pesan muncul untuk mengonfirmasi bahwa media Anda diinisialisasi.

Pada titik ini, Anda harus memiliki semuanya dikonfigurasi untuk mulai menggunakan pustaka pita virtual Anda dengan HPE Data Protector. Untuk memeriksa ulang apakah ini masalahnya, gunakan prosedur berikut.

Untuk memverifikasi bahwa pustaka rekaman Anda dikonfigurasi untuk digunakan

- Pilih Drive, lalu buka menu konteks (klik kanan) untuk drive Anda, dan pilih Pindai.

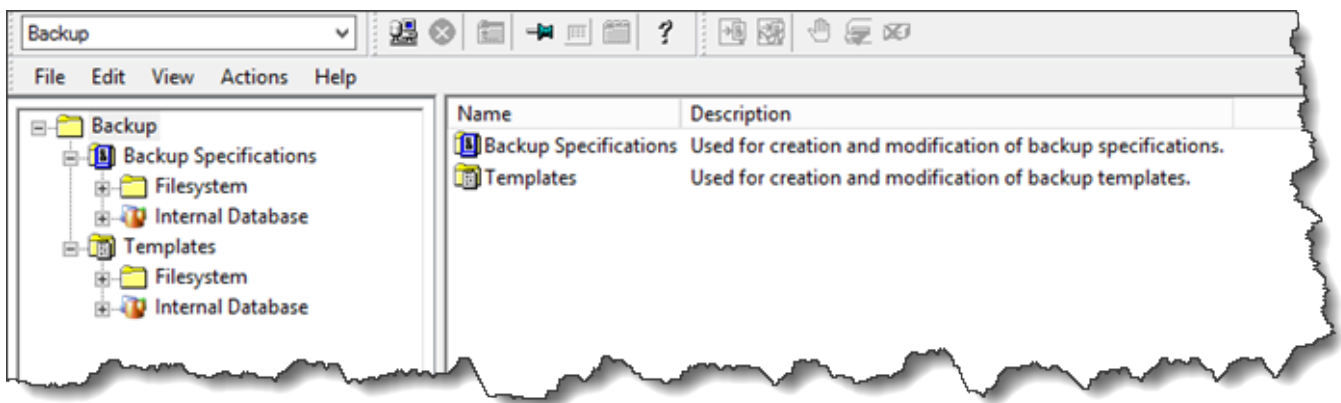
Jika konfigurasi Anda benar, pesan mengonfirmasi bahwa media Anda berhasil dipindai.

Mencadangkan Data ke Tape

Ketika kaset Anda telah dimuat ke kolam media, Anda dapat mencadangkan data ke mereka.

Untuk mencadangkan data ke kaset

1. Pilih rak Backup di kiri atas layar.



2. Buka menu konteks (klik kanan) untuk Filesystem, dan pilih Add Backup.
3. Pada layar Create New Backup, di bawah Filesystem, pilih Blank File System Backup, lalu pilih OK.
4. Pada simpul pohon yang menunjukkan sistem host Anda, pilih sistem file atau sistem file yang ingin Anda cadangkan, dan pilih Berikutnya untuk melanjutkan.
5. Buka simpul pohon untuk pustaka tape yang ingin Anda gunakan, buka menu konteks (klik kanan) untuk tape drive yang ingin Anda gunakan, lalu pilih Properties.
6. Pilih kumpulan media Anda, pilih OK, lalu pilih Berikutnya.
7. Untuk tiga layar berikutnya, terima pengaturan default dan pilih Berikutnya.
8. Pada Lakukan langkah penyelesaian di layar desain cadangan/templat Anda, pilih Simpan sebagai untuk menyimpan sesi ini. Di jendela pop-up, berikan nama cadangan dan tetapkan ke grup tempat Anda ingin menyimpan spesifikasi cadangan baru Anda.
9. Pilih Mulai Cadangan Interaktif.

Jika sistem host berisi sistem database, Anda dapat memilihnya sebagai sistem cadangan target Anda. Layar dan pilihannya mirip dengan cadangan sistem file yang baru saja dijelaskan.

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan gagal, dan tape drive di Pelindung Data ditandai sebagai Kotor. Pelindung Data juga menandai kualitas rekaman sebagai Buruk, dan mencegah penulisan ke kaset. Untuk terus membaca data dari kaset, Anda harus membersihkan drive dan memasang kembali rekaman itu. Untuk menyelesaikan pekerjaan pencadangan yang gagal, Anda harus mengirimkannya kembali pada rekaman baru.

Mengarsipkan Pita

Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka kaset ke penyimpanan offline. Sebelum Anda mengeluarkan dan mengarsipkan rekaman, Anda mungkin ingin memeriksa konten di dalamnya.

Untuk memeriksa konten rekaman sebelum mengarsipkannya

1. Pilih Slot dan kemudian pilih kaset yang ingin Anda periksa.
2. Pilih Objek dan periksa konten apa yang ada di rekaman itu.

Ketika Anda telah memilih kaset untuk diarsipkan, gunakan prosedur berikut.

Untuk mengeluarkan dan mengarsipkan kaset

1. Buka menu konteks (klik kanan) untuk rekaman itu, dan pilih Keluarkan.
2. Pada konsol Storage Gateway, pilih gateway Anda, lalu pilih VTL Tape Cartridges dan verifikasi status pita virtual yang Anda arsipkan.

Setelah rekaman dikeluarkan, itu akan secara otomatis diarsipkan dalam penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman ditampilkan sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Ketika pengarsipan selesai, rekaman

tidak lagi terdaftar di VTL tetapi diarsipkan dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive.

Memulihkan Data dari Tape

Memulihkan data yang diarsipkan adalah proses dua langkah.

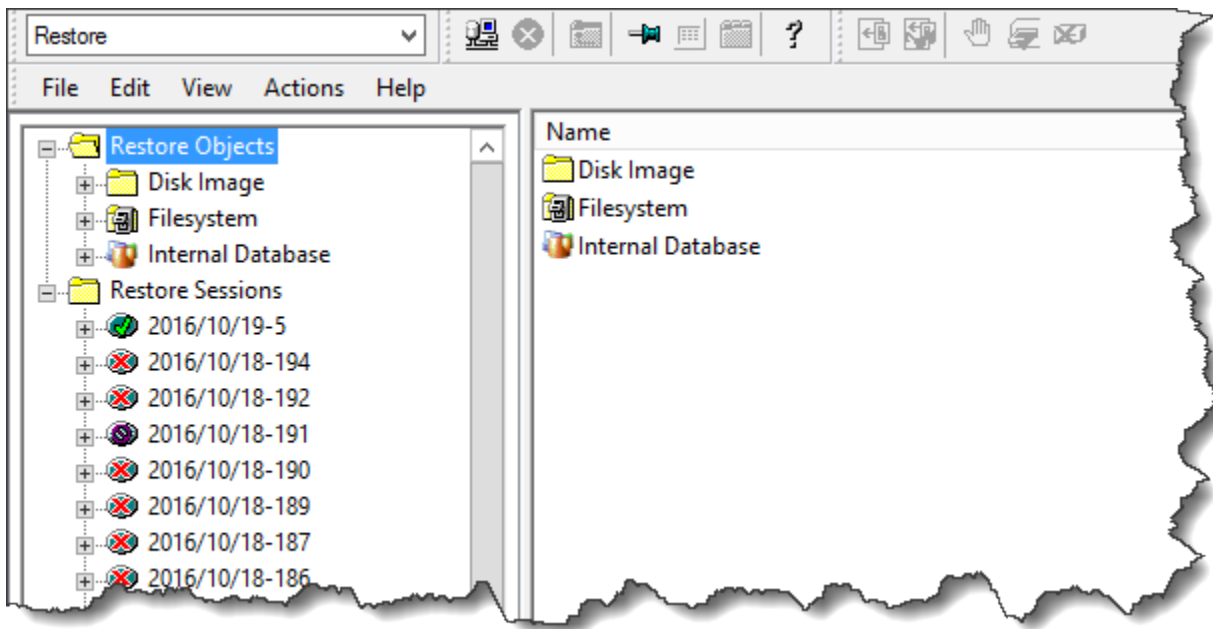
Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Gunakan HPE Data Protector untuk memulihkan data. Proses ini sama dengan memulihkan data dari kaset fisik.

Untuk memulihkan data dari kaset, gunakan prosedur berikut.

Untuk memulihkan data dari kaset

1. Pilih rak Restore di kiri atas layar.



2. Pilih sistem file atau sistem database yang ingin Anda pulihkan. Untuk cadangan yang ingin Anda pulihkan, pastikan kotak tersebut dipilih. Pilih Pulihkan.
3. Di jendela Mulai Pulihkan Sesi, pilih Media yang Dibutuhkan. Pilih Semua media, dan Anda akan melihat rekaman yang awalnya digunakan untuk cadangan. Pilih kaset itu, lalu pilih Tutup.

4. Di jendela Mulai Pulihkan Sesi, terima pengaturan default, pilih Berikutnya, lalu pilih Selesai.

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan Menggunakan Microsoft System Center Data Protection Manager

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Microsoft System Center 2012 R2 atau 2016 Data Protection Manager (DPM). Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi aplikasi cadangan DPM untuk Tape Gateway dan melakukan operasi pencadangan dan pemulihan.

Untuk informasi terperinci tentang cara menggunakan DPM, lihat [dokumentasi DPM di situs](#) web Microsoft System Center. Untuk informasi selengkapnya tentang aplikasi cadangan yang kompatibel, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Topik

- [Mengkonfigurasi DPM untuk Mengenali Perangkat VTL](#)
- [Mengimpor Tape ke DPM](#)
- [Menulis Data ke Tape di DPM](#)
- [Mengarsipkan Tape dengan Menggunakan DPM](#)
- [Memulihkan Data dari Tape yang Diarsipkan dalam DPM](#)

Mengkonfigurasi DPM untuk Mengenali Perangkat VTL

Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) ke klien Windows, Anda mengonfigurasi DPM untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows, lihat [Menghubungkan Perangkat VTL Anda](#)

Secara default, server DPM tidak mengenali perangkat Tape Gateway. Untuk mengonfigurasi server agar berfungsi dengan perangkat Tape Gateway, Anda melakukan tugas-tugas berikut:

1. Perbarui driver perangkat untuk perangkat VTL untuk mengeksposnya ke server DPM.
2. Memetakan perangkat VTL secara manual ke perpustakaan pita DPM.

Untuk memperbarui driver perangkat VTL

- Di Device Manager, perbarui driver untuk medium changer. Untuk petunjuk, lihat [Memperbarui Driver Perangkat untuk Pengubah Medium Anda](#).

Anda menggunakan DPM DriveMappingTool untuk memetakan tape drive Anda ke perpustakaan pita DPM.

Untuk memetakan tape drive ke pustaka pita server DPM

1. Buat setidaknya satu kaset untuk gateway Anda. Untuk informasi tentang cara melakukannya di konsol, lihat [Membuat Kaset](#).
2. Impor rekaman ke perpustakaan DPM. Untuk informasi tentang cara melakukannya, silakan lihat [Mengimpor Tape ke DPM](#).
3. Jika layanan DPMLA sedang berjalan, hentikan dengan membuka terminal perintah dan mengetik yang berikut pada baris perintah.

net stop DPMLA

4. Temukan file berikut di server DPM:%ProgramFiles%\System Center 2016 R2\DPM\DPM\Config\DPMLA.xml.

Note

Jika file ini ada, DPM akan DriveMappingTool menyimpannya. Jika Anda ingin menyimpan file asli Anda, buat salinan cadangan.

5. Buka terminal perintah, ubah direktori ke%ProgramFiles%\System Center 2016 R2\DPM\DPM\Bin, dan jalankan perintah berikut.

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

Output untuk perintah terlihat seperti berikut.

```

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

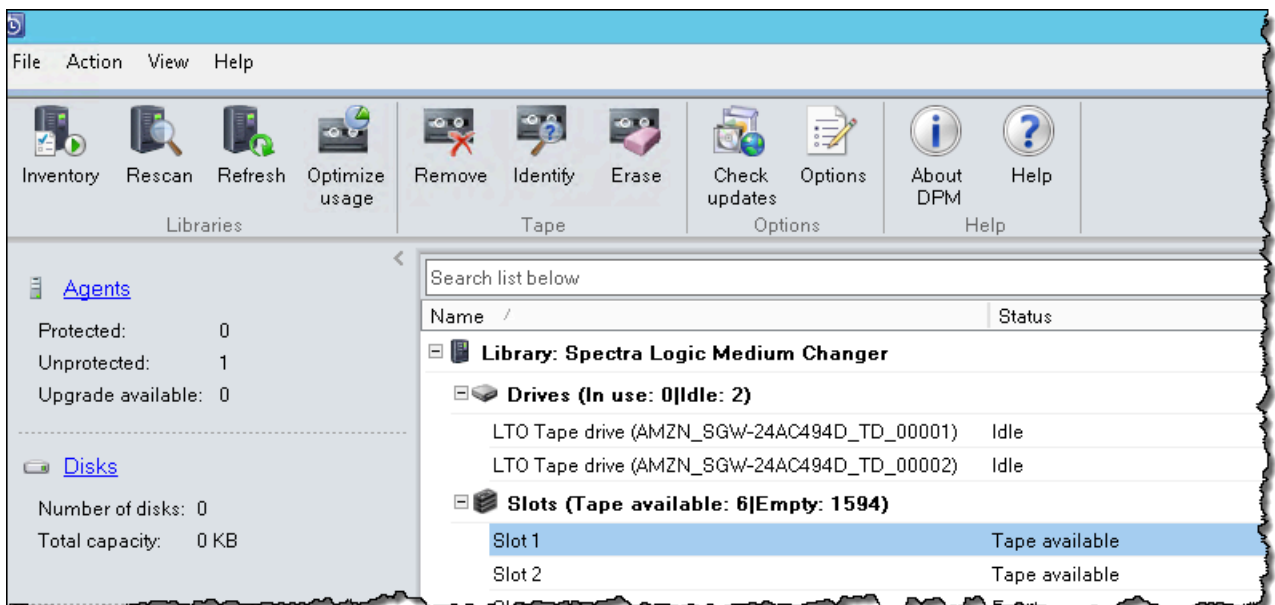
```

Mengimpor Tape ke DPM

Anda sekarang siap untuk mengimpor kaset dari Tape Gateway Anda ke perpustakaan aplikasi cadangan DPM.

Untuk mengimpor kaset ke pustaka aplikasi cadangan DPM

1. Di server DPM, buka Management Console, pilih Rescan, lalu pilih Refresh. Melakukan hal ini akan menampilkan medium changer dan tape drive Anda.



2. Buka menu konteks (klik kanan) untuk pengubah media di bagian Perpustakaan, lalu pilih Tambahkan pita (port I/E) untuk menambahkan rekaman ke daftar Slot.

Note

Proses menambahkan kaset bisa memakan waktu beberapa menit untuk diselesaikan.

Label kaset muncul sebagai Tidak Diketahui, dan rekaman itu tidak dapat digunakan. Agar rekaman itu dapat digunakan, Anda harus mengidentifikasinya.

3. Buka menu konteks (klik kanan) untuk rekaman yang ingin Anda identifikasi, lalu pilih Identifikasi rekaman yang tidak dikenal.

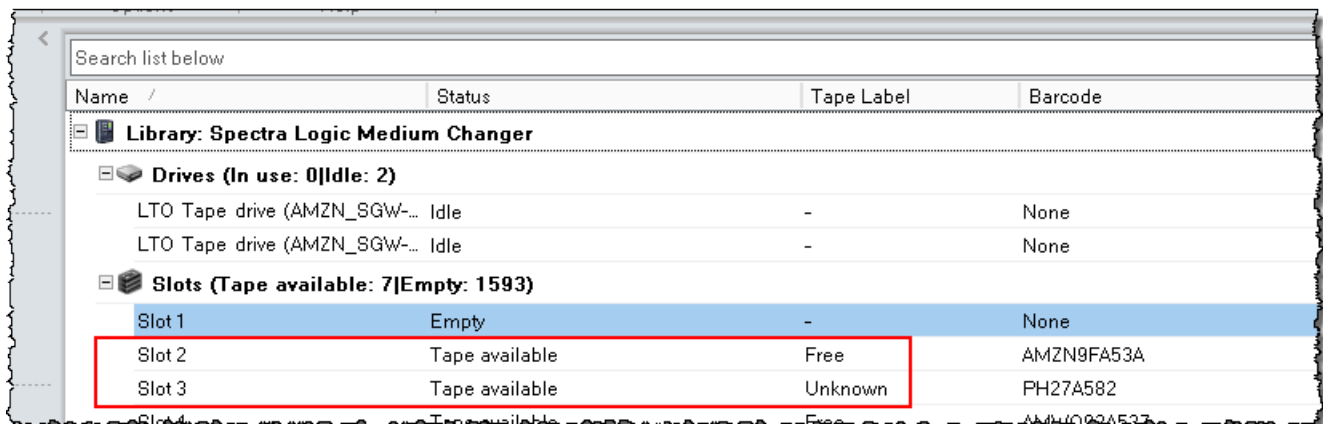
Note

Proses mengidentifikasi kaset dapat memakan waktu beberapa detik atau beberapa menit.

Jika kaset tidak menampilkan barcode dengan benar, Anda perlu mengubah driver media changer ke Sun/ Library. StorageTek Untuk informasi selengkapnya, lihat [Menampilkan Barcode untuk Kaset di Microsoft System Center DPM](#).

Saat identifikasi selesai, label pita berubah menjadi Gratis. Artinya, rekaman itu gratis untuk data yang akan ditulis untuk itu.

Pada tangkapan layar berikut, rekaman di slot 2 telah diidentifikasi dan bebas digunakan tetapi pita di slot 3 tidak.



Name /	Status	Tape Label	Barcode
Library: Spectra Logic Medium Changer			
Drives (In use: 0 Idle: 2)			
LTO Tape drive (AMZN_SGW-...	Idle	-	None
LTO Tape drive (AMZN_SGW-...	Idle	-	None
Slots (Tape available: 7 Empty: 1593)			
Slot 1	Empty	-	None
Slot 2	Tape available	Free	AMZN9FA53A
Slot 3	Tape available	Unknown	PH27A582
Slot 4	Tape available	Free	AMZN9FA537

Menulis Data ke Tape di DPM

Anda menulis data ke pita virtual Tape Gateway dengan menggunakan prosedur dan kebijakan perlindungan yang sama yang Anda lakukan dengan kaset fisik. Anda membuat grup perlindungan dan menambahkan data yang ingin Anda cadangkan, lalu mencadangkan data dengan membuat titik

pemulihan. Untuk informasi terperinci tentang cara menggunakan DPM, lihat [dokumentasi DPM di situs](#) web Microsoft System Center.

Secara default, kapasitas kaset adalah 30GB. Ketika Anda mencadangkan data yang lebih besar dari kapasitas tape, kesalahan I/O perangkat terjadi. Jika posisi di mana kesalahan terjadi lebih besar dari ukuran pita, Microsoft DPM memperlakukan kesalahan sebagai indikasi akhir pita. Jika posisi di mana kesalahan terjadi kurang dari ukuran rekaman, pekerjaan cadangan gagal. Untuk mengatasi masalah, ubah TapeSize nilai dalam entri registri agar sesuai dengan ukuran rekaman Anda. Untuk selengkapnya tentang cara melakukannya, lihat [ID Kesalahan: 30101](#) di Pusat Sistem Microsoft.

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan gagal. Untuk menyelesaikan pekerjaan pencadangan yang gagal, Anda harus mengirimkannya kembali.

Mengarsipkan Tape dengan Menggunakan DPM

Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka pita DPM ke penyimpanan offline. Anda memulai arsip rekaman dengan menghapus kaset dari slot menggunakan aplikasi cadangan Anda — yaitu, DPM.

Untuk mengarsipkan kaset di DPM

1. Buka menu konteks (klik kanan) untuk rekaman yang ingin Anda arsipkan, lalu pilih Hapus pita (port I/E).



2. Di kotak dialog yang muncul, pilih Ya. Melakukan hal ini mengeluarkan pita dari slot penyimpanan medium changer dan memindahkan pita ke salah satu slot I/E gateway. Ketika sebuah kaset dipindahkan ke slot I/E gateway, itu segera dikirim untuk pengarsipan.
3. Pada konsol Storage Gateway, pilih gateway Anda, lalu pilih VTL Tape Cartridges dan verifikasi status pita virtual yang Anda arsipkan.

Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman ditampilkan sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Saat pengarsipan selesai, rekaman itu tidak lagi tercantum dalam VTL.

Memulihkan Data dari Tape yang Diarsipkan dalam DPM

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan dari arsip ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Gunakan aplikasi cadangan DPM untuk memulihkan data. Anda melakukan ini dengan membuat titik pemulihan, seperti yang Anda lakukan saat memulihkan data dari kaset fisik. Untuk petunjuk, lihat [Memulihkan Data Komputer Klien](#) di situs web DPM.

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan NovaStor DataCenter Menggunakan/Jaringan

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan NovaStor DataCenter menggunakan/Jaringan versi 6.4 atau 7.1. Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi aplikasi pencadangan NovaStor DataCenter /Network versi 7.1 untuk Tape Gateway dan melakukan operasi pencadangan dan pemulihan. Untuk informasi rinci tentang cara NovaStor DataCenter menggunakan/Jaringan versi 7.1, lihat [NovaStor DataCenterDokumentasi/Jaringan](#).

NovaStor DataCenterMenyiapkan/Jaringan

Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) Anda ke klien Microsoft Windows Anda, Anda mengonfigurasi NovaStor perangkat lunak untuk mengenali perangkat

Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows Anda, lihat.

[Menghubungkan Perangkat VTL Anda](#)

NovaStor DataCenter/Jaringan membutuhkan driver dari produsen driver. Anda dapat menggunakan driver Windows, tetapi Anda harus terlebih dahulu menonaktifkan aplikasi cadangan lainnya.

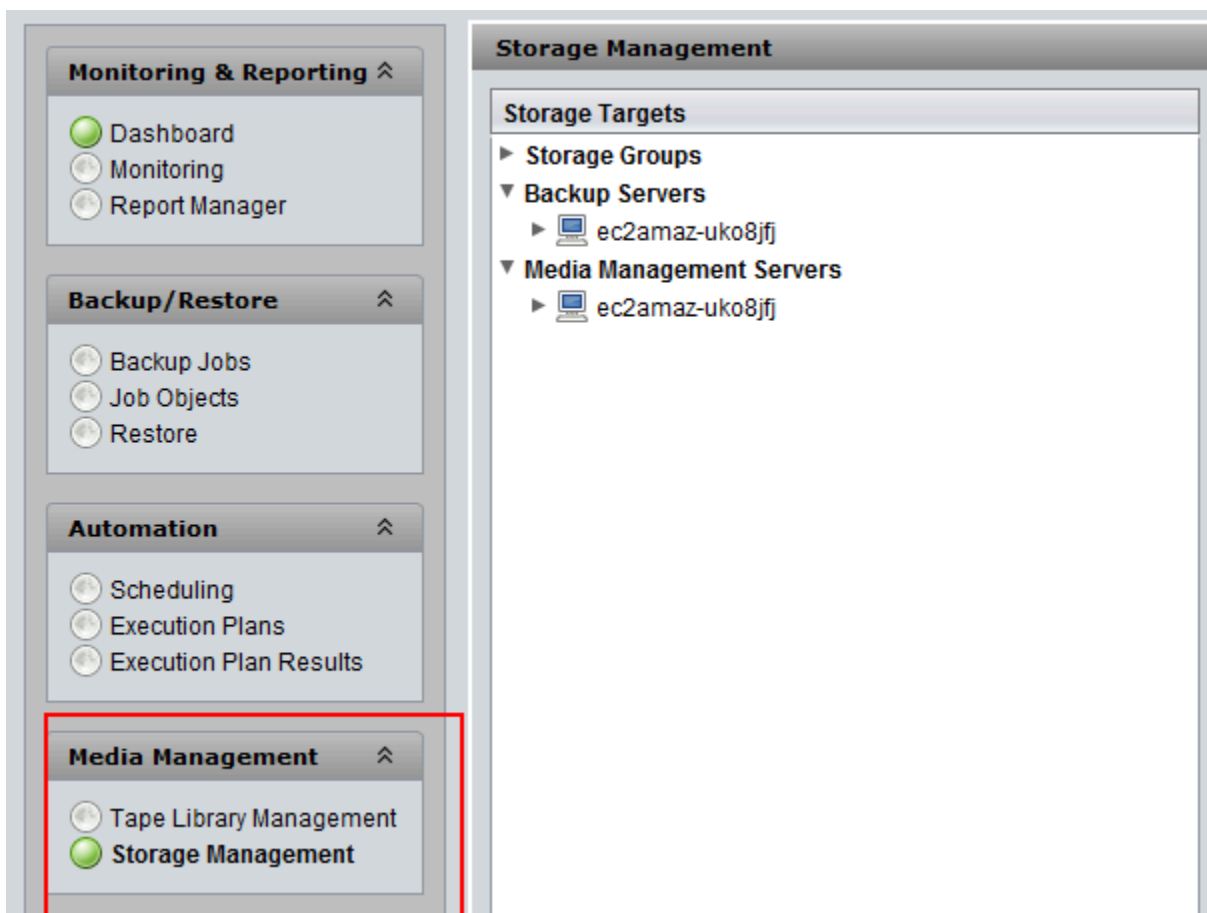
NovaStor DataCenterKonfigurasi/Jaringan untuk Bekerja dengan Perangkat VTL

Saat mengonfigurasi perangkat VTL agar berfungsi dengan NovaStor DataCenter /Network versi 6.4 atau 7.1, Anda mungkin melihat pesan kesalahan yang berbunyi. External Program did not exit correctly Masalah ini memerlukan solusi, yang perlu Anda lakukan sebelum melanjutkan.

Anda dapat mencegah masalah dengan membuat solusi sebelum Anda mulai mengonfigurasi perangkat VTL Anda. Untuk informasi tentang cara membuat solusi, lihat. [Menyelesaikan Kesalahan “Program Eksternal Tidak Keluar dengan Benar”](#)

Untuk NovaStor DataCenter mengkonfigurasi/Jaringan untuk bekerja dengan perangkat VTL

1. Di konsol NovaStor DataCenter /Network Admin, pilih Media Management, lalu pilih Storage Management.



- Di menu Target Penyimpanan, buka menu konteks (klik kanan) untuk Server Manajemen Media, pilih Baru, dan pilih OK untuk membuat dan mengisi node penyimpanan.

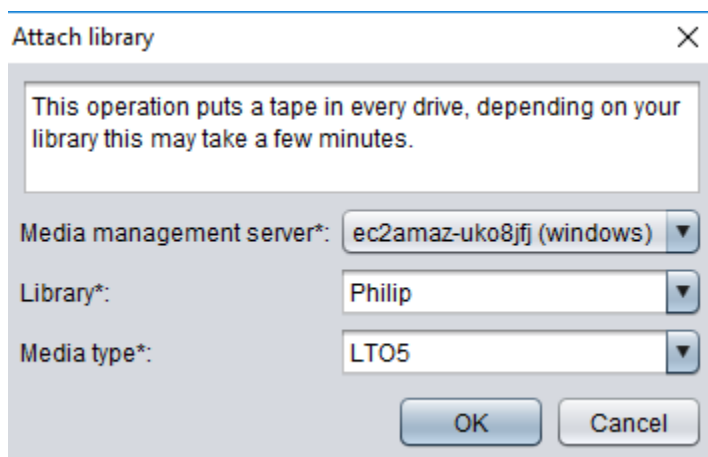
Jika Anda melihat pesan kesalahan yang mengatakan `External Program did not exit correctly`, selesaikan masalah sebelum melanjutkan. Masalah ini membutuhkan solusi.

Untuk informasi tentang cara mengatasi masalah ini, lihat [Menyelesaikan Kesalahan “Program Eksternal Tidak Keluar dengan Benar”](#).

⚠ Important

Kesalahan ini terjadi karena rentang penetapan elemen dari AWS Storage Gateway untuk drive penyimpanan dan tape drive melebihi jumlah yang diizinkan NovaStor DataCenter /Network.

- Buka menu konteks (klik kanan) untuk simpul penyimpanan yang dibuat, dan pilih Perpustakaan Baru.
- Pilih server pustaka dari daftar. Daftar pustaka diisi secara otomatis.
- Beri nama perpustakaan dan pilih OK.
- Pilih pustaka untuk menampilkan semua properti pustaka pita virtual Storage Gateway.
- Di menu Target Penyimpanan, perluas Server Cadangan, buka menu konteks (klik kanan) untuk server, dan pilih Lampirkan Perpustakaan.
- Di kotak dialog Lampirkan Perpustakaan yang muncul, pilih jenis media LTO5, lalu pilih OK.



- Perluas Server Cadangan untuk melihat pustaka pita virtual Storage Gateway dan partisi perpustakaan yang menampilkan semua tape drive yang dipasang.

Membuat Tape Pool

Sebuah tape pool secara dinamis dibuat dalam perangkat lunak NovaStor DataCenter /Network sehingga tidak berisi sejumlah media tetap. Sebuah kolam tape yang membutuhkan selotip mendapatkannya dari kolam awal. Kolam gores adalah reservoir kaset yang tersedia secara bebas untuk satu atau lebih kolam tape untuk digunakan. Sebuah tape pool kembali ke kolam awal media apa pun yang telah melebihi waktu retensi mereka dan yang tidak lagi diperlukan.

Membuat tape pool adalah tugas tiga langkah:

1. Anda membuat kolam goresan.
2. Anda menetapkan kaset ke kolam awal.
3. Anda membuat kolam tape.

Untuk membuat kolam goresan

1. Di menu navigasi kiri, pilih tab Scratch Pools.
2. Buka menu konteks (klik kanan) untuk Scratch Pools, dan pilih Create Scratch Pool.
3. Di kotak dialog Scratch Pools, beri nama scratch pool Anda, lalu pilih jenis media Anda.
4. Pilih Volume Label, dan buat tanda air rendah untuk kolam goresan. Ketika kolam goresan dikosongkan ke tanda air rendah, peringatan muncul.
5. Di kotak dialog peringatan yang muncul, pilih OK untuk membuat kumpulan awal.

Untuk menetapkan kaset ke kolam goresan

1. Di menu navigasi kiri, pilih Tape Library Management.
2. Pilih tab Perpustakaan untuk melihat inventaris perpustakaan Anda.
3. Pilih kaset yang ingin Anda tetapkan ke kolam goresan. Pastikan kaset diatur ke jenis media yang benar.
4. Buka menu konteks (klik kanan) untuk perpustakaan dan pilih Tambahkan ke Scratch Pool.

Anda sekarang memiliki kolam goresan penuh yang dapat Anda gunakan untuk kolam tape.

Untuk membuat kolam tape

1. Dari menu navigasi kiri, pilih Tape Library Management.

2. Buka menu konteks (klik kanan) untuk tab Media Pools dan pilih Create Media Pool.
3. Beri nama kumpulan media dan pilih Server Cadangan.
4. Pilih partisi perpustakaan untuk kumpulan media.
5. Pilih kolom awal tempat Anda ingin kolom untuk mendapatkan kasetnya.
6. Untuk Jadwal, pilih Tidak Terjadwal.

Mengkonfigurasi Impor Media dan Ekspor ke Kaset Arsip

NovaStor DataCenter/Jaringan dapat menggunakan slot impor/ekspor jika mereka adalah bagian dari media changer.

Untuk ekspor, NovaStor DataCenter /Network harus tahu kaset mana yang akan dikeluarkan secara fisik dari perpustakaan.

Untuk impor, NovaStor DataCenter /Network mengenali media tape yang diekspor di pustaka tape dan menawarkan untuk mengimpor semuanya, baik dari slot data atau slot ekspor. Tape Gateway Anda mengarsipkan kaset di penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive).

Untuk mengkonfigurasi impor dan ekspor media

1. Arahkan ke Manajemen Perpustakaan Tape, pilih server untuk Server Manajemen Media, lalu pilih Perpustakaan.
2. Pilih tab Lokasi Off-site.
3. Buka menu konteks (klik kanan) untuk area putih, dan pilih Tambahkan untuk membuka panel baru.
4. Di panel, ketik **S3 Glacier Flexible Retrieval** atau **S3 Glacier Deep Archive** dan tambahkan deskripsi opsional di kotak teks.

Mencadangkan Data ke Tape

Anda membuat pekerjaan cadangan dan menulis data ke rekaman virtual dengan menggunakan prosedur yang sama yang Anda lakukan dengan kaset fisik. Untuk informasi rinci tentang cara mencadangkan data menggunakan NovaStor perangkat lunak, lihat [NovaStor DataCenterDokumentasi/Jaringan](#).

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan gagal, dan rekaman itu akan menjadi tidak dapat ditulis. Anda dapat mengarsipkan rekaman atau terus membaca data darinya. Untuk menyelesaikan pekerjaan pencadangan yang gagal, Anda harus mengirimkannya kembali pada rekaman baru.

Mengarsipkan Pita

Saat Anda mengarsipkan kaset, Tape Gateway mengeluarkan selotip dari tape drive ke slot penyimpanan. Kemudian mengekspor rekaman dari slot ke arsip dengan menggunakan aplikasi cadangan Anda — yaitu, /Network. NovaStor DataCenter

Untuk mengarsipkan kaset

1. Di menu navigasi kiri, pilih Tape Library Management.
2. Pilih tab Perpustakaan untuk melihat inventaris perpustakaan.
3. Sorot kaset yang ingin Anda arsipkan, buka menu konteks (klik kanan) untuk kaset, dan pilih lokasi arsip di luar situs Anda.

Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman itu muncul sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Saat pengarsipan selesai, rekaman itu tidak lagi tercantum dalam VTL.

Di NovaStor DataCenter /Network, verifikasi bahwa rekaman itu tidak lagi ada di slot penyimpanan.

Di panel navigasi konsol Storage Gateway, pilih Tapes. Verifikasi bahwa status rekaman arsip Anda DIARSIPKAN.

Memulihkan Data dari Pita yang Diarsipkan dan Diambil

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan dari arsip ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).

- Gunakan perangkat lunak NovaStor DataCenter /Network untuk memulihkan data. Anda melakukan ini dengan menyegarkan slot surat dan memindahkan setiap kaset yang ingin Anda ambil ke slot kosong, seperti yang Anda lakukan saat memulihkan data dari kaset fisik. Untuk informasi tentang memulihkan data, lihat [Dokumentasi NovaStor DataCenter /Jaringan](#).

Menulis Beberapa Pekerjaan Backup ke Tape Drive pada Saat yang Sama

Dalam NovaStor perangkat lunak, Anda dapat menulis beberapa pekerjaan ke tape drive secara bersamaan menggunakan fitur multiplexing. Fitur ini tersedia ketika multiplexer tersedia untuk kolam media. Untuk informasi tentang cara menggunakan multiplexing, lihat [NovaStor DataCenterDokumentasi/Jaringan](#).

Menyelesaikan Kesalahan “Program Eksternal Tidak Keluar dengan Benar”

Saat mengonfigurasi perangkat VTL agar berfungsi dengan NovaStor DataCenter /Network versi 6.4 atau 7.1, Anda mungkin melihat pesan kesalahan yang berbunyi. `External Program did not exit correctly` Kesalahan ini terjadi karena rentang penetapan elemen dari Storage Gateway untuk drive penyimpanan dan tape drive melebihi jumlah yang diizinkan NovaStor DataCenter / Network.

Storage Gateway mengembalikan 3200 slot penyimpanan dan impor/ekspor, yang lebih dari batas 2400 yang diizinkan /Network. NovaStor DataCenter Untuk mengatasi masalah ini, Anda menambahkan file konfigurasi yang mengaktifkan NovaStor perangkat lunak untuk membatasi jumlah slot penyimpanan dan impor/ekspor dan mengkonfigurasi rentang penetapan elemen.

Untuk menerapkan solusi untuk kesalahan “program eksternal tidak keluar dengan benar”

- Arahkan ke folder Tape di komputer tempat Anda menginstal perangkat NovaStor lunak.
- Di folder Tape, buat file teks dan beri nama `hijacc.ini`.
- Salin konten berikut, tempel ke `hijacc.ini` file, dan simpan file.

```
port:12001
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
```



```
1 Configuration
2 Status Handler
3 Status Import/Export
4 Status Drive
5 Status Slot
6 Mount Medium
7 Unmount Medium
8 Find Address by Tag

9 Reset Stacker
11 Move Element
88 Inventory
99 Exit

What ([#,#[,#]])? 11
Source Address? 30000
Destination Address? 20000

1 Configuration
2 Status Handler
3 Status Import/Export
4 Status Drive
5 Status Slot
6 Mount Medium
7 Unmount Medium
8 Find Address by Tag
9 Reset Stacker
```

6. Lampirkan perpustakaan ke server cadangan.
7. Dalam perangkat NovaStor lunak, impor semua kaset dari slot impor/ekspor ke perpustakaan.

Menguji Pengaturan Anda dengan Menggunakan Quest NetVault Backup

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan versi Cadangan Quest (sebelumnya Dell) berikut: NetVault

- NetVault Cadangan Quest 12.4
- NetVault Cadangan Quest 13.x

Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi aplikasi Quest NetVault Backup untuk Tape Gateway dan melakukan operasi pencadangan dan pemulihan.

Untuk informasi rinci tentang cara menggunakan aplikasi Quest NetVault Backup, lihat Quest NetVault Backup — Panduan Administrasi. Untuk informasi selengkapnya tentang aplikasi cadangan yang kompatibel, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Topik

- [Mengkonfigurasi NetVault Cadangan Quest untuk Bekerja dengan Perangkat VTL](#)
- [Mencadangkan Data ke Tape di Cadangan Quest NetVault](#)
- [Mengarsipkan Tape dengan Menggunakan Cadangan Quest NetVault](#)
- [Memulihkan Data dari Tape yang Diarsipkan di Cadangan Quest NetVault](#)

Mengkonfigurasi NetVault Cadangan Quest untuk Bekerja dengan Perangkat VTL

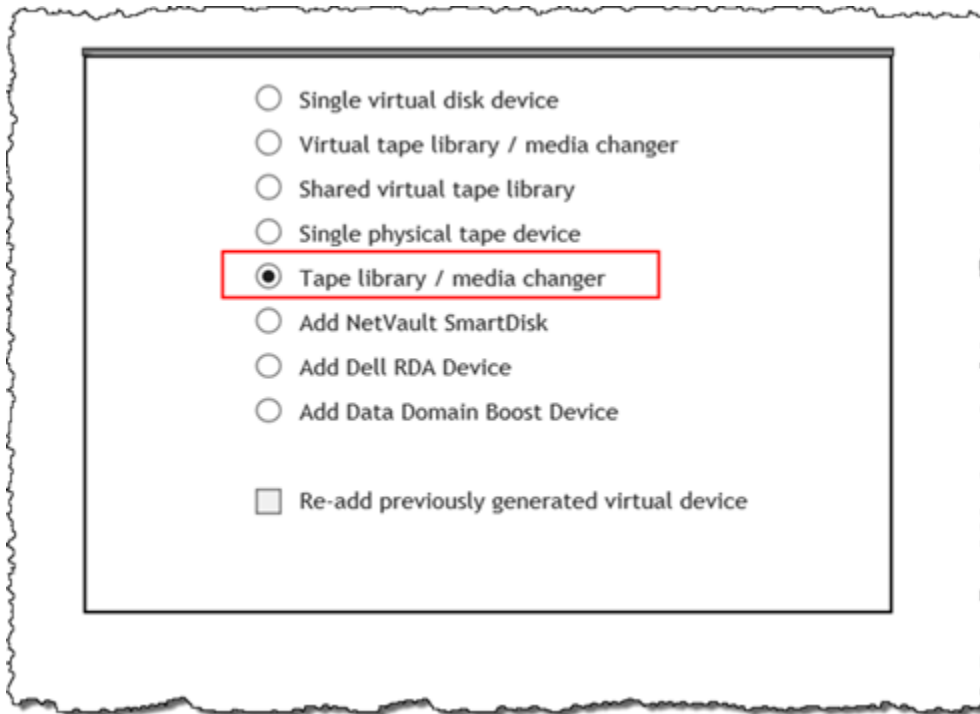
Setelah Anda menghubungkan perangkat virtual tape library (VTL) ke klien Windows, Anda mengonfigurasi Quest NetVault Backup untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows, lihat [Menghubungkan Perangkat VTL Anda](#)

Aplikasi Quest NetVault Backup tidak secara otomatis mengenali perangkat Tape Gateway. Anda harus menambahkan perangkat secara manual untuk mengeksposnya ke aplikasi Quest NetVault Backup dan kemudian menemukan perangkat VTL.

Menambahkan Perangkat VTL

Untuk menambahkan perangkat VTL

1. Di Quest NetVault Backup, pilih Kelola Perangkat di tab Konfigurasi.
2. Pada halaman Kelola Perangkat, pilih Tambah Perangkat.
3. Di Add Storage Wizard, pilih Tape library /media changer, lalu pilih Berikutnya.



4. Pada halaman berikutnya, pilih mesin klien yang secara fisik terpasang ke perpustakaan dan pilih Berikutnya untuk memindai perangkat.
5. Jika perangkat ditemukan, mereka ditampilkan. Dalam hal ini, pengubah media Anda ditampilkan di kotak perangkat.
6. Pilih medium changer Anda dan pilih Berikutnya. Informasi terperinci tentang perangkat ditampilkan di wizard.
7. Pada halaman Tambahkan Kaset ke Teluk, pilih Pindai Perangkat, pilih mesin klien Anda, lalu pilih Berikutnya.

Semua drive Anda ditampilkan di halaman. Quest NetVault Backup menampilkan 10 bay yang dapat Anda tambahkan drive Anda. Teluk ditampilkan satu per satu.

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

1 - 5 of 5 items

- Pilih drive yang ingin Anda tambahkan ke bay yang ditampilkan, lalu pilih Berikutnya.

⚠ Important

Saat Anda menambahkan drive ke teluk, nomor drive dan bay harus cocok. Misalnya, jika bay 1 ditampilkan, Anda harus menambahkan drive 1. Jika drive tidak terhubung, biarkan ruang yang cocok kosong.

- Ketika mesin klien Anda muncul, pilih, dan kemudian pilih Berikutnya. Mesin klien dapat muncul beberapa kali.
- Saat drive ditampilkan, ulangi langkah 7 hingga 9 untuk menambahkan semua drive ke teluk.
- Di tab Konfigurasi, pilih Kelola perangkat dan pada halaman Kelola Perangkat, perluas pengubah media Anda untuk melihat perangkat yang Anda tambahkan.

Mencadangkan Data ke Tape di Cadangan Quest NetVault

Anda membuat pekerjaan cadangan dan menulis data ke rekaman virtual dengan menggunakan prosedur yang sama yang Anda lakukan dengan kaset fisik. Untuk informasi rinci tentang cara mencadangkan data, lihat [NetVault Backup Quest - Panduan Administrasi](#).

Note

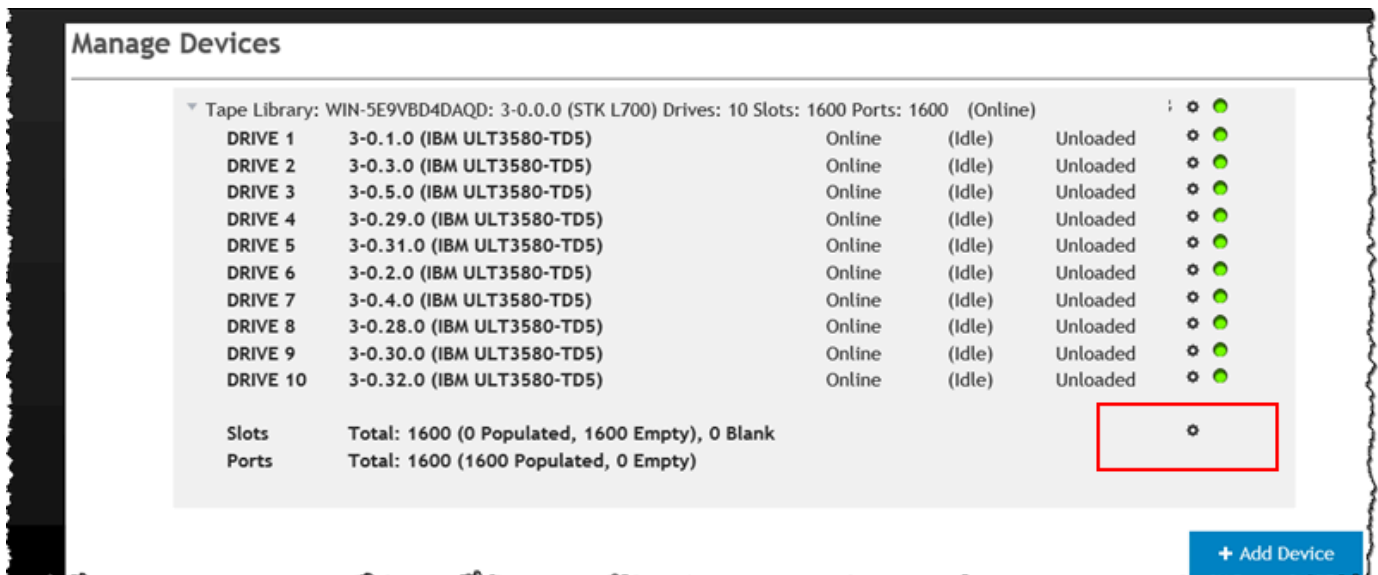
Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan gagal. Untuk menyelesaikan pekerjaan pencadangan yang gagal, Anda harus mengirimkannya kembali.

Mengarsipkan Tape dengan Menggunakan Cadangan Quest NetVault

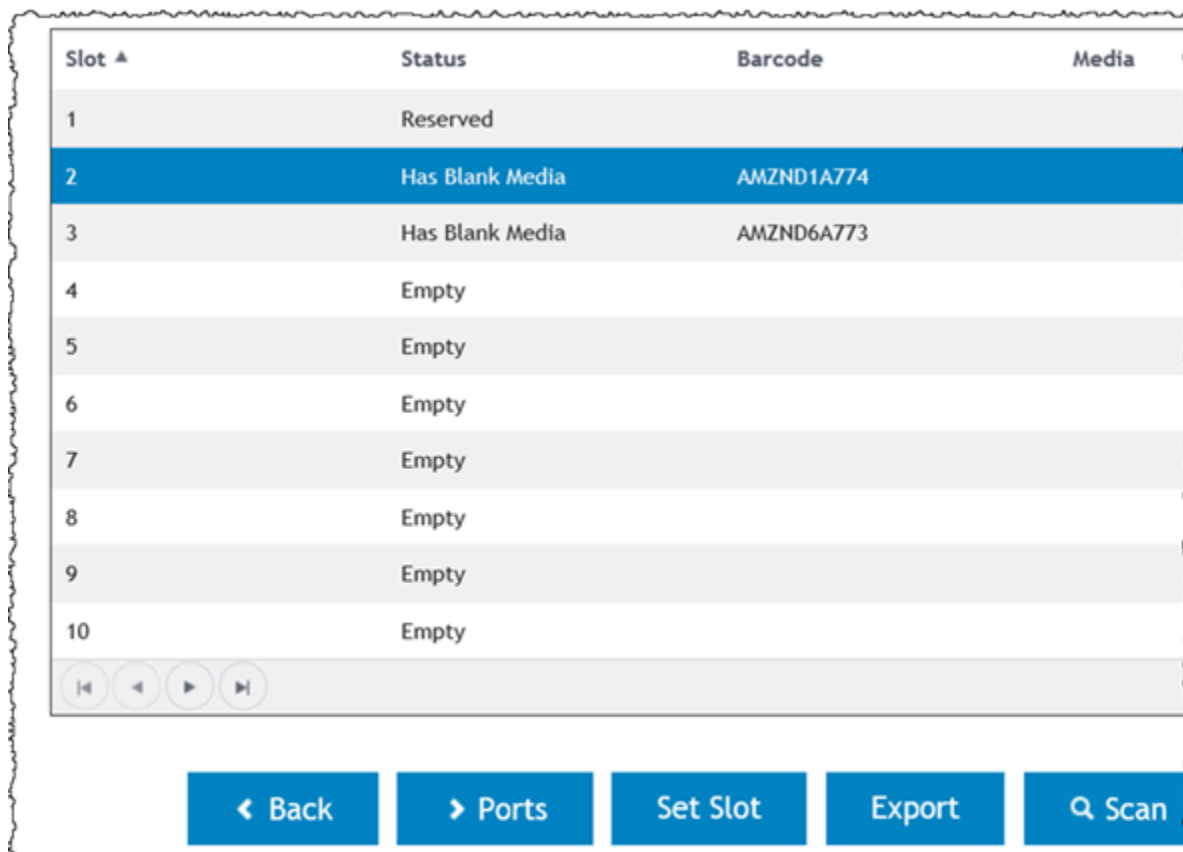
Saat Anda mengarsipkan kaset, Tape Gateway mengeluarkan selotip dari tape drive ke slot penyimpanan. Kemudian mengekspor rekaman dari slot ke arsip dengan menggunakan aplikasi cadangan Anda — yaitu, Quest Backup. NetVault

Untuk mengarsipkan rekaman di Quest NetVault Backup

1. Di tab Quest NetVault Backup Configuration, pilih dan perluas medium changer Anda untuk melihat kaset Anda.
2. Pada baris Slot, pilih ikon pengaturan untuk membuka Browser Slot untuk pengubah media.



3. Di slot, cari rekaman yang ingin Anda arsipkan, pilih, lalu pilih Ekspor.



Slot ▲	Status	Barcode	Media
1	Reserved		
2	Has Blank Media	AMZND1A774	
3	Has Blank Media	AMZND6A773	
4	Empty		
5	Empty		
6	Empty		
7	Empty		
8	Empty		
9	Empty		
10	Empty		

Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman itu muncul sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Saat pengarsipan selesai, rekaman itu tidak lagi tercantum dalam VTL.

Dalam perangkat lunak Quest NetVault Backup, verifikasi bahwa rekaman itu tidak lagi ada di slot penyimpanan.

Di panel navigasi konsol Storage Gateway, pilih Tapes. Verifikasi bahwa status rekaman arsip Anda DIARSIPKAN.

Memulihkan Data dari Tape yang Diarsipkan di Cadangan Quest NetVault

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan dari arsip ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).

- Gunakan aplikasi Quest NetVault Backup untuk memulihkan data. Anda melakukan ini dengan membuat memulihkan file folder, seperti yang Anda lakukan saat memulihkan data dari kaset fisik. Untuk petunjuk cara membuat pekerjaan pemulihan, lihat [NetVault Cadangan Quest - Panduan Administrasi](#).

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan Menggunakan Cadangan & Replikasi Veeam

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Veeam Backup & Replication 11A. Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi perangkat lunak Cadangan & Replikasi Veeam untuk Tape Gateway dan melakukan operasi pencadangan dan pemulihan. Untuk informasi rinci tentang cara menggunakan perangkat lunak Veeam, lihat [Tentang Veeam Backup & Replication](#) di Pusat Bantuan Veeam. Untuk informasi selengkapnya tentang aplikasi cadangan yang kompatibel, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Topik

- [Mengkonfigurasi Veeam untuk Bekerja dengan Perangkat VTL](#)
- [Mengimpor Tape ke Veeam](#)
- [Mencadangkan Data ke Tape di Veeam](#)
- [Mengarsipkan Tape dengan Menggunakan Veeam](#)
- [Memulihkan Data dari Tape yang Diarsipkan di Veeam](#)

Mengkonfigurasi Veeam untuk Bekerja dengan Perangkat VTL

Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) Anda ke klien Windows, Anda mengonfigurasi Veeam Backup & Replication untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows, lihat. [Menghubungkan Perangkat VTL Anda](#)

Memperbarui Driver Perangkat VTL

Untuk mengonfigurasi perangkat lunak agar berfungsi dengan perangkat Tape Gateway, Anda memperbarui driver perangkat untuk perangkat VTL untuk mengeksposnya ke perangkat lunak

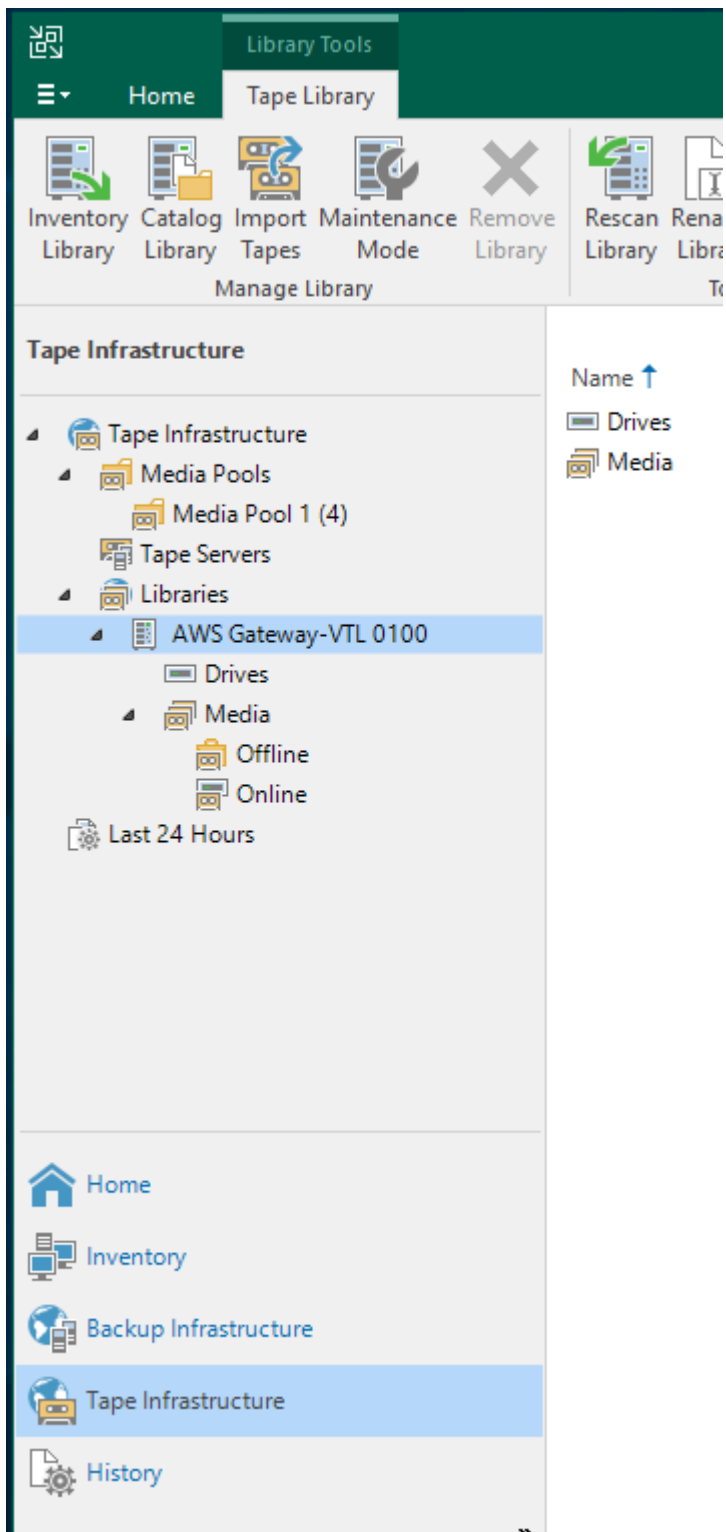
Veeam dan kemudian menemukan perangkat VTL. Di Device Manager, perbarui driver untuk medium changer. Untuk petunjuk, lihat [Memperbarui Driver Perangkat untuk Pengubah Medium Anda](#).

Menemukan Perangkat VTL

Anda harus menggunakan perintah SCSI asli alih-alih driver Windows untuk menemukan pustaka rekaman Anda jika pengubah media Anda tidak diketahui. Untuk petunjuk terperinci, lihat [Pustaka Tape](#).

Untuk menemukan perangkat VTL

1. Dalam perangkat lunak Veeam, pilih Tape Infrastructure. Ketika Tape Gateway terhubung, kaset virtual tercantum di tab Tape Infrastructure.



2. Perluas pohon Tape untuk melihat tape drive dan medium changer Anda.
3. Perluas pohon pengubah sedang. Jika tape drive Anda dipetakan ke medium changer, drive akan muncul di bawah Drive. Jika tidak, pustaka kaset dan tape drive Anda muncul sebagai perangkat terpisah.

Jika drive tidak dipetakan secara otomatis, ikuti [instruksi di situs web Veeam](#) untuk memetakan drive.

Mengimpor Tape ke Veeam

Anda sekarang siap untuk mengimpor kaset dari Tape Gateway Anda ke perpustakaan aplikasi cadangan Veeam.

Untuk mengimpor rekaman ke perpustakaan Veeam

1. Buka menu konteks (klik kanan) untuk pengubah medium, dan pilih Impor untuk mengimpor kaset ke slot I/E.
2. Buka menu konteks (klik kanan) untuk pengisi daya medium, dan pilih Perpustakaan Inventaris untuk mengidentifikasi kaset yang tidak dikenal. Saat Anda memuat kaset virtual baru ke dalam tape drive untuk pertama kalinya, rekaman itu tidak dikenali oleh aplikasi cadangan Veeam. Untuk mengidentifikasi rekaman yang tidak dikenal, Anda menginventarisasi kaset di perpustakaan kaset.

Mencadangkan Data ke Tape di Veeam

Mendukung data ke kaset adalah proses dua langkah:

1. Anda membuat kolam media dan menambahkan rekaman ke kolam media.
2. Anda menulis data ke rekaman itu.

Anda membuat kumpulan media dan menulis data ke rekaman virtual dengan menggunakan prosedur yang sama yang Anda lakukan dengan kaset fisik. Untuk informasi terperinci tentang cara mencadangkan data, lihat [Memulai dengan Kaset di Pusat Bantuan Veeam](#).

Note

Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan gagal. Untuk menyelesaikan pekerjaan pencadangan yang gagal, Anda harus mengirimkannya kembali.

Mengarsipkan Tape dengan Menggunakan Veeam

Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka pita Veeam ke penyimpanan offline. Anda memulai arsip rekaman dengan mengeluarkan dari tape drive ke slot penyimpanan dan kemudian mengekspor kaset dari slot ke arsip dengan menggunakan aplikasi cadangan Anda — yaitu, perangkat lunak Veeam.

Untuk mengarsipkan kaset di perpustakaan Veeam

1. Pilih Tape Infrastructure, dan pilih kumpulan media yang berisi rekaman yang ingin Anda arsipkan.

The screenshot shows the AWS Management Console interface for Tape Gateway. The top navigation bar includes 'Home' and 'Tape Media'. The 'Media Tools' ribbon contains several action groups: 'Import Media' (Inventory, Catalog), 'Media Actions' (Restore Content, Verify, Copy), 'Manage Media' (Move to, Export, Eject), 'Erase Media' (Erase, Mark as Free, Remove), and 'Protect' (Protect). The left sidebar shows the 'Tape Infrastructure' tree view, with 'Online' media selected. The main content area displays a table of tapes:

Name ↑	Location	Expires
Tape 2	Slot 2	Not def
Tape 3	Slot 3	Not def
Tape 4	Slot 4	Not def

A context menu is open over 'Tape 4', listing actions: Inventory, Catalog, Restore content..., Copy..., Verify, Export (highlighted), Eject, Move to, Erase, Mark as free, Protect, and Properties.

2. Buka menu konteks (klik kanan) untuk rekaman yang ingin Anda arsipkan, lalu pilih Eject Tape.
3. Untuk Ejecting tape, pilih Tutup. Lokasi rekaman berubah dari tape drive ke slot.
4. Buka menu konteks (klik kanan) untuk rekaman itu lagi, lalu pilih Ekspor. Status rekaman berubah dari Tape drive ke Offline.

5. Untuk Mengekspor kaset, pilih Tutup. Lokasi rekaman berubah dari Slot ke Offline.
6. Pada konsol Storage Gateway, pilih gateway Anda, lalu pilih VTL Tape Cartridges dan verifikasi status pita virtual yang Anda arsipkan.

Proses pengarsipan dapat memakan waktu untuk diselesaikan. Status awal rekaman itu muncul sebagai IN TRANSIT TO VTS. Saat pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Ketika pengarsipan selesai, rekaman tidak lagi terdaftar di VTL tetapi diarsipkan dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive.

Memulihkan Data dari Tape yang Diarsipkan di Veeam

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan dari arsip ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Gunakan perangkat lunak Veeam untuk memulihkan data. Anda melakukan ini dengan membuat memulihkan file folder, seperti yang Anda lakukan saat memulihkan data dari kaset fisik. Untuk petunjuk, lihat [Memulihkan File dari Tape](#) di Pusat Bantuan Veeam.

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan Menggunakan Veritas Backup Exec

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Veritas Backup Exec. Dalam topik ini, Anda dapat menemukan dokumentasi dasar yang diperlukan untuk melakukan operasi pencadangan dan pemulihan menggunakan versi Backup Exec berikut:

- Eksekutif Cadangan Veritas 2014
- Eksekutif Cadangan Veritas 15
- Eksekutif Cadangan Veritas 16
- Exec Cadangan Veritas 20.x
- Exec Cadangan Veritas 22.x

Prosedur untuk menggunakan versi Backup Exec ini dengan Tape Gateway adalah sama. Lihat [situs web dukungan Veritas](#) untuk informasi terperinci tentang cara menggunakan Backup Exec, termasuk cara membuat cadangan aman dengan Backup Exec, daftar kompatibilitas perangkat lunak dan perangkat keras, dan panduan administrator untuk Backup Exec.

Untuk informasi selengkapnya tentang aplikasi cadangan yang didukung, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Topik

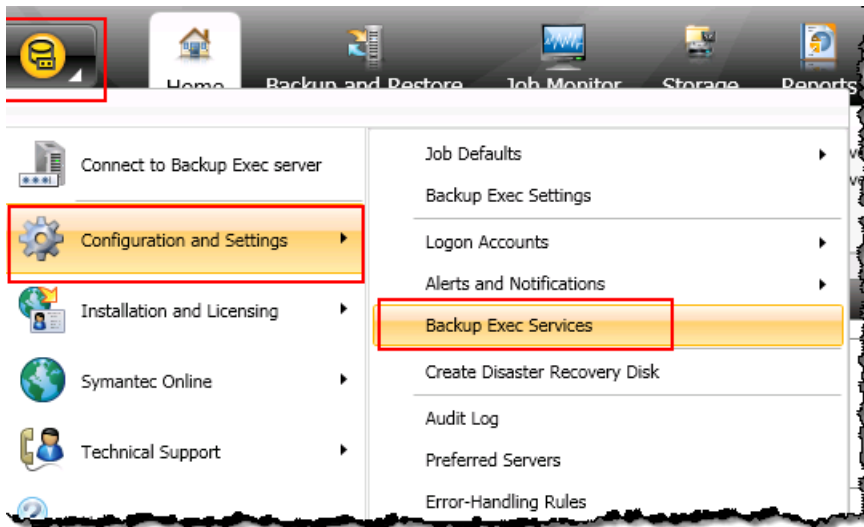
- [Mengkonfigurasi Penyimpanan di Backup Exec](#)
- [Mengimpor Tape di Backup Exec](#)
- [Menulis Data ke Tape di Backup Exec](#)
- [Mengarsipkan Tape Menggunakan Backup Exec](#)
- [Memulihkan Data dari Tape yang Diarsipkan di Backup Exec](#)
- [Menonaktifkan Tape Drive di Backup Exec](#)

Mengkonfigurasi Penyimpanan di Backup Exec

Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) ke klien Windows, Anda mengonfigurasi penyimpanan Backup Exec untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows, lihat [Menghubungkan Perangkat VTL Anda](#)

Untuk mengkonfigurasi penyimpanan

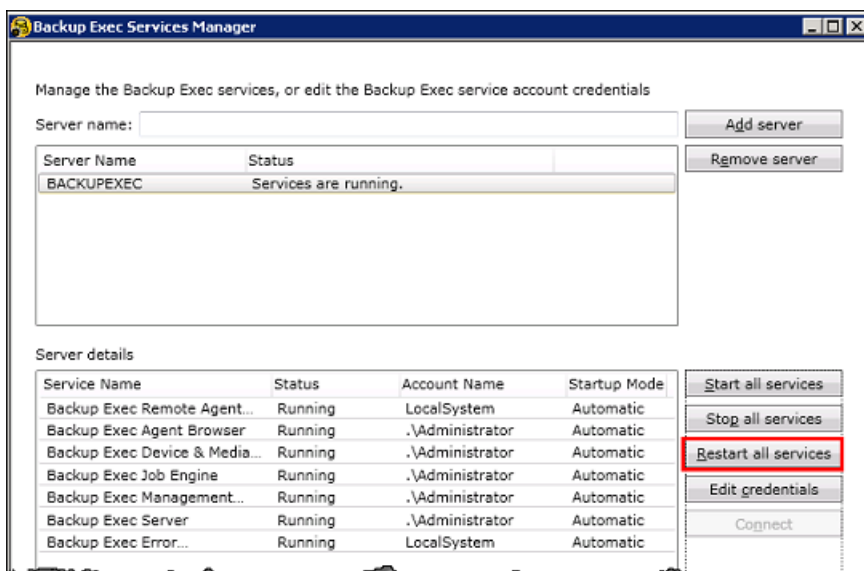
1. Mulai perangkat lunak Backup Exec, lalu pilih ikon kuning di sudut kiri atas pada bilah alat.
2. Pilih Konfigurasi dan Pengaturan, lalu pilih Backup Exec Services untuk membuka Backup Exec Service Manager.



3. Pilih Mulai Ulang Semua Layanan. Backup Exec kemudian mengenali perangkat VTL (yaitu, medium changer dan tape drive). Proses restart mungkin memakan waktu beberapa menit.

Note

Tape Gateway menyediakan 10 tape drive. Namun, perjanjian lisensi Backup Exec Anda mungkin memerlukan aplikasi cadangan Anda untuk bekerja dengan kurang dari 10 tape drive. Dalam hal ini, Anda harus menonaktifkan tape drive di perpustakaan robot Backup Exec untuk hanya menyisakan jumlah tape drive yang diizinkan oleh perjanjian lisensi Anda yang digerakkan. Untuk petunjuk, lihat [Menonaktifkan Tape Drive di Backup Exec](#).



4. Setelah restart selesai, tutup Backup Exec Service Manager.

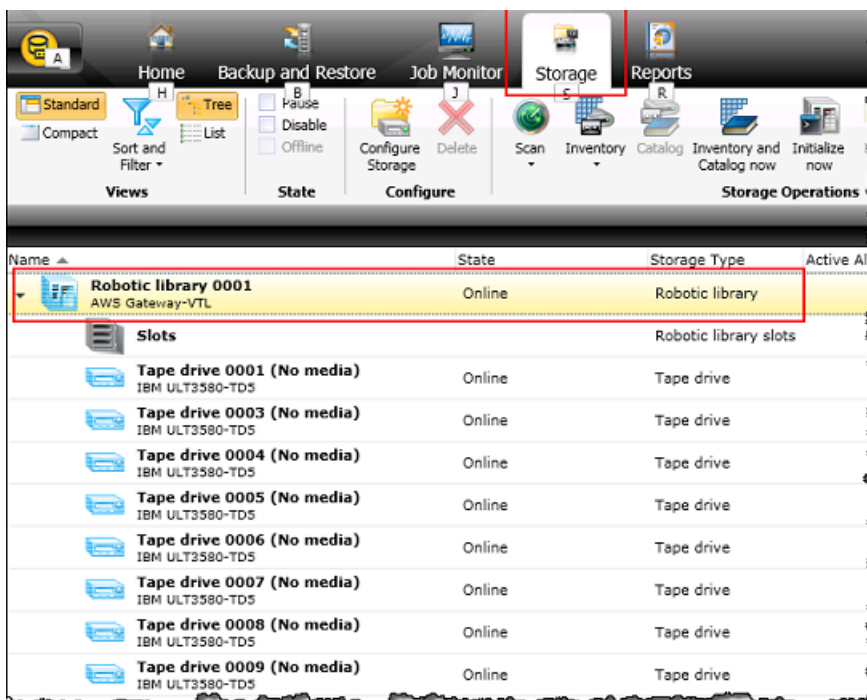
Mengimpor Tape di Backup Exec

Anda sekarang siap untuk mengimpor kaset dari gateway Anda ke dalam slot.

1. Pilih tab Penyimpanan, lalu perluas pohon perpustakaan Robotik untuk menampilkan perangkat VTL.

⚠ Important

Perangkat lunak Veritas Backup Exec membutuhkan tipe medium changer Tape Gateway. Jika tipe medium changer yang tercantum di bawah perpustakaan Robotik bukan Tape Gateway, Anda harus mengubahnya sebelum mengonfigurasi penyimpanan di aplikasi cadangan. Untuk informasi tentang cara memilih jenis medium changer yang berbeda, lihat [Memilih Medium Changer Setelah Aktivasi Gateway](#).



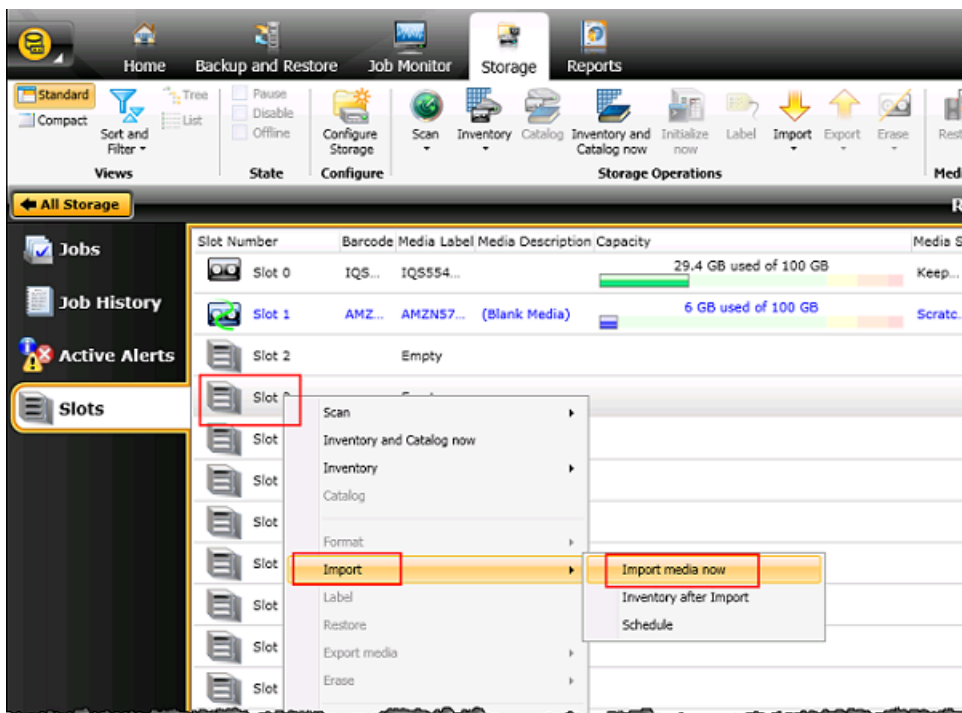
2. Pilih ikon Slots untuk menampilkan semua slot.

Note

Saat Anda mengimpor kaset ke perpustakaan robot, kaset disimpan dalam slot, bukan tape drive. Oleh karena itu, tape drive mungkin memiliki pesan yang menunjukkan tidak ada media di drive (Tidak ada media). Saat Anda memulai pekerjaan pencadangan atau pemulihan, kaset dipindahkan ke tape drive.

Anda harus memiliki kaset yang tersedia di perpustakaan pita gateway Anda untuk mengimpor kaset ke slot penyimpanan. Untuk petunjuk tentang cara membuat kaset, lihat [Menambahkan Kaset Virtual](#).

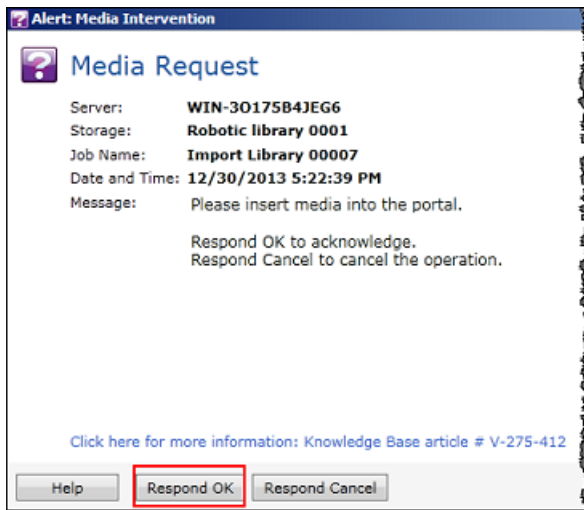
3. Buka menu konteks (klik kanan) untuk slot kosong, pilih Impor, lalu pilih Impor media sekarang. Dalam tangkapan layar berikut, nomor slot 3 kosong. Anda dapat memilih lebih dari satu slot dan mengimpor beberapa kaset dalam satu operasi impor.



4. Di jendela Permintaan Media yang muncul, pilih Lihat detail.



5. Di jendela Action Alert: Media Intervention, pilih Respon OK untuk memasukkan media ke dalam slot.



Rekaman itu muncul di slot yang Anda pilih.

Note

Kaset yang diimpor termasuk kaset kosong dan kaset yang telah diambil dari arsip ke gateway.

Menulis Data ke Tape di Backup Exec

Anda menulis data ke pita virtual Tape Gateway dengan menggunakan prosedur dan kebijakan cadangan yang sama yang Anda lakukan dengan kaset fisik. Untuk informasi rinci, lihat Backup Exec Administrative Guide di bagian dokumentasi di perangkat lunak Backup Exec.

Note

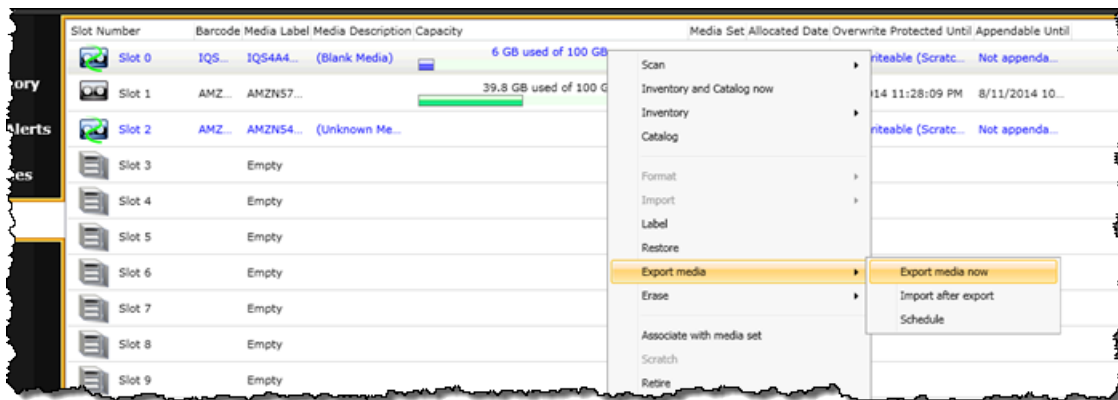
Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan mungkin gagal. Jika pekerjaan pencadangan gagal, status rekaman di Veritas Backup Exec berubah menjadi Tidak Dapat Ditambahkan. Anda dapat mengarsipkan rekaman atau terus membaca data darinya. Untuk menyelesaikan pekerjaan pencadangan yang gagal, Anda harus mengirimkannya kembali pada rekaman baru.

Mengarsipkan Tape Menggunakan Backup Exec

Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka pita virtual (VTL) gateway Anda ke penyimpanan offline. Anda memulai arsip rekaman dengan mengekspor rekaman menggunakan perangkat lunak Backup Exec Anda.

Untuk mengarsipkan rekaman Anda

1. Pilih menu Penyimpanan, pilih Slot, buka menu konteks (klik kanan) untuk slot tempat Anda ingin mengekspor rekaman, pilih Ekspor media, lalu pilih Ekspor media sekarang. Anda dapat memilih lebih dari satu slot dan mengekspor beberapa kaset dalam satu operasi ekspor.



2. Di jendela pop-up Permintaan Media, pilih Lihat detail, lalu pilih Tanggapi OK di jendela Peringatan: Intervensi Media.

Di konsol Storage Gateway, Anda dapat memverifikasi status rekaman yang Anda arsipkan. Mungkin perlu beberapa waktu untuk menyelesaikan pengunggahan data ke AWS. Selama waktu ini, rekaman yang diekspor tercantum dalam Tape Gateway VTL dengan status IN TRANSIT TO VTS. Ketika unggahan selesai dan proses pengarsipan dimulai, status berubah menjadi PENGARSIPAN. Ketika pengarsipan data telah selesai, rekaman yang diekspor tidak

lagi terdaftar di VTL tetapi diarsipkan dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive.

3. Pilih gateway Anda, lalu pilih VTL Tape Cartridges dan verifikasi bahwa pita virtual tidak lagi terdaftar di gateway Anda.
4. Pada panel Navigasi konsol Storage Gateway, pilih Tapes. Verifikasi bahwa status rekaman Anda DIARSIPKAN.

Memulihkan Data dari Tape yang Diarsipkan di Backup Exec

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Gunakan Backup Exec untuk memulihkan data. Proses ini sama dengan memulihkan data dari kaset fisik. Untuk petunjuk, lihat Backup Exec Administrative Guide di bagian dokumentasi di perangkat lunak Backup Exec.

Menonaktifkan Tape Drive di Backup Exec

Tape Gateway menyediakan 10 tape drive, tetapi Anda mungkin memutuskan untuk menggunakan lebih sedikit tape drive. Dalam hal ini, Anda menonaktifkan tape drive yang tidak Anda gunakan.

1. Buka Backup Exec, dan pilih tab Penyimpanan.
2. Di pohon perpustakaan Robotic, buka menu konteks (klik kanan) untuk tape drive yang ingin Anda nonaktifkan, lalu pilih Nonaktifkan.

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Menguji Pengaturan Anda dengan Menggunakan Veritas NetBackup

Anda dapat mencadangkan data Anda ke kaset virtual, mengarsipkan kaset, dan mengelola perangkat pustaka pita virtual (VTL) Anda dengan menggunakan Veritas. NetBackup Dalam topik ini, Anda dapat menemukan dokumentasi dasar tentang cara mengkonfigurasi NetBackup aplikasi untuk

Tape Gateway dan melakukan operasi pencadangan dan pemulihan. Untuk melakukannya, Anda dapat menggunakan versi berikut NetBackup:

- Veritas 7.x NetBackup
- Veritas 8.x NetBackup

Prosedur untuk menggunakan versi Backup Exec ini dengan Tape Gateway serupa. Untuk informasi rinci tentang cara menggunakan NetBackup, lihat [Veritas Services and Operations Readiness Tools \(SORT\) di situs](#) web Veritas. Untuk informasi dukungan Veritas tentang kompatibilitas perangkat keras, lihat Daftar Kompatibilitas Perangkat Keras [NetBackup 7.0 - 7.6.x](#), [Daftar Kompatibilitas Perangkat Keras NetBackup 8.0 - 8.1.x](#), atau [Daftar Kompatibilitas Perangkat Keras NetBackup 8.2 - 8.xx](#) di situs web Veritas.

Untuk informasi selengkapnya tentang aplikasi cadangan yang kompatibel, lihat [Aplikasi cadangan pihak ketiga yang didukung untuk Tape Gateway](#).

Topik

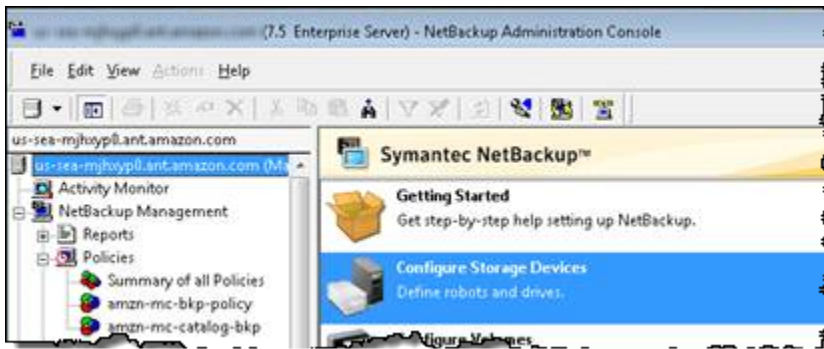
- [Mengkonfigurasi Perangkat NetBackup Penyimpanan](#)
- [Mencadangkan Data ke Tape](#)
- [Mengarsipkan Pita](#)
- [Memulihkan Data dari Tape](#)

Mengkonfigurasi Perangkat NetBackup Penyimpanan

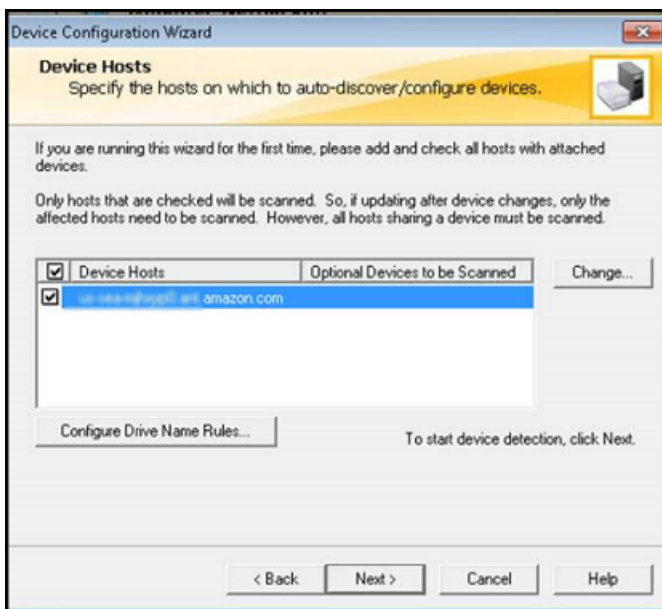
Setelah Anda menghubungkan perangkat pustaka pita virtual (VTL) ke klien Windows, Anda mengonfigurasi NetBackup penyimpanan Veritas untuk mengenali perangkat Anda. Untuk informasi tentang cara menghubungkan perangkat VTL ke klien Windows, lihat [Menghubungkan Perangkat VTL Anda](#)

Mengkonfigurasi NetBackup untuk menggunakan perangkat penyimpanan di Tape Gateway

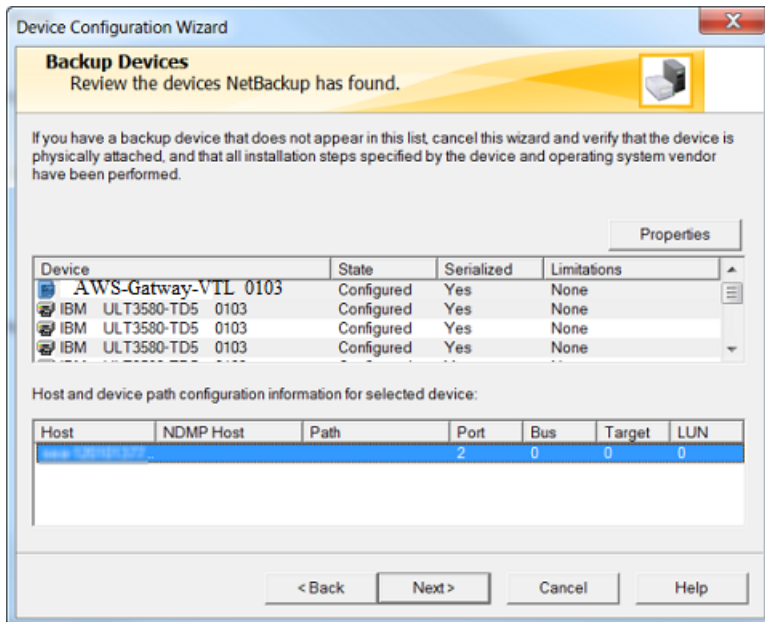
1. Buka Konsol NetBackup Administrasi dan jalankan sebagai administrator.



2. Pilih Konfigurasi Perangkat Penyimpanan untuk membuka panduan Konfigurasi Perangkat.
3. Pilih Berikutnya. NetBackup Aplikasi mendeteksi komputer Anda sebagai host perangkat.
4. Di kolom Device Hosts, pilih komputer Anda, lalu pilih Berikutnya. NetBackup Aplikasi memindai komputer Anda untuk perangkat dan menemukan semua perangkat.



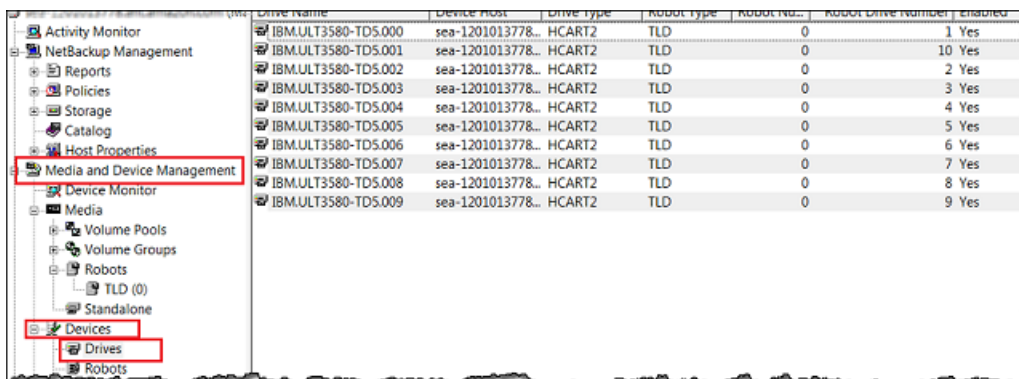
5. Di halaman Scanning Host, pilih Berikutnya, lalu pilih Berikutnya. NetBackup Aplikasi ini menemukan semua 10 tape drive dan medium changer di komputer Anda.



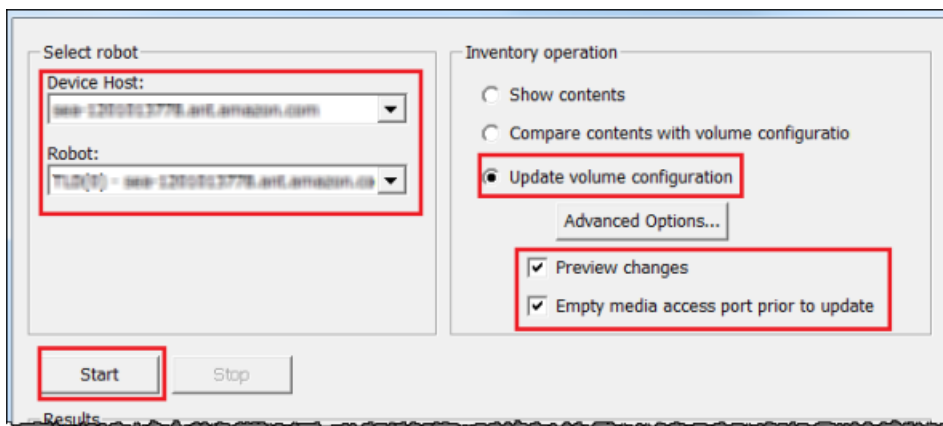
6. Di jendela Perangkat Cadangan, pilih Berikutnya.
7. Di jendela Drag and Drop Configuration, verifikasi bahwa medium changer Anda dipilih, lalu pilih Next.
8. Di kotak dialog yang muncul, pilih Ya untuk menyimpan konfigurasi di komputer Anda. NetBackup Aplikasi memperbarui konfigurasi perangkat.
9. Ketika pembaruan selesai, pilih Berikutnya untuk membuat perangkat tersedia untuk NetBackup aplikasi.
10. Di Selesai! jendela, pilih Selesai.

Untuk memverifikasi perangkat Anda dalam NetBackup aplikasi

1. Di Konsol NetBackup Administrasi, perluas node Media dan Manajemen Perangkat, lalu perluas node Devices. Pilih Drive untuk menampilkan semua tape drive.

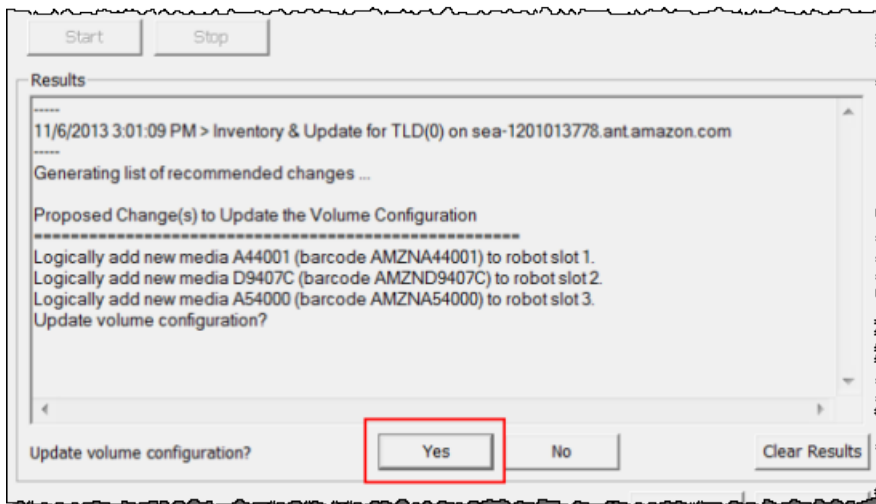


2. Di node Devices, pilih Robots untuk menampilkan semua medium changer Anda. Dalam NetBackup aplikasinya, medium changer disebut robot.
3. Di panel All Robots, buka menu konteks (klik kanan) untuk TLD (0) (yaitu robot Anda), lalu pilih Inventory Robot.
4. Di jendela Robot Inventory, verifikasi bahwa host Anda dipilih dari daftar Device-Host yang terletak di kategori Select robot.
5. Verifikasi bahwa robot Anda dipilih dari daftar Robot.
6. Di jendela Robot Inventory, pilih Perbarui konfigurasi volume, pilih Pratinjau perubahan, pilih port akses media kosong sebelum memperbarui, lalu pilih Mulai.

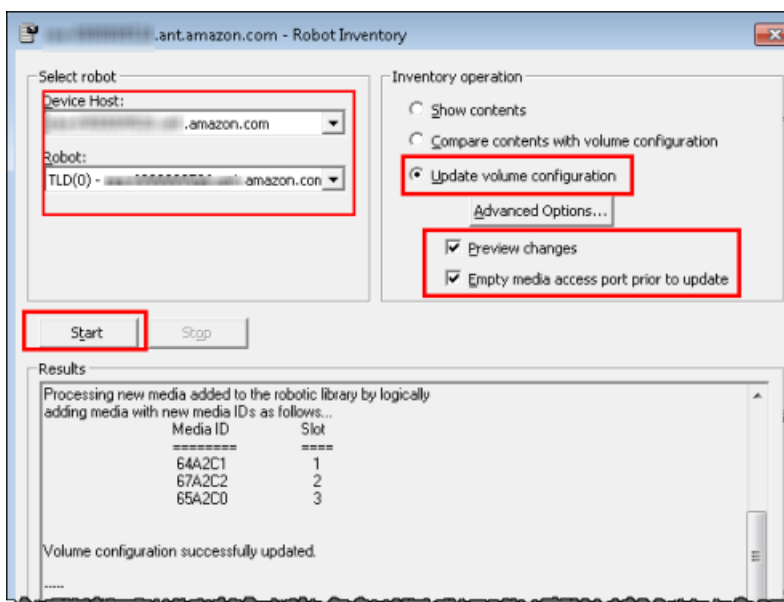


Proses ini kemudian menginventarisasi medium changer dan kaset virtual Anda dalam database NetBackup Enterprise Media Management (EMM). NetBackup menyimpan informasi media, konfigurasi perangkat, dan status tape di EMM.

7. Di jendela Robot Inventory, pilih Ya setelah inventaris selesai. Memilih Ya di sini memperbarui konfigurasi dan memindahkan kaset virtual yang ditemukan di slot impor/ekspor ke pustaka pita virtual.



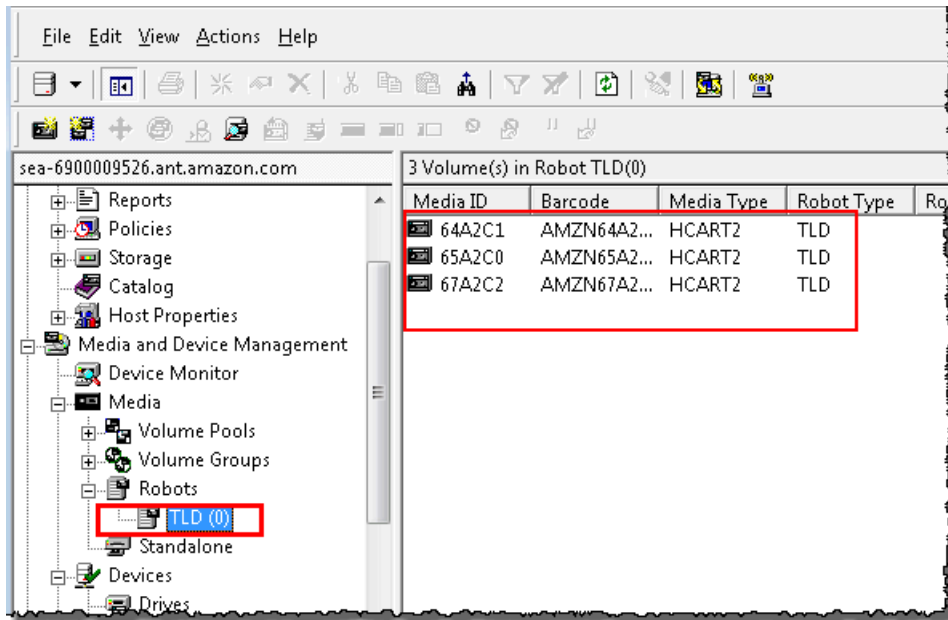
Misalnya, tangkapan layar berikut menunjukkan tiga kaset virtual yang ditemukan di slot impor/eksport.



8. Tutup jendela Robot Inventory.
9. Di node Media, perluas node Robots dan pilih TLD (0) untuk menampilkan semua kaset virtual yang tersedia untuk robot Anda (medium changer).

i Note

Jika sebelumnya Anda telah menghubungkan perangkat lain ke NetBackup aplikasi, Anda mungkin memiliki beberapa robot. Pastikan Anda memilih robot yang tepat.



Sekarang setelah Anda menghubungkan perangkat Anda dan membuatnya tersedia untuk aplikasi cadangan Anda, Anda siap untuk menguji gateway Anda. Untuk menguji gateway Anda, Anda mencadangkan data ke kaset virtual yang Anda buat dan arsipkan kaset.

Mencadangkan Data ke Tape

Anda menguji penyiapan Tape Gateway dengan mencadangkan data ke kaset virtual Anda.

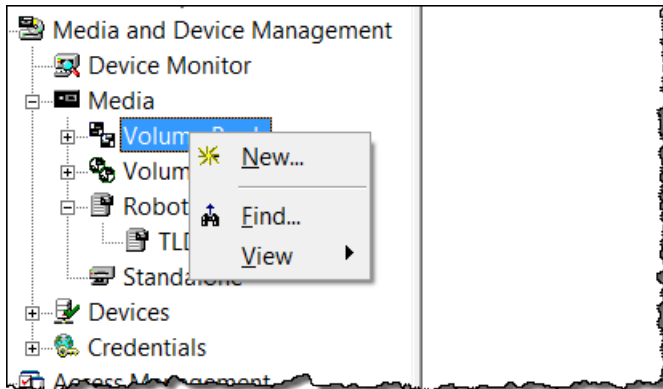
Note

- Anda harus mencadangkan hanya sejumlah kecil data untuk latihan Memulai ini, karena ada biaya yang terkait dengan penyimpanan, pengarsipan, dan pengambilan data. Untuk informasi harga, lihat [Harga](#) di halaman detail Storage Gateway.
- Jika Tape Gateway Anda dimulai ulang karena alasan apa pun selama pekerjaan pencadangan yang sedang berlangsung, pekerjaan pencadangan akan ditangguhkan. Pekerjaan pencadangan yang ditangguhkan akan dilanjutkan secara otomatis ketika gateway Anda selesai dimulai ulang.

Untuk membuat kolam volume

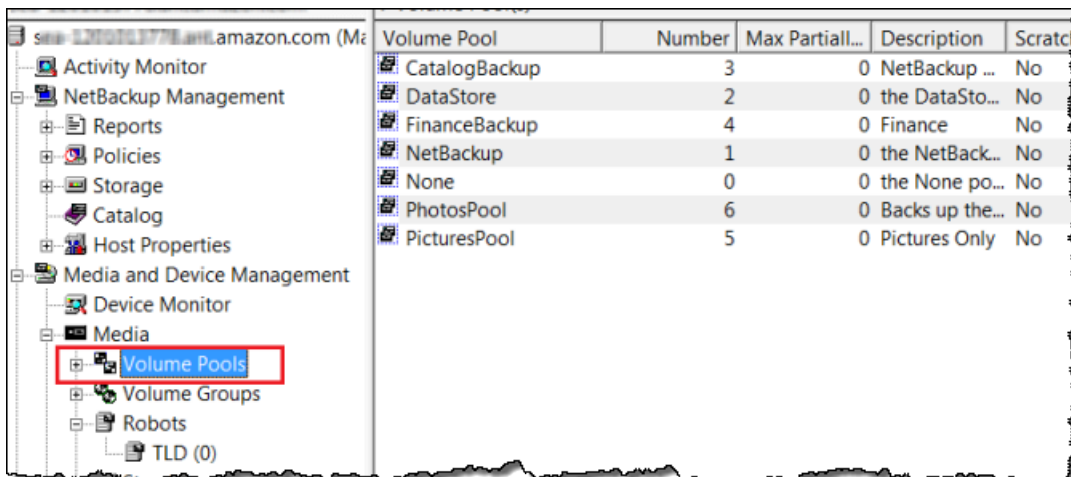
Volume pool adalah kumpulan kaset virtual untuk digunakan untuk cadangan.

1. Mulai Konsol NetBackup Administrasi.
2. Perluas node Media, buka menu konteks (klik kanan) untuk Volume Pool, lalu pilih Baru. Kotak dialog New Volume Pool muncul.



3. Untuk Nama, ketikkan nama untuk kumpulan volume Anda.
4. Untuk Deskripsi, ketikkan deskripsi untuk kumpulan volume, lalu pilih OK. Volume pool yang baru saja Anda buat ditambahkan ke daftar volume pool.

Tangkapan layar berikut menunjukkan daftar kumpulan volume.

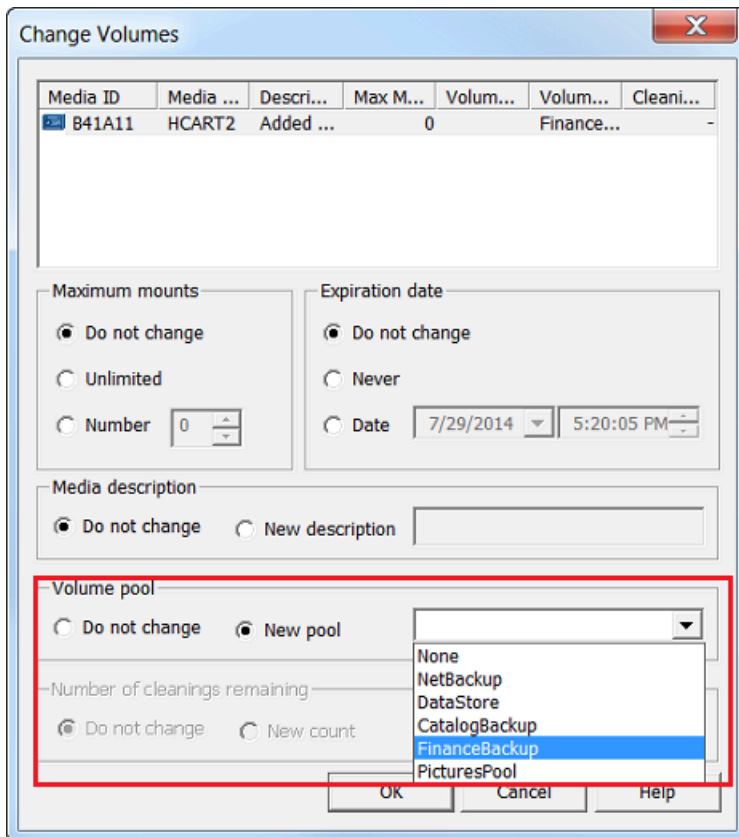


Untuk menambahkan kaset virtual ke kumpulan volume

1. Perluas node Robots, dan pilih robot TLD (0) untuk menampilkan kaset virtual yang diketahui robot ini.

Jika sebelumnya Anda telah menghubungkan robot, robot Tape Gateway Anda mungkin memiliki nama yang berbeda.

2. Dari daftar kaset virtual, buka menu konteks (klik kanan) untuk rekaman yang ingin Anda tambahkan ke kumpulan volume, dan pilih Ubah untuk membuka kotak dialog Ubah Volume. Tangkapan layar berikut menunjukkan Ubah Volume kotak dialog.



3. Untuk Volume Pool, pilih New pool.
4. Untuk kolom Baru, pilih kolom yang baru saja Anda buat, lalu pilih OK.

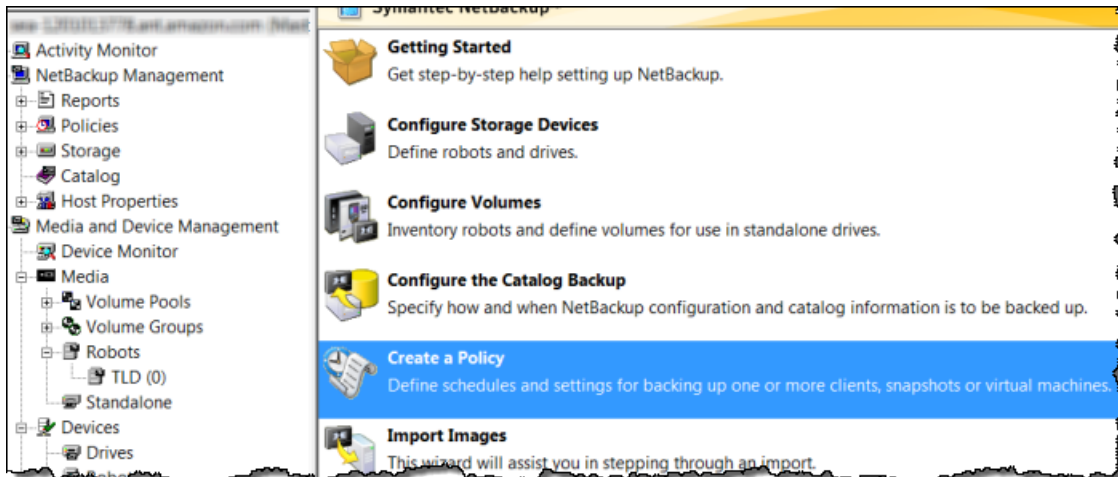
Anda dapat memverifikasi bahwa kumpulan volume Anda berisi rekaman virtual yang baru saja Anda tambahkan dengan memperluas node Media dan memilih kumpulan volume Anda.

Untuk membuat kebijakan backup

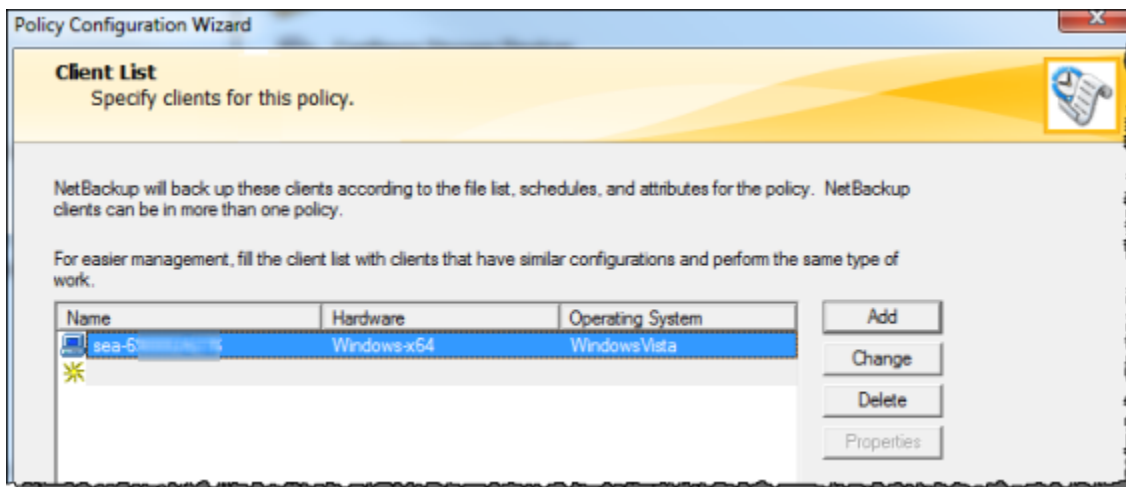
Kebijakan pencadangan menentukan data apa yang akan dicadangkan, kapan harus mencadangkannya, dan kumpulan volume mana yang akan digunakan.

1. Pilih Master Server Anda untuk kembali ke NetBackup konsol Veritas.

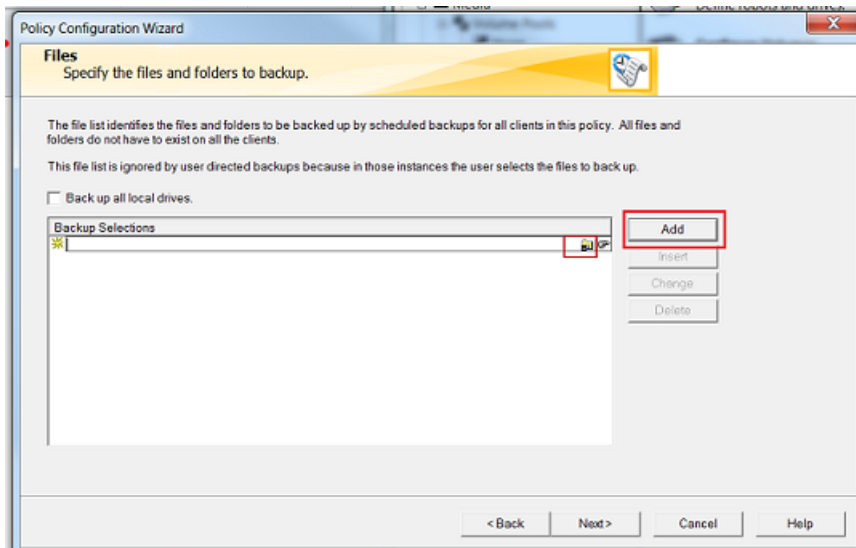
Screenshot berikut menunjukkan NetBackup konsol dengan Create a Policy dipilih.



2. Pilih Buat Kebijakan untuk membuka jendela Wisaya Konfigurasi Kebijakan.
3. Pilih Sistem file, database, aplikasi, dan pilih Berikutnya.
4. Untuk Nama Kebijakan, ketik nama untuk kebijakan Anda dan verifikasi bahwa MS-Windows dipilih dari daftar Pilih jenis kebijakan, lalu pilih Berikutnya.
5. Di jendela Daftar Klien, pilih Tambah, ketik nama host komputer Anda di kolom Nama, lalu pilih Berikutnya. Langkah ini menerapkan kebijakan yang Anda definisikan localhost (komputer klien Anda).



6. Di jendela File, pilih Tambah, lalu pilih ikon folder.

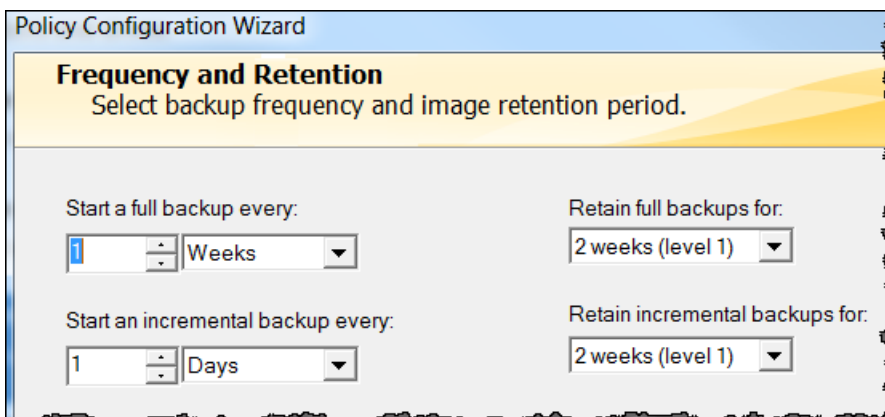


7. Di jendela Browse, telusuri folder atau file yang ingin Anda cadangkan, pilih OK, lalu pilih Berikutnya.
8. Di jendela Jenis Cadangan, terima defaultnya, lalu pilih Berikutnya.

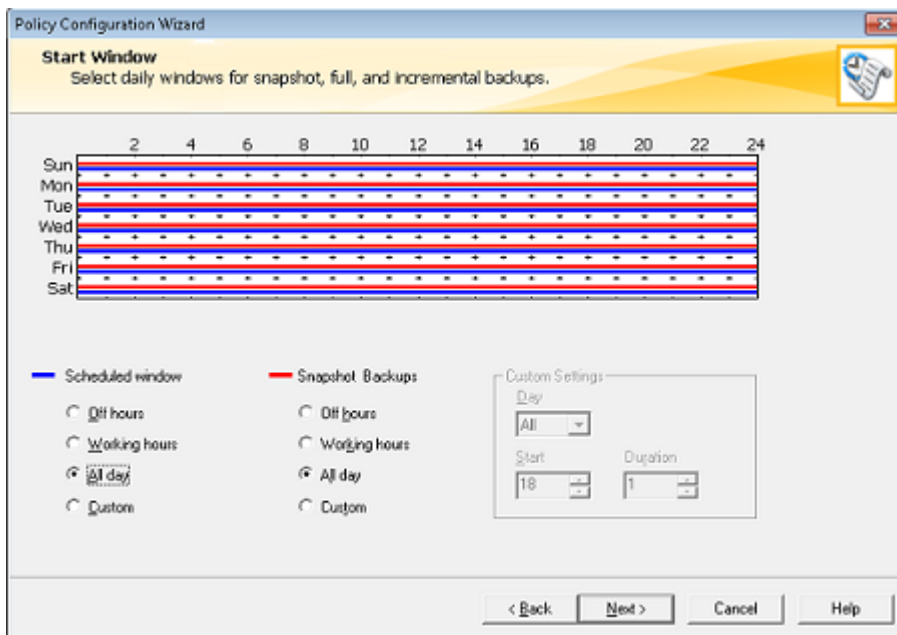
Note

Jika Anda ingin memulai pencadangan sendiri, pilih Cadangan Pengguna.

9. Di jendela Frekuensi dan Retensi, pilih kebijakan frekuensi dan retensi yang ingin Anda terapkan pada cadangan. Untuk latihan ini, Anda dapat menerima semua default dan memilih Berikutnya.



10. Di jendela Start, pilih Off hours, lalu pilih Next. Pilihan ini menentukan bahwa folder Anda harus dicadangkan selama jam off saja.

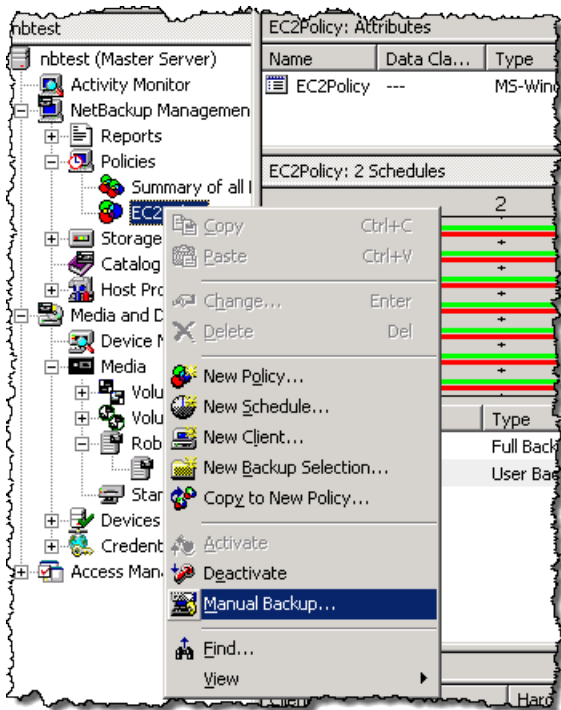


11. Di wizard Konfigurasi Kebijakan, pilih Selesai.

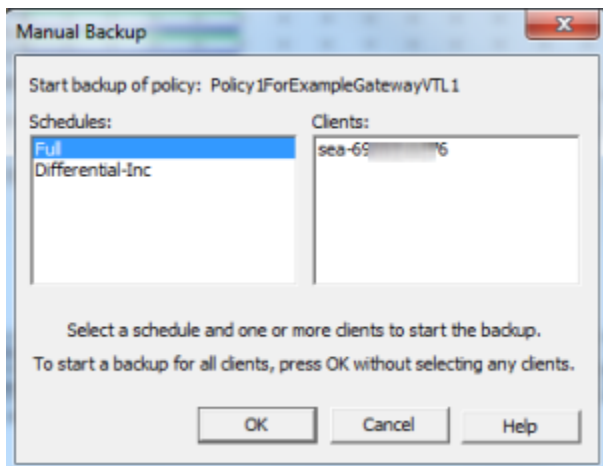
Kebijakan menjalankan backup sesuai dengan jadwal. Anda juga dapat melakukan pencadangan manual kapan saja, yang kami lakukan pada langkah berikutnya.

Untuk melakukan backup manual

1. Pada panel navigasi NetBackup konsol, perluas simpul NetBackup Manajemen.
2. Perluas simpul Kebijakan.
3. Buka menu konteks (klik kanan) untuk kebijakan Anda, dan pilih Backup Manual.



4. Di jendela Backup Manual, pilih jadwal, pilih klien, lalu pilih OK.



5. Di kotak dialog Pencadangan Manual Dimulai yang muncul, pilih OK.

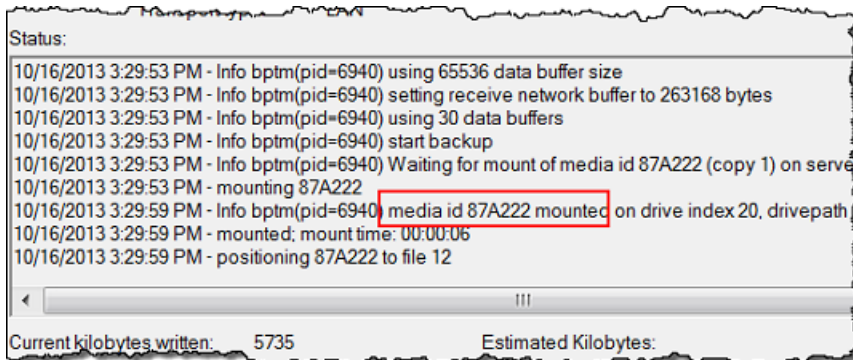
6. Pada panel navigasi, pilih Monitor Aktivitas untuk melihat status cadangan Anda di kolom ID Job.

nbtest: 11 Jobs (0 Queued 0 Active 0 Waiting for Retry 0 Suspended 0 Incomplete 11 Done)								
	Job ID	Type	Job State	State Details	Status	Job Policy	Job Schedule	Client
	18	Backup	Done		0	EC2Policy	Full	localhost
	17	Backup	Done		0	EC2Policy	Full	localhost
	14	Backup	Done		0	EC2Policy	Full	localhost
	10	Image Cleanup	Done		1			
	11	Image Cleanup	Done		1			

Untuk menemukan kode batang pita virtual tempat NetBackup menulis data file selama pencadangan, lihat di jendela Rincian Pekerjaan seperti yang dijelaskan dalam prosedur berikut. Anda memerlukan barcode ini dalam prosedur di bagian selanjutnya, tempat Anda mengarsipkan rekaman itu.

Untuk menemukan kode batang kaset

1. Di Monitor Aktivitas, buka menu konteks (klik kanan) untuk pengenalan pekerjaan cadangan Anda di kolom ID Pekerjaan, lalu pilih Detail.
2. Di jendela Job Details, pilih tab Status Terperinci.
3. Di kotak Status, cari ID media. Misalnya, pada tangkapan layar berikut, ID media adalah 87A222. ID ini membantu Anda menentukan rekaman mana yang telah Anda tulis data.



Anda sekarang telah berhasil menerapkan Tape Gateway, membuat kaset virtual, dan mencadangkan data Anda. Selanjutnya, Anda dapat mengarsipkan kaset virtual dan mengambilnya dari arsip.

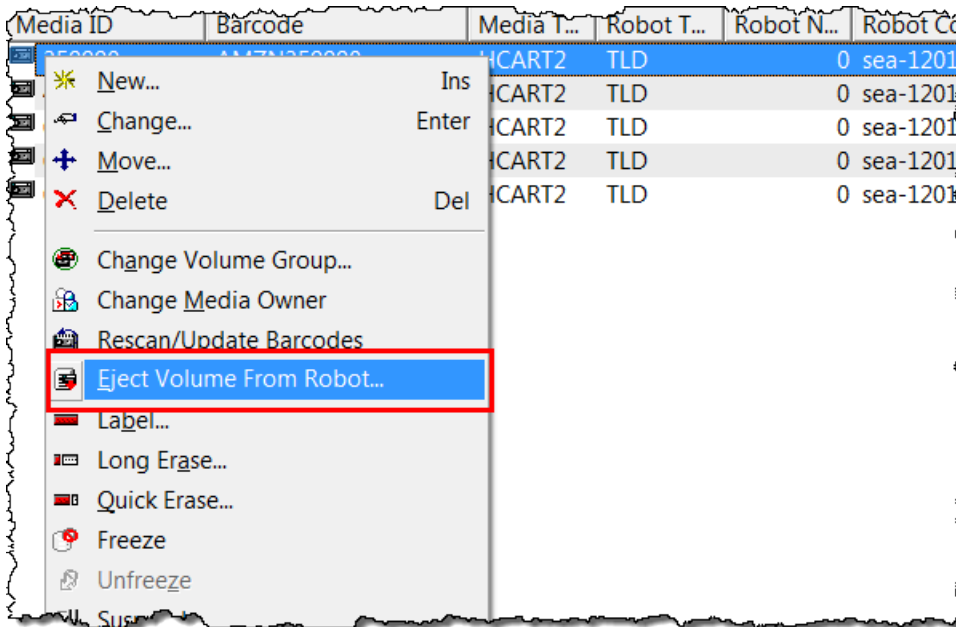
Mengarsipkan Pita

Saat Anda mengarsipkan kaset, Tape Gateway memindahkan kaset dari pustaka pita virtual (VTL) gateway Anda ke arsip, yang menyediakan penyimpanan offline. Anda memulai arsip kaset dengan mengeluarkan kaset menggunakan aplikasi cadangan Anda.

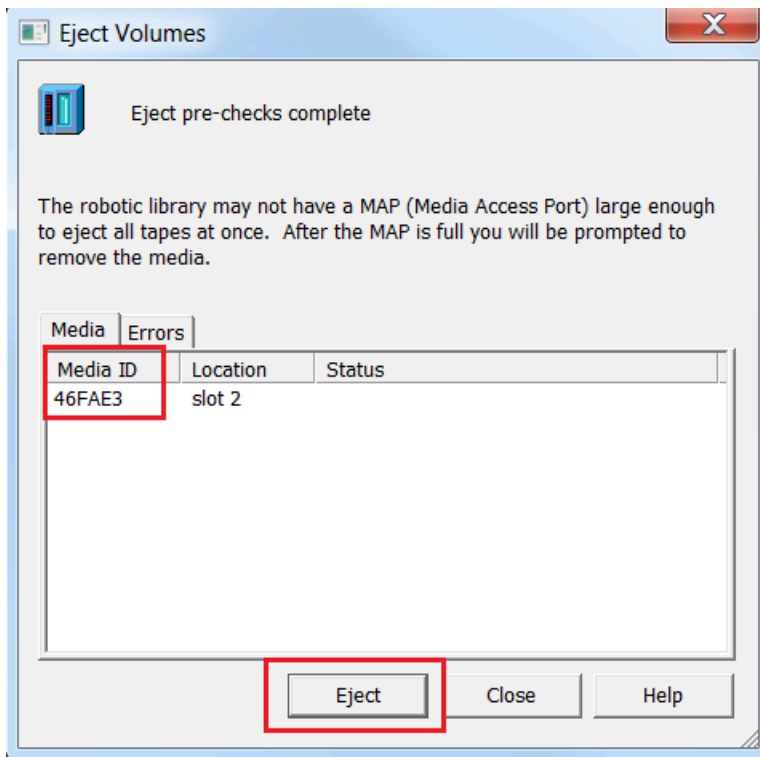
Untuk mengarsipkan rekaman virtual

1. Di konsol NetBackup Administrasi, perluas node Media dan Manajemen Perangkat, dan perluas node Media.
2. Perluas Robot dan pilih TLD (0).

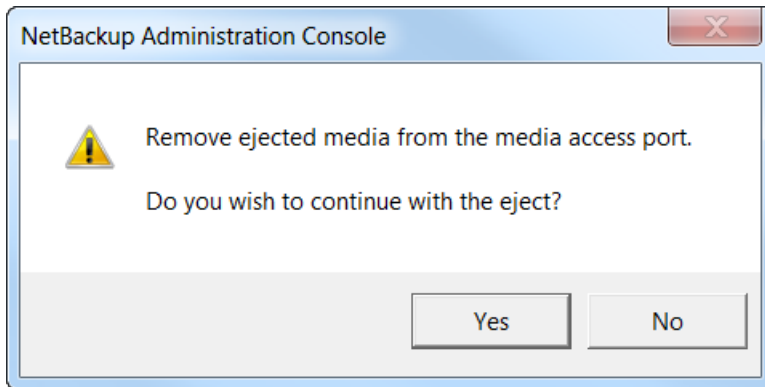
3. Buka menu konteks (klik kanan) untuk rekaman virtual yang ingin Anda arsipkan, dan pilih Keluarkan Volume Dari Robot.



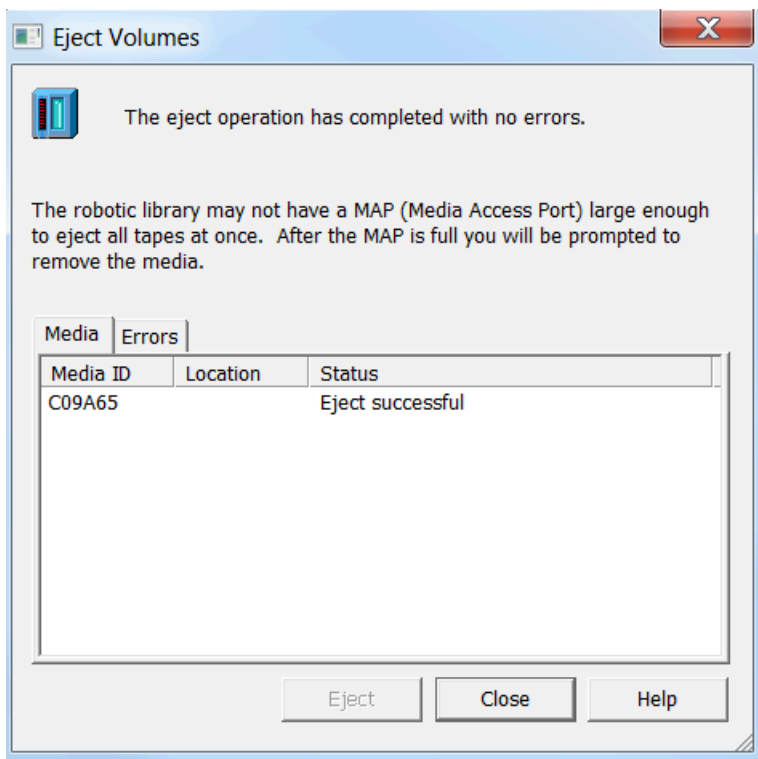
4. Di jendela Eject Volumes, pastikan ID Media cocok dengan pita virtual yang ingin Anda keluarkan, lalu pilih Eject.



5. Di kotak dialog, pilih Ya. Kotak dialog ditampilkan sebagai berikut.



Ketika proses eject selesai, status rekaman di kotak dialog Eject Volumes menunjukkan bahwa eject berhasil.



6. Pilih Tutup untuk menutup jendela Eject Volumes.
7. Di konsol Storage Gateway, verifikasi status rekaman yang Anda arsipkan di VTL gateway. Diperlukan beberapa waktu untuk menyelesaikan pengunggahan data ke AWS. Selama waktu ini, rekaman yang dikeluarkan terdaftar di VTL gateway dengan status IN TRANSIT TO VTS. Saat pengarsipan dimulai, statusnya adalah PENGARSIPAN. Setelah pengunggahan data selesai, rekaman yang dikeluarkan tidak lagi terdaftar di VTL tetapi diarsipkan dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive.

8. Untuk memverifikasi bahwa pita virtual tidak lagi terdaftar di gateway Anda, pilih gateway Anda, lalu pilih VTL Tape Cartridges.
9. Di panel navigasi konsol Storage Gateway, pilih Tapes. Verifikasi bahwa status rekaman arsip Anda DIARSIPKAN.

Memulihkan Data dari Tape

Memulihkan data yang diarsipkan adalah proses dua langkah.

Untuk memulihkan data dari rekaman yang diarsipkan

1. Ambil rekaman yang diarsipkan ke Tape Gateway. Untuk petunjuk, lihat [Mengambil Kaset yang Diarsipkan](#).
2. Gunakan perangkat lunak Backup, Archive, dan Restore yang diinstal dengan NetBackup aplikasi Veritas. Proses ini sama dengan memulihkan data dari kaset fisik. Untuk petunjuk, lihat [Veritas Services and Operations Readiness Tools \(SORT\) di situs](#) web Veritas.

Langkah Selanjutnya

[Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#)

Apa Langkah Berikutnya?

Setelah Tape Gateway dalam produksi, Anda dapat melakukan beberapa tugas pemeliharaan, seperti menambahkan dan menghapus kaset, memantau dan mengoptimalkan kinerja gateway, dan pemecahan masalah. Untuk informasi umum tentang tugas-tugas manajemen ini, lihat [Mengelola Gateway Anda](#).

Anda dapat melakukan beberapa tugas pemeliharaan Tape Gateway AWS Management Console, seperti mengonfigurasi batas laju bandwidth gateway Anda dan mengelola pembaruan perangkat lunak gateway. Jika Tape Gateway digunakan di lokasi, Anda dapat melakukan beberapa tugas pemeliharaan di konsol lokal gateway. Ini termasuk merutekan Tape Gateway Anda melalui proxy dan mengonfigurasi gateway Anda untuk menggunakan alamat IP statis. Jika menjalankan gateway sebagai instans Amazon EC2, Anda dapat melakukan tugas pemeliharaan tertentu di konsol Amazon EC2, seperti menambahkan dan menghapus volume Amazon EBS. Untuk informasi selengkapnya tentang cara memelihara Tape Gateway Anda, lihat [Mengelola Tape Gateway Anda](#).

Jika Anda berencana untuk menggunakan gateway Anda dalam produksi, Anda harus mempertimbangkan beban kerja Anda yang sebenarnya dalam menentukan ukuran disk. Untuk

informasi tentang cara menentukan ukuran disk dunia nyata, lihat [Mengelola disk lokal untuk Storage Gateway Anda](#). Juga, pertimbangkan untuk membersihkan jika Anda tidak berencana untuk terus menggunakan Tape Gateway Anda. Membersihkan memungkinkan Anda menghindari biaya yang dikenakan. Untuk informasi tentang pembersihan, lihat [Membersihkan Sumber Daya yang Tidak Anda Butuhkan](#).

Membersihkan Sumber Daya yang Tidak Anda Butuhkan

Jika Anda membuat gateway sebagai contoh latihan atau tes, pertimbangkan untuk membersihkan untuk menghindari timbulnya biaya yang tidak terduga atau tidak perlu.

Jika Anda berencana untuk terus menggunakan Tape Gateway, lihat informasi tambahan di [Apa Langkah Berikutnya?](#)

Untuk membersihkan sumber daya yang tidak Anda butuhkan

1. Hapus kaset dari pustaka pita virtual (VTL) dan arsip gateway Anda. Untuk informasi selengkapnya, lihat [Menghapus Gateway Anda dengan Menggunakan AWS Storage Gateway Konsol dan Menghapus Sumber Daya Terkait](#).
 - a. Arsipkan kaset apa pun yang memiliki status RETRIEVED di VTL gateway Anda. Untuk petunjuk, lihat [Kaset Pengarsipan](#).
 - b. Hapus kaset yang tersisa dari VTL gateway Anda. Untuk petunjuk, lihat [Menghapus Kaset](#).
 - c. Hapus semua kaset yang Anda miliki di arsip. Untuk petunjuk, lihat [Menghapus Kaset](#).
2. Kecuali Anda berencana untuk terus menggunakan Tape Gateway, hapus: Untuk petunjuk, lihat [Menghapus Gateway Anda dengan Menggunakan AWS Storage Gateway Konsol dan Menghapus Sumber Daya Terkait](#).
3. Hapus VM Storage Gateway dari host lokal Anda. Jika Anda membuat gateway di instans Amazon EC2, hentikan instans.

Mengaktifkan gateway Anda di cloud pribadi virtual

Anda dapat membuat sambungan pribadi antara alat gateway lokal dan infrastruktur penyimpanan berbasis cloud. Anda dapat menggunakan koneksi ini untuk mengaktifkan gateway Anda dan memungkinkannya mentransfer data ke layanan AWS penyimpanan tanpa berkomunikasi melalui internet publik. Dengan menggunakan layanan Amazon VPC, Anda dapat meluncurkan AWS sumber daya, termasuk titik akhir antarmuka jaringan pribadi, di cloud pribadi virtual (VPC) khusus. VPC memberi Anda kontrol atas pengaturan jaringan seperti rentang alamat IP, subnet, tabel rute,

dan gateway jaringan. Untuk informasi selengkapnya tentang VPC, lihat [Apa itu Amazon VPC?](#) di Panduan Pengguna Amazon VPC.

Untuk mengaktifkan gateway Anda di VPC, gunakan Konsol VPC Amazon untuk membuat titik akhir VPC untuk Storage Gateway dan dapatkan ID titik akhir VPC, lalu tentukan ID titik akhir VPC ini saat Anda membuat dan mengaktifkan gateway. Untuk informasi selengkapnya, lihat [Connect Tape Gateway Anda untuk AWS](#).

Note

Anda harus mengaktifkan gateway Anda di wilayah yang sama di mana Anda membuat titik akhir VPC untuk Storage Gateway

Topik

- [Membuat Endpoint VPC untuk Storage Gateway](#)

Membuat Endpoint VPC untuk Storage Gateway

Ikuti petunjuk ini untuk membuat titik akhir VPC. Jika Anda sudah memiliki titik akhir VPC untuk Storage Gateway, Anda dapat menggunakannya untuk mengaktifkan gateway Anda.

Untuk membuat titik akhir VPC untuk Storage Gateway

1. [Masuk ke AWS Management Console dan buka konsol VPC Amazon di https://console.aws.amazon.com/vpc/.](https://console.aws.amazon.com/vpc/)
2. Di panel navigasi, pilih Endpoints, lalu pilih Create Endpoint.
3. Pada halaman Buat Titik Akhir, pilih kategori AWS Layanan untuk Layanan.
4. Untuk Nama Layanan, pilih `com.amazonaws.region.storagegateway`. Sebagai contoh, `com.amazonaws.us-east-2.storagegateway`.
5. Untuk VPC, pilih VPC Anda dan catat Availability Zones dan subnetnya.
6. Verifikasi bahwa Aktifkan Nama DNS Pribadi tidak dipilih.
7. Untuk grup Keamanan, pilih grup keamanan yang ingin Anda gunakan untuk VPC Anda. Anda dapat menerima grup keamanan default. Verifikasi bahwa semua port TCP berikut diizinkan di grup keamanan Anda:
 - TCP 443

- TCP 1026
 - TCP 1027
 - TCP 1028
 - TCP 1031
 - TCP 2222
8. Pilih Buat titik akhir. Keadaan awal titik akhir tertunda. Saat titik akhir dibuat, perhatikan ID titik akhir VPC yang baru saja Anda buat.
 9. Saat titik akhir dibuat, pilih Titik Akhir, lalu pilih titik akhir VPC baru.
 10. Di tab Detail titik akhir gateway penyimpanan yang dipilih, di bawah Nama DNS, gunakan nama DNS pertama yang tidak menentukan Availability Zone. Nama DNS Anda terlihat mirip dengan ini: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Sekarang setelah Anda memiliki titik akhir VPC, Anda dapat membuat gateway Anda. Untuk informasi selengkapnya, lihat [Membuat Gateway](#) .

Mengelola Gateway Anda

Mengelola gateway Anda mencakup tugas-tugas seperti mengonfigurasi penyimpanan cache dan mengunggah ruang buffer, bekerja dengan volume atau kaset virtual, dan melakukan pemeliharaan umum. Jika Anda belum membuat gateway, lihat [Memulai](#).

Rilis perangkat lunak Gateway secara berkala akan mencakup pembaruan OS dan patch keamanan yang telah divalidasi. Pembaruan ini diterapkan sebagai bagian dari proses pembaruan gateway reguler selama jendela pemeliharaan terjadwal, dan biasanya dirilis setiap enam bulan. Catatan: Pengguna harus memperlakukan alat Storage Gateway sebagai mesin virtual terkelola, dan tidak boleh mencoba mengakses atau memodifikasi instance alat Storage Gateway. Mencoba menginstal atau memperbarui paket perangkat lunak apa pun menggunakan metode lain (misalnya: SSM atau alat Hypervisor) daripada mekanisme pembaruan gateway normal dapat mengakibatkan gangguan pada berfungsinya Gateway dengan benar.

Topik

- [Mengelola Tape Gateway Anda](#)
- [Memindahkan data Anda ke gateway baru](#)

Mengelola Tape Gateway Anda

Setelah itu, Anda dapat menemukan informasi tentang cara mengelola sumber daya Tape Gateway Anda di AWS Storage Gateway.

Topik

- [Mengedit Informasi Gateway Dasar](#)
- [Menambahkan Kaset Virtual](#)
- [Mengelola Pembuatan Pita Otomatis](#)
- [Pengarsipan Kaset Virtual](#)
- [Memindahkan Tape Anda dari Pengambilan Fleksibel Gletser S3 ke Kelas Penyimpanan S3 Glacier Deep Archive](#)
- [Mengambil Kaset yang Diarsipkan](#)
- [Penggunaan Tape Melihat](#)
- [Menghapus Kaset](#)

- [Menghapus Kolam Pita Kustom](#)
- [Menonaktifkan Tape Gateway Anda](#)
- [Memahami Status Pita](#)

Mengedit Informasi Gateway Dasar

Anda dapat menggunakan konsol Storage Gateway untuk mengedit informasi dasar untuk gateway yang ada, termasuk nama gateway, zona waktu, dan grup CloudWatch log.

Untuk mengedit informasi dasar untuk gateway yang ada

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Pilih Gateway, lalu pilih gateway yang ingin Anda edit informasi dasarnya.
3. Dari menu tarik-turun Tindakan, pilih Edit informasi gateway.
4. Ubah pengaturan yang ingin Anda ubah, lalu pilih Simpan perubahan.

Note

Mengubah nama gateway akan memutuskan CloudWatch alarm apa pun yang diatur untuk memantau gateway. Untuk menghubungkan kembali alarm, perbarui GatewayName untuk setiap alarm di konsol. CloudWatch

Menambahkan Kaset Virtual

Anda dapat menambahkan kaset di Tape Gateway saat Anda membutuhkannya. Untuk selengkapnya tentang cara membuat kaset, lihat [Membuat Kaset](#).

Setelah rekaman Anda dibuat, Anda dapat menemukan informasi tentangnya di halaman ikhtisar Tape. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti. Untuk informasi tentang kuota pita Tape Gateway, lihat [AWS Storage Gateway kuota](#).

Mengelola Pembuatan Pita Otomatis

Tape Gateway secara otomatis membuat kaset virtual baru untuk mempertahankan jumlah minimum kaset yang tersedia yang Anda konfigurasi. Kemudian membuat kaset baru ini tersedia untuk diimpor oleh aplikasi cadangan sehingga pekerjaan cadangan Anda dapat berjalan tanpa gangguan. Pembuatan pita otomatis menghilangkan kebutuhan akan skrip khusus selain proses manual untuk membuat kaset virtual baru.

Untuk menghapus kebijakan pembuatan pita otomatis

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih tab Gateways.
3. Pilih gateway yang Anda butuhkan untuk mengelola pembuatan pita otomatis.
4. Di menu Actions, pilih Configure tape auto-create.
5. Untuk menghapus kebijakan pembuatan rekaman otomatis di gateway, pilih Hapus di sebelah kanan kebijakan yang ingin Anda hapus.

Untuk menghentikan pembuatan pita otomatis di gateway, hapus semua kebijakan pembuatan pita otomatis untuk gateway itu.

Pilih Simpan perubahan untuk mengonfirmasi penghapusan kebijakan pembuatan otomatis tape untuk Tape Gateway yang dipilih.


Note

Menghapus kebijakan pembuatan otomatis tape dari gateway tidak dapat dibatalkan.

Untuk mengubah kebijakan pembuatan tape otomatis untuk Tape Gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih tab Gateways.
3. Pilih gateway yang Anda butuhkan untuk mengelola pembuatan pita otomatis.
4. Di menu Actions, pilih Configure tape auto-create, dan ubah pengaturan pada halaman yang muncul.

5. Untuk jumlah minimum kaset, masukkan jumlah minimum kaset virtual yang harus tersedia di Tape Gateway setiap saat. Rentang yang valid untuk nilai ini adalah minimal 1 dan maksimum 10.
6. Untuk Kapasitas, masukkan ukuran, dalam byte kapasitas pita virtual. Rentang yang valid untuk nilai ini adalah minimal 100 GiB dan maksimum 15 TiB.
7. Untuk awalan Barcode, masukkan awalan yang ingin Anda tambahkan ke barcode kaset virtual Anda.

 Note

Kaset virtual diidentifikasi secara unik oleh kode batang, dan Anda dapat menambahkan awalan ke kode batang. Awalan adalah opsional, tetapi Anda dapat menggunakannya untuk membantu mengidentifikasi kaset virtual Anda. Awalan harus huruf besar (A-Z) dan harus satu sampai empat karakter panjang.

8. Untuk Pool, pilih Glacier Pool atau Deep Archive Pool. Kumpulan ini mewakili kelas penyimpanan tempat kaset Anda disimpan saat dikeluarkan oleh perangkat lunak cadangan Anda.
 - Pilih Glacier Pool jika Anda ingin mengarsipkan kaset di kelas penyimpanan S3 Glacier Flexible Retrieval. Ketika perangkat lunak cadangan Anda mengeluarkan kaset, mereka secara otomatis diarsipkan dalam S3 Glacier Flexible Retrieval. Anda menggunakan S3 Glacier Flexible Retrieval untuk arsip yang lebih aktif, di mana Anda dapat mengambil rekaman biasanya dalam waktu 3-5 jam. Untuk informasi selengkapnya, lihat [Kelas Penyimpanan untuk Mengarsipkan Objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
 - Pilih Deep Archive Pool jika Anda ingin mengarsipkan kaset di S3 Glacier Deep Archive. Saat perangkat lunak cadangan Anda mengeluarkan kaset, rekaman itu secara otomatis diarsipkan di S3 Glacier Deep Archive. Anda menggunakan S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital, di mana data diakses sekali atau dua kali setahun. Anda dapat mengambil rekaman yang diarsipkan di S3 Glacier Deep Archive biasanya dalam waktu 12 jam. Untuk informasi selengkapnya, lihat [Kelas Penyimpanan untuk Mengarsipkan Objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Jika Anda mengarsipkan kaset di S3 Glacier Flexible Retrieval, Anda dapat memindahkannya ke S3 Glacier Deep Archive nanti. Untuk informasi selengkapnya, lihat [Memindahkan Tape Anda dari Pengambilan Fleksibel Gletser S3 ke Kelas Penyimpanan S3 Glacier Deep Archive](#).

9. Anda dapat menemukan informasi tentang kaset Anda di halaman ikhtisar Tape. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.

Status kaset virtual yang tersedia awalnya diatur ke CREATING ketika kaset sedang dibuat. Setelah kaset dibuat, statusnya berubah menjadi TERSEDIA. Untuk informasi selengkapnya, lihat [Mengelola Tape Gateway Anda](#).

Untuk informasi selengkapnya tentang mengaktifkan pembuatan pita otomatis, lihat [Membuat Kaset Secara Otomatis](#).

Pengarsipan Kaset Virtual

Anda dapat mengarsipkan kaset Anda ke S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive. Saat Anda membuat rekaman, Anda memilih kumpulan arsip yang ingin Anda gunakan untuk mengarsipkan rekaman Anda.

Anda memilih Glacier Pool jika Anda ingin mengarsipkan rekaman di S3 Glacier Flexible Retrieval. Ketika perangkat lunak cadangan Anda mengeluarkan rekaman, itu secara otomatis diarsipkan dalam S3 Glacier Flexible Retrieval. Anda menggunakan Pengambilan Fleksibel Gletser S3 untuk arsip yang lebih aktif di mana data diambil secara teratur dan dibutuhkan dalam hitungan menit. Untuk informasi selengkapnya, lihat [Kelas Penyimpanan untuk Objek Pengarsipan](#)

Anda memilih Deep Archive Pool jika Anda ingin mengarsipkan rekaman di S3 Glacier Deep Archive. Saat perangkat lunak cadangan Anda mengeluarkan kaset, rekaman itu secara otomatis diarsipkan di S3 Glacier Deep Archive. Anda menggunakan S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital dengan biaya yang sangat rendah. Data di S3 Glacier Deep Archive tidak sering diambil atau jarang diambil. Untuk informasi lebih lanjut, lihat [Kelas Penyimpanan untuk Mengarsipkan Objek](#).

Note

Rekaman apa pun yang dibuat sebelum 27 Maret 2019, diarsipkan langsung di S3 Glacier Flexible Retrieval saat perangkat lunak cadangan Anda mengeluarkannya.

Ketika perangkat lunak cadangan Anda mengeluarkan kaset, itu secara otomatis diarsipkan di kolam yang Anda pilih saat Anda membuat rekaman itu. Proses untuk mengeluarkan kaset bervariasi tergantung pada perangkat lunak cadangan Anda. Beberapa perangkat lunak cadangan mengharuskan Anda mengekspor kaset setelah dikeluarkan sebelum pengarsipan dapat dimulai. Untuk informasi tentang perangkat lunak pencadangan yang didukung, lihat [Menggunakan Perangkat Lunak Cadangan untuk Menguji Pengaturan Gateway Anda](#).

Memindahkan Tape Anda dari Pengambilan Fleksibel Gletser S3 ke Kelas Penyimpanan S3 Glacier Deep Archive

Pindahkan kaset Anda dari S3 Glacier Flexible Retrieval ke S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital dengan biaya yang sangat rendah. Anda menggunakan S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital di mana data diakses sekali atau dua kali setahun. Untuk informasi lebih lanjut, lihat [Kelas Penyimpanan untuk Mengarsipkan Objek](#).

Untuk memindahkan kaset dari S3 Glacier Flexible Retrieval ke S3 Glacier Deep Archive

1. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.
2. Pilih kotak centang untuk kaset yang ingin Anda pindahkan ke S3 Glacier Deep Archive. Anda dapat melihat kolam yang dikaitkan dengan setiap pita di kolom Pool.
3. Pilih Tetapkan ke kolam.
4. Dalam kotak dialog Tetapkan pita ke kumpulan, verifikasi kode batang untuk kaset yang Anda pindahkan dan pilih Tetapkan.

Note

Jika rekaman telah dikeluarkan oleh aplikasi cadangan dan diarsipkan dalam S3 Glacier Deep Archive, Anda tidak dapat memindahkannya kembali ke S3 Glacier Flexible Retrieval. Ada biaya untuk memindahkan kaset Anda dari S3 Glacier Flexible Retrieval ke S3 Glacier Deep Archive. Selain itu, jika Anda memindahkan kaset dari S3 Glacier Flexible Retrieval ke S3 Glacier Deep Archive sebelum 90 hari, ada biaya penghapusan awal untuk S3 Glacier Flexible Retrieval.

5. Setelah rekaman dipindahkan, Anda dapat melihat status yang diperbarui di kolom Pool pada halaman ikhtisar Tape.

Mengambil Kaset yang Diarsipkan

Untuk mengakses data yang disimpan pada rekaman virtual yang diarsipkan, Anda harus terlebih dahulu mengambil rekaman yang Anda inginkan ke Tape Gateway Anda. Tape Gateway Anda menyediakan satu pustaka pita virtual (VTL) untuk setiap gateway.

Jika Anda memiliki lebih dari satu Tape Gateway di sebuah Wilayah AWS, Anda dapat mengambil kaset ke hanya satu gateway.

Rekaman yang diambil dilindungi oleh tulisan, Anda hanya dapat membaca data pada rekaman itu.

Important


Jika Anda mengarsipkan kaset di S3 Glacier Flexible Retrieval, Anda dapat mengambil rekaman itu biasanya dalam waktu 3-5 jam. Jika Anda mengarsipkan rekaman itu di S3 Glacier Deep Archive, Anda dapat mengambilnya biasanya dalam waktu 12 jam.

Note

Ada biaya untuk mengambil kaset dari arsip. Untuk informasi harga terperinci, lihat [Harga Storage Gateway](#).

Untuk mengambil rekaman yang diarsipkan ke gateway Anda


1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.
3. Pilih pita virtual yang ingin Anda ambil dari tab Virtual Tape Shelf, dan pilih Ambil kaset.

 Note

Status rekaman virtual yang ingin Anda ambil harus diarsipkan.

4. Dalam kotak dialog Retrieve tape, untuk Barcode, verifikasi bahwa barcode mengidentifikasi pita virtual yang ingin Anda ambil.
5. Untuk Gateway, pilih gateway yang ingin Anda ambil rekaman yang diarsipkan, lalu pilih Ambil kaset.

Status rekaman berubah dari ARCHIVED ke RETRIEVING. Pada titik ini, data Anda sedang dipindahkan dari rak pita virtual (didukung oleh S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive) ke pustaka pita virtual (didukung oleh Amazon S3). Setelah semua data dipindahkan, status rekaman virtual dalam arsip berubah menjadi RETRIEVED.

 Note

Kaset virtual yang diambil hanya bisa dibaca.

Penggunaan Tape Melihat

Ketika Anda menulis data ke tape, Anda dapat melihat jumlah data yang disimpan pada tape di konsol Storage Gateway. Tab Detail untuk setiap rekaman menunjukkan informasi penggunaan rekaman.

Untuk melihat jumlah data yang disimpan pada kaset

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.
3. Pilih rekaman yang Anda minati.
4. Halaman yang muncul memberikan berbagai detail dan informasi tentang rekaman itu, termasuk yang berikut:
 - Ukuran: Total kapasitas pita yang dipilih.
 - Digunakan: Ukuran data yang ditulis ke rekaman oleh aplikasi cadangan Anda.

Note

Nilai ini tidak tersedia untuk kaset yang dibuat sebelum 13 Mei 2015.

Menghapus Kaset


Anda dapat menghapus kaset virtual dari Tape Gateway Anda dengan menggunakan konsol Storage Gateway.

Note

Jika rekaman yang ingin Anda hapus dari Tape Gateway Anda memiliki status RETRIEVED, Anda harus terlebih dahulu mengeluarkan kaset menggunakan aplikasi cadangan Anda sebelum menghapus kaset. Untuk petunjuk tentang cara mengeluarkan kaset menggunakan NetBackup perangkat lunak Symantec, lihat [Mengarsipkan](#) Tape. Setelah rekaman dikeluarkan, status rekaman berubah kembali ke ARCHIVED. Anda kemudian dapat menghapus rekaman itu.

Buat salinan data Anda sebelum Anda menghapus kaset Anda. Setelah Anda menghapus kaset, Anda tidak bisa mendapatkannya kembali.

Untuk menghapus rekaman virtual

 Warning

Prosedur ini secara permanen menghapus pita virtual yang dipilih.

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.
3. Pilih satu atau beberapa kaset untuk dihapus.
4. Untuk Tindakan pilih Hapus pita. Kotak dialog konfirmasi muncul.
5. Pastikan Anda ingin menghapus kaset yang ditentukan, lalu ketik kata hapus di kotak konfirmasi dan pilih Hapus.

Setelah rekaman itu dihapus, itu menghilang dari Tape Gateway.

Menghapus Kolam Pita Kustom


Anda dapat menghapus kumpulan pita khusus hanya jika tidak ada kaset yang diarsipkan di kolam, dan tidak ada kebijakan pembuatan pita otomatis yang dilampirkan ke kolam.

Untuk menghapus kumpulan pita kustom Anda

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Pools untuk melihat pool yang tersedia.
3. Pilih satu atau beberapa kumpulan rekaman untuk dihapus.

Jika Tape Count untuk kumpulan tape yang ingin Anda hapus adalah 0, dan jika tidak ada kebijakan pembuatan tape otomatis yang mereferensikan kumpulan pita kustom, Anda dapat menghapus kumpulan tersebut.

4. Pilih Hapus. Kotak dialog konfirmasi muncul.
5. Verifikasi bahwa Anda ingin menghapus kumpulan rekaman yang ditentukan, lalu ketik kata hapus di kotak konfirmasi dan pilih Hapus.

 Warning

Prosedur ini secara permanen menghapus kumpulan pita yang dipilih dan tidak dapat dibatalkan.

Setelah kumpulan rekaman dihapus, mereka menghilang dari perpustakaan kaset.

Menonaktifkan Tape Gateway Anda

Anda menonaktifkan Tape Gateway jika Tape Gateway gagal dan Anda ingin memulihkan kaset dari gateway yang gagal ke gateway lain.

Untuk memulihkan kaset, Anda harus terlebih dahulu menonaktifkan gateway yang gagal.

Menonaktifkan Tape Gateway mengunci kaset virtual di gateway itu. Artinya, data apa pun yang mungkin Anda tulis ke kaset ini setelah menonaktifkan gateway tidak dikirim ke AWS. Anda hanya dapat menonaktifkan gateway di konsol Storage Gateway jika gateway tidak lagi terhubung AWS. Jika gateway terhubung AWS, Anda tidak dapat menonaktifkan Tape Gateway.

Anda menonaktifkan Tape Gateway sebagai bagian dari pemulihan data. Untuk informasi lebih lanjut tentang memulihkan kaset, lihat [Anda Perlu Memulihkan Pita Virtual dari Gateway Tape yang Rusak](#)

Untuk menonaktifkan gateway Anda

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway yang gagal.
3. Pilih tab Detail untuk gateway untuk menampilkan pesan gateway nonaktifkan.
4. Pilih Buat kaset pemulihan.
5. Pilih Nonaktifkan gateway.

Memahami Status Pita

Setiap rekaman memiliki status terkait yang memberi tahu Anda sekilas tentang kesehatan rekaman itu. Sebagian besar waktu, status menunjukkan bahwa rekaman berfungsi normal dan tidak ada tindakan yang diperlukan di pihak Anda. Dalam beberapa kasus, status menunjukkan masalah dengan rekaman yang mungkin memerlukan tindakan di pihak Anda. Anda dapat menemukan informasi berikut untuk membantu Anda memutuskan kapan Anda perlu bertindak.


Topik

- [Memahami Informasi Status Tape dalam VTL](#)
- [Menentukan Status Tape dalam Arsip](#)

Memahami Informasi Status Tape dalam VTL

Status rekaman harus TERSEDIA bagi Anda untuk membaca atau menulis ke rekaman itu. Tabel berikut mencantumkan dan menjelaskan kemungkinan nilai status.

Status	Deskripsi	Data Tape Disimpan Di
SEDANG MEMBUAT	Rekaman virtual sedang dibuat. Rekaman itu tidak dapat dimuat ke dalam tape drive, karena rekaman itu sedang dibuat.	—
TERSEDIA	Pita virtual dibuat dan siap dimuat ke dalam tape drive.	Amazon S3
DALAM PERJALANAN KE VTS	Rekaman virtual telah dikeluarkan dan sedang diunggah untuk arsip. Pada titik ini, Tape Gateway Anda mengunggah data ke AWS. Jika jumlah data yang diunggah kecil, status ini mungkin tidak muncul. Saat unggahan selesai, status berubah menjadi PENGARSIPAN.	Amazon S3
PENGARSIPAN	Rekaman virtual sedang dipindahkan oleh Tape Gateway Anda ke arsip, yang didukung oleh S3 Glacier Flexible Retrieval atau S3 Glacier Deep	Data sedang dipindahkan dari Amazon S3 ke S3 Glacier Flexible Retrieval

Status	Deskripsi	Data Tape Disimpan Di
	Archive. Proses ini terjadi setelah pengunggahan data AWS selesai.	atau S3 Glacier Deep Archive.
SEDANG MENGHAPUS	Rekaman virtual sedang dihapus.	Data sedang dihapus dari Amazon S3
DIHAPUS	Rekaman virtual telah berhasil dihapus.	—
MENGAMBIL	<p>Rekaman virtual sedang diambil dari arsip ke Tape Gateway Anda.</p> <div data-bbox="354 709 391 747" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; display: inline-block; margin-bottom: 5px;">  </div> <p>Note Rekaman virtual hanya dapat diambil ke Tape Gateway.</p>	Data sedang dipindahkan dari S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive ke Amazon S3
MENGAMBIL KEMBALI	Rekaman virtual diambil dari arsip. Rekaman yang diambil dilindungi oleh tulisan.	Amazon S3
PULIH	<p>Rekaman virtual dipulihkan dan hanya-baca.</p> <p>Ketika Tape Gateway Anda tidak dapat diakses karena alasan apa pun, Anda dapat memulihkan kaset virtual yang terkait dengan Tape Gateway itu ke Tape Gateway lain. Untuk memulihkan kaset virtual, pertama-tama nonaktifkan Tape Gateway yang tidak dapat diakses.</p>	Amazon S3
TIDAK DAPAT DIPULIHKAN	Rekaman virtual tidak dapat dibaca atau ditulis. Status ini menunjukkan kesalahan di Tape Gateway Anda.	Amazon S3

Menentukan Status Tape dalam Arsip


Anda dapat menggunakan prosedur berikut untuk menentukan status rekaman virtual dalam arsip.

Untuk menentukan status rekaman virtual

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Kaset.
3. Di kolom Status dari kisi perpustakaan pita, periksa status rekaman itu.

Status rekaman juga muncul di tab Detail dari setiap rekaman virtual.

Berikut ini, Anda dapat menemukan deskripsi nilai status yang mungkin.

Status	Deskripsi
DIARSIPKAN	Rekaman virtual telah dikeluarkan dan diunggah ke arsip.
MENGAMBIL	Rekaman virtual sedang diambil dari arsip. <div data-bbox="402 892 1507 1066"><p> Note Rekaman virtual hanya dapat diambil ke Tape Gateway.</p></div>
MENGAMBIL KEMBALI	Rekaman virtual telah diambil dari arsip. Rekaman yang diambil hanya baca.


Untuk informasi tambahan tentang cara bekerja dengan kaset dan perangkat VTL, lihat. [Bekerja Dengan Kaset](#)

Memindahkan data Anda ke gateway baru

Anda dapat memindahkan data antar gateway saat data dan kebutuhan kinerja bertambah, atau jika Anda menerima AWS pemberitahuan untuk memigrasi gateway Anda. Berikut ini adalah beberapa alasan untuk melakukan ini:

- Pindahkan data Anda ke platform host yang lebih baik atau instans Amazon EC2 yang lebih baru.
- Segarkan perangkat keras yang mendasarinya untuk server Anda.

Langkah-langkah yang Anda ikuti untuk memindahkan data Anda ke gateway baru bergantung pada jenis gateway yang Anda miliki.

 Note

Data hanya dapat dipindahkan di antara jenis gateway yang sama.

Memindahkan kaset virtual ke Tape Gateway baru

Untuk memindahkan rekaman virtual Anda ke Tape Gateway baru

1. Gunakan aplikasi cadangan Anda untuk mencadangkan semua data Anda ke pita virtual. Tunggu pencadangan selesai dengan sukses.
2. Gunakan aplikasi cadangan Anda untuk mengeluarkan kaset Anda. Rekaman itu akan disimpan di salah satu kelas penyimpanan Amazon S3. Kaset yang dikeluarkan diarsipkan dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive, dan hanya-baca.

Sebelum melanjutkan, konfirmasikan bahwa kaset yang dikeluarkan telah diarsipkan:

- a. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
- b. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.
- c. Di kolom Status daftar, periksa status rekaman itu.

Status rekaman juga muncul di tab Detail dari setiap rekaman virtual.

Untuk informasi selengkapnya tentang menentukan status rekaman dalam arsip, lihat [Menentukan Status Tape dalam Arsip](#).

3. Dengan menggunakan aplikasi cadangan Anda, verifikasi bahwa tidak ada pekerjaan pencadangan aktif yang masuk ke Tape Gateway yang ada sebelum Anda menghentikannya.

Jika ada pekerjaan pencadangan aktif, tunggu sampai selesai dan keluarkan kaset Anda (lihat langkah sebelumnya) sebelum menghentikan gateway.

4. Gunakan langkah-langkah berikut untuk menghentikan Tape Gateway yang ada:
 - a. Di panel navigasi, pilih Gateway, lalu pilih Tape Gateway lama yang ingin Anda hentikan. Status gateway adalah Running.
 - b. Untuk Tindakan, pilih Stop gateway. Verifikasi ID gateway dari kotak dialog, lalu pilih Stop gateway.


Saat Tape Gateway lama berhenti, Anda mungkin melihat pesan yang menunjukkan status gateway. Ketika gateway dimatikan, pesan dan tombol Start gateway muncul di tab Detail.

Untuk informasi selengkapnya tentang menghentikan gateway, lihat [Memulai dan Menghentikan Tape Gateway](#).

5. Buat Tape Gateway baru. Untuk petunjuk mendetail, lihat [Membuat Gateway](#).
6. Gunakan langkah-langkah berikut untuk membuat kaset baru:
 - a. Di panel navigasi, pilih tab Gateways.
 - b. Pilih Buat pita untuk membuka kotak dialog Buat pita.
 - c. Untuk Gateway, pilih gateway. Rekaman itu dibuat untuk gateway ini.
 - d. Untuk Jumlah kaset, pilih jumlah kaset yang ingin Anda buat. Untuk informasi selengkapnya tentang batas rekaman, lihat [AWS Storage Gateway kuota](#).

Anda juga dapat mengatur pembuatan pita otomatis pada saat ini. Untuk informasi selengkapnya, lihat [Membuat Kaset Secara Otomatis](#).

- e. Untuk Kapasitas, masukkan ukuran pita virtual yang ingin Anda buat. Kaset harus lebih besar dari 100 GiB. Untuk informasi tentang batas kapasitas, lihat [AWS Storage Gateway kuota](#).
- f. Untuk awalan Barcode, masukkan awalan yang ingin Anda tambahkan ke barcode kaset virtual Anda.

 Note

Kaset virtual diidentifikasi secara unik oleh kode batang. Anda dapat menambahkan awalan ke barcode. Awalan adalah opsional, tetapi Anda dapat menggunakannya


untuk membantu mengidentifikasi kaset virtual Anda. Awalan harus huruf besar (A-Z) dan harus satu sampai empat karakter panjang.

- g. Untuk Pool, pilih Glacier Pool atau Deep Archive Pool. Kumpulan ini mewakili kelas penyimpanan di mana rekaman Anda akan disimpan ketika dikeluarkan oleh perangkat lunak cadangan Anda.

Pilih Glacier Pool jika Anda ingin mengarsipkan rekaman di S3 Glacier Flexible Retrieval. Ketika perangkat lunak cadangan Anda mengeluarkan rekaman, itu secara otomatis diarsipkan dalam S3 Glacier Flexible Retrieval. Anda menggunakan S3 Glacier Flexible Retrieval untuk arsip yang lebih aktif di mana Anda dapat mengambil kaset biasanya dalam waktu 3-5 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Pilih Deep Archive Pool jika Anda ingin mengarsipkan rekaman di S3 Glacier Deep Archive. Saat perangkat lunak cadangan Anda mengeluarkan kaset, rekaman itu secara otomatis diarsipkan di S3 Glacier Deep Archive. Anda menggunakan S3 Glacier Deep Archive untuk retensi data jangka panjang dan pelestarian digital di mana data diakses sekali atau dua kali setahun. Anda dapat mengambil rekaman yang diarsipkan di S3 Glacier Deep Archive biasanya dalam waktu 12 jam. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengarsipkan objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.


Jika Anda mengarsipkan kaset di S3 Glacier Flexible Retrieval, Anda dapat memindahkannya ke S3 Glacier Deep Archive nanti. Untuk informasi selengkapnya, lihat [Memindahkan Tape Anda dari Pengambilan Fleksibel Gletser S3 ke Kelas Penyimpanan S3 Glacier Deep Archive](#).

 Note

Kaset yang dibuat sebelum 27 Maret 2019, diarsipkan langsung di S3 Glacier Flexible Retrieval saat perangkat lunak cadangan Anda mengeluarkannya.


- h. (Opsional) Untuk Tag, masukkan kunci dan nilai untuk menambahkan tag ke rekaman Anda. Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengelola, memfilter, dan mencari kaset Anda.
- i. Pilih Buat kaset.

7. Gunakan aplikasi cadangan Anda untuk memulai pekerjaan pencadangan, dan buat cadangan data Anda ke rekaman baru.
8. (Opsional) Jika rekaman Anda diarsipkan dan Anda perlu memulihkan data darinya, ambil kembali ke Tape Gateway baru. Rekaman itu akan berada dalam mode hanya-baca. Untuk informasi selengkapnya tentang mengambil kaset yang diarsipkan, lihat. [Mengambil Kaset yang Diarsipkan](#)

 Note

Biaya data keluar mungkin berlaku.


- a. Di panel navigasi, pilih Tape Library > Tapes untuk melihat kaset Anda. Secara default, daftar ini menampilkan hingga 1.000 kaset sekaligus, tetapi penelusuran yang Anda lakukan berlaku untuk semua kaset Anda. Anda dapat menggunakan bilah pencarian untuk menemukan kaset yang cocok dengan kriteria tertentu, atau untuk mengurangi daftar menjadi kurang dari 1.000 kaset. Ketika daftar Anda berisi 1.000 kaset atau kurang, Anda kemudian dapat mengurutkan kaset Anda dalam urutan naik atau turun berdasarkan berbagai properti.
- b. Pilih rekaman virtual yang ingin Anda ambil. Untuk Tindakan, pilih Ambil Tape.

 Note

Status rekaman virtual yang ingin Anda ambil harus ARCHIVED.


- c. Dalam kotak dialog Retrieve tape, untuk Barcode, verifikasi bahwa barcode mengidentifikasi pita virtual yang ingin Anda ambil.
- d. Untuk Gateway, pilih Tape Gateway baru yang ingin Anda ambil rekaman yang diarsipkan, lalu pilih Ambil kaset.

Ketika Anda telah mengonfirmasi bahwa Tape Gateway baru Anda berfungsi dengan benar, Anda dapat menghapus Tape Gateway lama.

 Important

Sebelum Anda menghapus gateway, pastikan tidak ada aplikasi yang saat ini menulis ke volume gateway itu. Jika Anda menghapus gateway saat sedang digunakan, kehilangan data dapat terjadi.

9. Gunakan langkah-langkah berikut untuk menghapus Tape Gateway lama:

 Warning

Ketika gateway dihapus, tidak ada cara untuk memulihkannya.

- a. Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda hapus.
- b. Untuk Tindakan, pilih Hapus gateway.

Di kotak dialog konfirmasi yang muncul, pastikan ID gateway yang tercantum menentukan Gateway Tape lama yang ingin Anda hapus, masukkan **delete** di bidang konfirmasi, lalu pilih Hapus.

- c. Hapus VM. Untuk informasi selengkapnya tentang menghapus VM, lihat dokumentasi untuk hypervisor Anda.

Memantau Storage Gateway

Bagian ini menjelaskan cara memantau gateway, termasuk memantau sumber daya yang terkait dengan gateway, menggunakan Amazon CloudWatch. Anda dapat memantau buffer unggahan gateway dan penyimpanan cache. Anda menggunakan konsol Storage Gateway untuk melihat metrik dan alarm untuk gateway Anda. Misalnya, Anda dapat melihat jumlah byte yang digunakan dalam operasi baca dan tulis, waktu yang dihabiskan dalam operasi baca dan tulis, dan waktu yang dibutuhkan untuk mengambil data dari Amazon Web Services Cloud. Dengan metrik, Anda dapat melacak kesehatan gateway Anda dan mengatur alarm untuk memberi tahu Anda ketika satu atau beberapa metrik berada di luar ambang batas yang ditentukan.

Storage Gateway menyediakan CloudWatch metrik tanpa biaya tambahan. Metrik Storage Gateway dicatat untuk jangka waktu dua minggu. Dengan menggunakan metrik ini, Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang kinerja gateway dan volume Anda. Storage Gateway juga menyediakan CloudWatch alarm, kecuali alarm resolusi tinggi, tanpa biaya tambahan. Untuk informasi selengkapnya tentang CloudWatch harga, lihat [CloudWatch harga Amazon](#). Untuk informasi selengkapnya CloudWatch, lihat [Panduan CloudWatch Pengguna Amazon](#).


Topik

- [Memahami metrik gateway](#)
- [Dimensi untuk metrik Storage Gateway](#)
- [Memantau buffer unggahan](#)
- [Memantau penyimpanan cache](#)
- [Memahami CloudWatch alarm](#)
- [Membuat CloudWatch alarm yang direkomendasikan untuk gateway Anda](#)
- [Membuat CloudWatch alarm khusus untuk gateway Anda](#)
- [Memantau Tape Gateway Anda](#)

Memahami metrik gateway

Untuk diskusi dalam topik ini, kami mendefinisikan metrik gateway sebagai metrik yang dicakup ke gateway — yaitu, mereka mengukur sesuatu tentang gateway. Karena gateway berisi satu atau beberapa volume, metrik khusus gateway mewakili semua volume di gateway. Misalnya, `CloudBytesUploaded` metrik adalah jumlah total byte yang dikirim gateway ke cloud selama periode pelaporan. Metrik ini mencakup aktivitas semua volume di gateway.

Saat bekerja dengan data metrik gateway, Anda menentukan identifikasi unik gateway yang Anda minati untuk melihat metrik. Untuk melakukan ini, Anda menentukan nilai GatewayId dan GatewayName nilai. Bila Anda ingin bekerja dengan metrik untuk gateway, Anda menentukan dimensi gateway di namespace metrik, yang membedakan metrik khusus gateway dari metrik spesifik volume. Untuk informasi selengkapnya, lihat [Menggunakan Metrik CloudWatch Amazon](#).

 Note

Beberapa metrik mengembalikan titik data hanya ketika data baru telah dihasilkan selama periode pemantauan terbaru.

Metrik	Deskripsi
AvailabilityNotifications	<p>Jumlah pemberitahuan kesehatan terkait ketersediaan yang dihasilkan oleh gateway.</p> <p>Gunakan metrik ini dengan Sum statistik untuk mengamati apakah gateway mengalami peristiwa terkait ketersediaan. Untuk detail tentang peristiwa, periksa grup CloudWatch log yang dikonfigurasi.</p> <p>Satuan: Jumlah</p>
CacheHitPercent	<p>Persentase pembacaan aplikasi disajikan dari cache. Sampel diambil pada akhir periode pelaporan.</p> <p>Unit: Persen</p>
CacheUsed	<p>Jumlah total byte yang digunakan dalam penyimpanan cache gateway. Sampel</p>

Metrik	Deskripsi	
	diambil pada akhir periode pelaporan. Unit: Bit	
IoWaitPercent	Persentase waktu gateway menunggu respons dari disk lokal. Unit: Persen	
MemTotalBytes	Jumlah RAM yang disediakan ke VM gateway, dalam byte. Unit: Bit	
MemUsedBytes	Jumlah RAM yang saat ini digunakan oleh gateway VM, dalam byte. Unit: Bit	
QueuedWrites	Jumlah byte yang menunggu untuk ditulis AWS, diambil sampelnya pada akhir periode pelaporan untuk semua volume di gateway. Byte ini disimpan di penyimpanan kerja gateway Anda. Unit: Bit	
TotalCacheSize	Ukuran total cache dalam byte. Sampel diambil pada akhir periode pelaporan. Unit: Bit	

Metrik	Deskripsi
<code>UploadBufferPercentUsed</code>	<p>Persentase penggunaan buffer unggahan gateway. Sampel diambil pada akhir periode pelaporan.</p> <p>Unit: Persen</p>
<code>UploadBufferUsed</code>	<p>Jumlah total byte yang digunakan dalam buffer upload gateway. Sampel diambil pada akhir periode pelaporan.</p> <p>Unit: Bit</p>
<code>UserCpuPercent</code>	<p>Persentase waktu CPU yang dihabiskan untuk pemrosesan gateway, dirata-ratakan di semua core.</p> <p>Unit: Persen</p>

Dimensi untuk metrik Storage Gateway

CloudWatch Namespace untuk layanan Storage Gateway adalah `AWS/StorageGateway` Data tersedia secara otomatis dalam periode 5 menit tanpa biaya.

Dimensi	Deskripsi
<code>GatewayId</code> , <code>GatewayName</code>	<p>Dimensi ini memfilter data yang Anda minta ke metrik khusus gateway. Anda dapat mengidentifikasi gateway untuk bekerja berdasarkan nilai untuk <code>GatewayId</code> atau <code>GatewayName</code> . Jika nama gateway Anda berbeda untuk rentang waktu yang Anda minati untuk melihat metrik, gunakan <code>GatewayId</code></p>

Dimensi	Deskripsi
	Data throughput dan latensi gateway didasarkan pada semua volume untuk gateway. Untuk informasi tentang bekerja dengan metrik gateway, lihat Mengukur Kinerja Antara Gateway Anda dan AWS .

Memantau buffer unggahan

Anda dapat menemukan informasi berikut tentang cara memantau buffer unggahan gateway dan cara membuat alarm sehingga Anda mendapatkan pemberitahuan ketika buffer melebihi ambang batas yang ditentukan. Dengan menggunakan pendekatan ini, Anda dapat menambahkan penyimpanan buffer ke gateway sebelum terisi sepenuhnya dan aplikasi penyimpanan Anda berhenti mencadangkan. AWS

Anda memantau buffer unggahan dengan cara yang sama di arsitektur volume cache dan Tape Gateway. Untuk informasi selengkapnya, lihat [Cara kerja Tape Gateway \(arsitektur\)](#).

Note

`WorkingStorageFree` Metrik `WorkingStoragePercentUsed` `WorkingStorageUsed`, dan mewakili buffer unggahan untuk volume tersimpan hanya sebelum rilis fitur volume cache di Storage Gateway. Sekarang, gunakan metrik buffer upload yang setara `UploadBufferPercentUsed`, `UploadBufferUsed`, dan `UploadBufferFree`. Metrik ini berlaku untuk kedua arsitektur gateway.

Item yang menarik	Cara Mengukur
Unggah pengguna n buffer	Gunakan <code>UploadBufferPercentUsed</code> , <code>UploadBufferUsed</code> , dan <code>UploadBufferFree</code> metrik dengan Average statistik. Misalnya, gunakan <code>UploadBufferUsed</code> dengan Average statistik untuk menganalisis penggunaan penyimpanan selama periode waktu tertentu.

Untuk mengukur persentase buffer upload yang digunakan

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih dimensi StorageGateway: Gateway Metrics, dan temukan gateway yang ingin Anda gunakan.
3. Pilih UploadBufferPercentUsed metrik.
4. Untuk Rentang Waktu, pilih nilai.
5. Pilih Average statistiknya.
6. Untuk Periode, pilih nilai 5 menit agar sesuai dengan waktu pelaporan default.

Kumpulan titik data yang diurutkan waktu yang dihasilkan berisi persen yang digunakan dari buffer unggahan.

Dengan menggunakan prosedur berikut, Anda dapat membuat alarm menggunakan CloudWatch konsol. Untuk mempelajari lebih lanjut tentang alarm dan ambang batas, lihat [Membuat CloudWatch Alarm di Panduan Pengguna](#) Amazon. CloudWatch

Untuk menyetel alarm ambang batas atas untuk buffer unggahan gateway

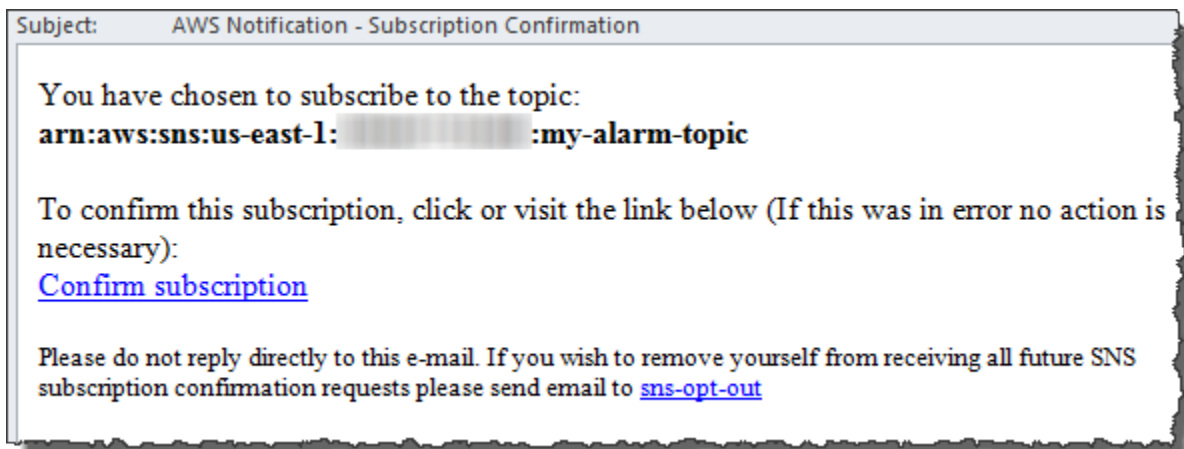
1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih Buat Alarm untuk memulai wizard Buat Alarm.
3. Tentukan metrik untuk alarm Anda:
 - a. Pada halaman Select Metric dari wizard Create Alarm GatewayId, pilih GatewayName dimensi AWS/StorageGateway:, lalu temukan gateway yang ingin Anda gunakan.
 - b. Pilih UploadBufferPercentUsed metrik. Gunakan Average statistik dan jangka waktu 5 menit.
 - c. Pilih Lanjutkan.
4. Tentukan nama alarm, deskripsi, dan ambang batas:
 - a. Pada halaman Tentukan Alarm dari wizard Buat Alarm, identifikasi alarm Anda dengan memberinya nama dan deskripsi di kotak Nama dan Deskripsi.
 - b. Tentukan ambang alarm.
 - c. Pilih Lanjutkan.
5. Konfigurasi tindakan email untuk alarm:

- a. Pada halaman Konfigurasi Tindakan dari wizard Buat Alarm, pilih Alarm untuk Status Alarm.
- b. Pilih Pilih atau buat topik email untuk Topik.

Untuk membuat topik email berarti Anda menyiapkan topik Amazon SNS. Untuk informasi selengkapnya tentang Amazon SNS, lihat [Mengatur Amazon SNS](#) di Panduan Pengguna Amazon CloudWatch .

- c. Untuk Topik, masukkan nama deskriptif untuk topik tersebut.
 - d. Pilih Tambahkan Tindakan.
 - e. Pilih Lanjutkan.
6. Tinjau pengaturan alarm, lalu buat alarm:
 - a. Pada halaman Tinjauan wizard Buat Alarm, tinjau definisi alarm, metrik, dan tindakan terkait yang akan diambil (misalnya, mengirim pemberitahuan email).
 - b. Setelah meninjau ringkasan alarm, pilih Simpan Alarm.
 7. Konfirmasikan langganan Anda ke topik alarm:
 - a. Buka email Amazon SNS yang dikirim ke alamat email yang Anda tentukan saat membuat topik.

Gambar berikut menunjukkan pemberitahuan email khas.



- b. Konfirmasikan langganan Anda dengan mengklik tautan di email.

Konfirmasi berlangganan muncul.

Memantau penyimpanan cache

Anda dapat menemukan informasi berikut tentang cara memantau penyimpanan cache gateway dan cara membuat alarm sehingga Anda mendapatkan pemberitahuan ketika parameter cache melewati ambang batas yang ditentukan. Dengan menggunakan alarm ini, Anda tahu kapan harus menambahkan penyimpanan cache ke gateway.

Anda hanya memantau penyimpanan cache dalam arsitektur volume cache. Untuk informasi selengkapnya, lihat [Cara kerja Tape Gateway \(arsitektur\)](#).

Item yang menarik	Cara Mengukur
Total penggunaan cache	<p>Gunakan <code>CachePercentUsed</code> dan <code>TotalCacheSize</code> metrik dengan <code>Average</code> statistik. Misalnya, gunakan <code>CachePercentUsed</code> dengan <code>Average</code> statistik untuk menganalisis penggunaan cache selama periode waktu tertentu.</p> <p><code>TotalCacheSize</code> Metrik berubah hanya ketika Anda menambahkan cache ke gateway.</p>
Persentase permintaan baca yang disajikan dari cache	<p>Gunakan <code>CacheHitPercent</code> metrik dengan <code>Average</code> statistik.</p> <p>Biasanya, Anda <code>CacheHitPercent</code> ingin tetap tinggi.</p>
Persentase cache yang kotor—yaitu, berisi konten yang belum diunggah AWS	<p>Gunakan <code>CachePercentDirty</code> metrik dengan <code>Average</code> statistik.</p> <p>Biasanya, Anda <code>CachePercentDirty</code> ingin tetap rendah.</p>

Untuk mengukur persentase cache yang kotor untuk gateway dan semua volumenya

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih dimensi StorageGateway: Gateway Metrics, dan temukan gateway yang ingin Anda gunakan.
3. Pilih `CachePercentDirty` metrik.
4. Untuk Rentang Waktu, pilih nilai.

5. Pilih Average statistiknya.
6. Untuk Periode, pilih nilai 5 menit agar sesuai dengan waktu pelaporan default.

Kumpulan titik data yang diurutkan waktu yang dihasilkan berisi persentase cache yang kotor selama 5 menit.

Untuk mengukur persentase cache yang kotor untuk volume

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih dimensi StorageGateway: Volume Metrics, dan temukan volume yang ingin Anda kerjakan.
3. Pilih CachePercentDirty metrik.
4. Untuk Rentang Waktu, pilih nilai.
5. Pilih Average statistiknya.
6. Untuk Periode, pilih nilai 5 menit agar sesuai dengan waktu pelaporan default.

Kumpulan titik data yang diurutkan waktu yang dihasilkan berisi persentase cache yang kotor selama 5 menit.

Memahami CloudWatch alarm


CloudWatch alarm memantau informasi tentang gateway Anda berdasarkan metrik dan ekspresi. Anda dapat menambahkan CloudWatch alarm untuk gateway dan melihat statusnya di konsol Storage Gateway. Untuk setiap alarm, Anda menentukan kondisi yang akan memulai status ALARM. Indikator status alarm di konsol Storage Gateway berubah menjadi merah saat dalam status ALARM, sehingga memudahkan Anda untuk memantau status secara proaktif. Anda dapat mengonfigurasi alarm untuk menjalankan tindakan secara otomatis berdasarkan perubahan status yang berkelanjutan. Untuk informasi selengkapnya tentang CloudWatch alarm, lihat [Menggunakan CloudWatch alarm Amazon](#) di CloudWatch Panduan Pengguna Amazon.

Note

Jika Anda tidak memiliki izin untuk melihat CloudWatch, Anda tidak dapat melihat alarm.

Untuk setiap gateway yang diaktifkan, kami sarankan Anda membuat CloudWatch alarm berikut:

- Tunggu IO tinggi: `IoWaitpercent` ≥ 20 untuk 3 titik data dalam 15 menit
- Cache persen kotor: `CachePercentDirty` > 80 untuk 4 titik data dalam waktu 20 menit
- Pemberitahuan Kesehatan: `HealthNotifications` ≥ 1 untuk 1 titik data dalam 5 menit. Saat mengonfigurasi alarm ini, atur Perlakuan data hilang ke `NotBreaching`.

 Note

Anda dapat mengatur alarm pemberitahuan kesehatan hanya jika gateway memiliki pemberitahuan kesehatan sebelumnya CloudWatch.

Untuk gateway pada platform host VMware dengan mode HA diaktifkan, kami juga merekomendasikan alarm tambahan ini: CloudWatch

- Pemberitahuan ketersediaan: `AvailabilityNotifications` ≥ 1 untuk 1 titik data dalam waktu 5 menit. Saat mengonfigurasi alarm ini, atur Perlakuan data hilang ke `NotBreaching`.

Tabel berikut menjelaskan keadaan alarm.

Status	Deskripsi
OK	Metrik atau ekspresi berada dalam ambang batas yang ditentukan.
Alarm	Metrik atau ekspresi berada di luar ambang batas yang ditentukan.
Data tidak mencukupi	Alarm baru saja dimulai, metrik tidak tersedia, atau tidak cukup data tersedia untuk metrik untuk menentukan status alarm.
Tidak ada	Tidak ada alarm yang dibuat untuk gateway. Untuk membuat alarm baru, lihat Membuat CloudWatch alarm khusus untuk gateway Anda .

Status	Deskripsi
Tidak tersedia	Keadaan alarm tidak diketahui. Pilih Tidak tersedia untuk melihat informasi kesalahan di tab Monitoring.

Membuat CloudWatch alarm yang direkomendasikan untuk gateway Anda

Saat membuat gateway baru menggunakan konsol Storage Gateway, Anda dapat memilih untuk membuat semua CloudWatch alarm yang direkomendasikan secara otomatis sebagai bagian dari proses penyiapan awal. Untuk informasi selengkapnya, lihat [Mengonfigurasi Gateway Tape Mengkonfigurasi Gateway](#). Jika Anda ingin menambahkan atau memperbarui CloudWatch alarm yang direkomendasikan untuk gateway yang ada, gunakan prosedur berikut.

Untuk menambah atau memperbarui CloudWatch alarm yang disarankan untuk gateway yang ada

Note

Fitur ini memerlukan izin CloudWatch kebijakan, yang tidak secara otomatis diberikan sebagai bagian dari kebijakan akses penuh Storage Gateway yang telah dikonfigurasi sebelumnya. Pastikan kebijakan keamanan Anda memberikan izin berikut sebelum Anda mencoba membuat alarm yang direkomendasikan CloudWatch :

- `cloudwatch:PutMetricAlarm`- buat alarm
- `cloudwatch:DisableAlarmActions`- matikan tindakan alarm
- `cloudwatch:EnableAlarmActions`- Aktifkan tindakan alarm
- `cloudwatch>DeleteAlarms`- Hapus alarm

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home/>.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda buat alarm yang direkomendasikan. CloudWatch
3. Pada halaman detail gateway, pilih tab Pemantauan.

4. Di bawah Alarm, pilih Buat alarm yang direkomendasikan. Alarm yang disarankan dibuat secara otomatis.

Bagian Alarm mencantumkan semua CloudWatch alarm untuk gateway tertentu. Dari sini, Anda dapat memilih dan menghapus satu atau beberapa alarm, mengaktifkan atau menonaktifkan tindakan alarm, dan membuat alarm baru.

Membuat CloudWatch alarm khusus untuk gateway Anda

CloudWatch menggunakan Amazon Simple Notification Service (Amazon SNS) untuk mengirim notifikasi alarm saat alarm berubah status. Alarm mengawasi satu metrik selama periode waktu yang Anda tentukan, dan melakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakan ini adalah pemberitahuan yang dikirim ke topik Amazon SNS. Anda dapat membuat topik Amazon SNS saat membuat CloudWatch alarm. Untuk informasi selengkapnya tentang Amazon SNS, lihat [Apa itu Amazon SNS?](#) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Untuk membuat CloudWatch alarm di konsol Storage Gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home/>.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda buat alarm.
3. Pada halaman detail gateway, pilih tab Pemantauan.
4. Di bawah Alarm, pilih Buat alarm untuk membuka CloudWatch konsol.
5. Gunakan CloudWatch konsol untuk membuat jenis alarm yang Anda inginkan. Anda dapat membuat jenis alarm berikut:
 - Alarm ambang statis: Alarm berdasarkan ambang batas yang ditetapkan untuk metrik yang dipilih. Alarm memasuki status ALARM ketika metrik melanggar ambang batas untuk sejumlah periode evaluasi tertentu.

Untuk membuat alarm ambang statis, lihat [Membuat CloudWatch alarm berdasarkan ambang batas statis](#) di Panduan CloudWatch Pengguna Amazon.

- Alarm deteksi anomali: Deteksi anomali menambang data metrik masa lalu dan menciptakan model nilai yang diharapkan. Anda menetapkan nilai untuk ambang deteksi anomali, dan CloudWatch menggunakan ambang batas ini dengan model untuk menentukan rentang nilai "normal" untuk metrik. Nilai yang lebih tinggi untuk ambang batas akan menghasilkan pita yang lebih tebal dari nilai "normal". Anda dapat memilih untuk mengaktifkan alarm hanya ketika nilai

metrik berada di atas pita nilai yang diharapkan, hanya ketika itu di bawah band, atau ketika itu di atas atau di bawah band.

Untuk membuat alarm deteksi anomali, lihat [Membuat CloudWatch alarm berdasarkan deteksi anomali di Panduan Pengguna](#) Amazon. CloudWatch

- Alarm ekspresi matematika metrik: Alarm berdasarkan satu atau lebih metrik yang digunakan dalam ekspresi matematika. Anda menentukan ekspresi, ambang batas, dan periode evaluasi.

Untuk membuat alarm ekspresi matematika metrik, lihat [Membuat CloudWatch alarm berdasarkan ekspresi matematika metrik](#) di Panduan CloudWatch Pengguna Amazon.

- Alarm komposit: Alarm yang menentukan status alarmnya dengan menonton status alarm alarm lainnya. Alarm komposit dapat membantu Anda mengurangi kebisingan alarm.

Untuk membuat alarm komposit, lihat [Membuat alarm komposit](#) di Panduan CloudWatch Pengguna Amazon.

6. Setelah Anda membuat alarm di CloudWatch konsol, kembali ke konsol Storage Gateway. Anda dapat melihat alarm dengan melakukan salah satu hal berikut:

- Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda lihat alarm. Pada tab Detail, di bawah Alarm, pilih CloudWatch Alarm.
- Di panel navigasi, pilih Gateway, pilih gateway yang ingin Anda lihat alarm, lalu pilih tab Monitoring.

Bagian Alarm mencantumkan semua CloudWatch alarm untuk gateway tertentu. Dari sini, Anda dapat memilih dan menghapus satu atau beberapa alarm, mengaktifkan atau menonaktifkan tindakan alarm, dan membuat alarm baru.

- Di panel navigasi, pilih Gateway, lalu pilih status alarm gateway yang ingin Anda lihat alarm.

Untuk informasi tentang cara mengedit atau menghapus alarm, lihat [Mengedit atau menghapus CloudWatch alarm](#).

Note

Saat Anda menghapus gateway menggunakan konsol Storage Gateway, semua CloudWatch alarm yang terkait dengan gateway juga akan dihapus secara otomatis.

Memantau Tape Gateway Anda

Bagian ini menjelaskan cara memantau Tape Gateway, kaset virtual yang terkait dengan Tape Gateway, penyimpanan cache, dan buffer unggahan. Anda menggunakan metrik AWS Management Console untuk melihat untuk Tape Gateway Anda. Dengan metrik, Anda dapat melacak kesehatan Tape Gateway dan mengatur alarm untuk memberi tahu Anda ketika satu atau beberapa metrik berada di luar ambang batas yang ditentukan.

Storage Gateway menyediakan CloudWatch metrik tanpa biaya tambahan. Metrik Storage Gateway dicatat untuk jangka waktu dua minggu. Dengan menggunakan metrik ini, Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang kinerja Tape Gateway dan kaset virtual Anda. Untuk informasi selengkapnya CloudWatch, lihat [Panduan CloudWatch Pengguna Amazon](#).

Topik

- [Mendapatkan Log Kesehatan Tape Gateway dengan Grup CloudWatch Log](#)
- [Menggunakan Metrik CloudWatch Amazon](#)
- [Memahami Metrik Pita Virtual](#)
- [Mengukur Kinerja Antara Tape Gateway Anda dan AWS](#)

Mendapatkan Log Kesehatan Tape Gateway dengan Grup CloudWatch Log

Anda dapat menggunakan Amazon CloudWatch Logs untuk mendapatkan informasi tentang kesehatan Tape Gateway Anda dan sumber daya terkait. Anda dapat menggunakan log untuk memantau gateway Anda untuk kesalahan yang ditemuinya. Selain itu, Anda dapat menggunakan filter CloudWatch langganan Amazon untuk mengotomatiskan pemrosesan informasi log secara real time. Untuk informasi selengkapnya, lihat [Pemrosesan Data Log Secara Real-time dengan Langganan](#) di Panduan CloudWatch Pengguna Amazon.

Misalnya, misalkan gateway Anda digunakan di cluster yang diaktifkan dengan VMware HA dan Anda perlu tahu tentang kesalahan apa pun. Anda dapat mengonfigurasi grup CloudWatch log untuk memantau gateway Anda dan mendapatkan pemberitahuan saat gateway Anda menemukan kesalahan. Anda dapat mengonfigurasi grup saat Anda mengaktifkan gateway atau setelah gateway Anda diaktifkan dan aktif dan berjalan. Untuk informasi tentang cara mengonfigurasi grup CloudWatch log saat mengaktifkan gateway, lihat [Mengonfigurasi Gateway Tape Anda](#). Untuk informasi umum tentang grup CloudWatch log, lihat [Bekerja dengan Grup Log dan Aliran Log](#) di Panduan CloudWatch Pengguna Amazon.

Untuk informasi tentang cara memecahkan masalah dan memperbaiki jenis kesalahan ini, lihat.

[Memecahkan masalah rekaman virtual](#)

Prosedur berikut menunjukkan kepada Anda cara mengonfigurasi grup CloudWatch log setelah gateway Anda diaktifkan.

Untuk mengonfigurasi Grup CloudWatch Log agar bekerja dengan File Gateway Anda

1. Masuk ke AWS Management Console dan buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda konfigurasi untuk Grup CloudWatch Log.
3. Untuk Tindakan, pilih Edit informasi gateway atau pada tab Detail, di bawah Log Kesehatan dan Tidak Diaktifkan, pilih Konfigurasi grup log untuk membuka kotak CustomerGatewayNamedialog Edit.
4. Untuk grup log kesehatan Gateway, pilih salah satu dari berikut ini:
 - Nonaktifkan logging jika Anda tidak ingin memantau gateway Anda menggunakan grup CloudWatch log.
 - Buat grup log baru untuk membuat grup CloudWatch log baru.
 - Gunakan grup log yang ada untuk menggunakan grup CloudWatch log yang sudah ada.

Pilih grup log dari daftar grup log yang ada.

5. Pilih Simpan perubahan.
6. Untuk melihat log kesehatan untuk gateway Anda, lakukan hal berikut:
 1. Di panel navigasi, pilih Gateway, lalu pilih gateway yang Anda konfigurasi untuk Grup CloudWatch Log.
 2. Pilih tab Detail, dan di bawah log Kesehatan, pilih CloudWatch Log. Halaman detail grup Log terbuka di CloudWatch konsol.

Berikut ini adalah contoh pesan acara Tape Gateway yang dikirim ke CloudWatch. Contoh ini menunjukkan TapeStatusTransition pesan.

```
{  
  "severity": "INFO",
```



```

"source": "FZTT16FCF5",
"type": "TapeStatusTransition",
"gateway": "sgw-C51DFEAC",
"timestamp": "1581553463831",
"newStatus": "RETRIEVED"
}

```

Menggunakan Metrik CloudWatch Amazon

Anda bisa mendapatkan data pemantauan untuk Tape Gateway Anda dengan menggunakan API AWS Management Console atau CloudWatch API. Konsol menampilkan serangkaian grafik berdasarkan data mentah dari CloudWatch API. CloudWatch API juga dapat digunakan melalui salah satu [Kit Pengembangan AWS Perangkat Lunak Amazon \(SDK\)](#) atau alat [Amazon CloudWatch API](#). Tergantung kebutuhan, Anda mungkin lebih memilih menggunakan grafik yang ditampilkan di konsol atau diterima dari API.

Terlepas dari metode mana yang Anda pilih untuk digunakan untuk bekerja dengan metrik, Anda harus menentukan informasi berikut:

- Dimensi metrik untuk bekerja dengan. Dimensi adalah pasangan nama-nilai yang membantu Anda mengidentifikasi metrik secara unik. Dimensi untuk Storage Gateway adalah `GatewayId` dan `GatewayName`. Di CloudWatch konsol, Anda dapat menggunakan `Gateway Metrics` tampilan untuk dengan mudah memilih dimensi khusus gateway dan khusus pita. Untuk informasi selengkapnya tentang dimensi, lihat [Dimensi](#) di Panduan CloudWatch Pengguna Amazon.
- Nama metrik, seperti `ReadBytes`.

Tabel berikut merangkum jenis data metrik Storage Gateway yang tersedia untuk Anda.

Ruang CloudWatch Nama Amazon	Dimensi	Deskripsi
AWS/StorageGateway	<code>GatewayId</code> , <code>GatewayName</code>	Dimensi ini menyaring data metrik yang menjelaskan aspek Tape Gateway. Anda dapat mengidentifikasi Tape Gateway untuk dikerjakan dengan menentukan dimensi <code>GatewayId</code> dan <code>GatewayName</code> dimensi.

Ruang CloudWatch Nama Amazon	Dimensi	Deskripsi
		Data throughput dan latensi dari Tape Gateway didasarkan pada semua kaset virtual di Tape Gateway. Data tersedia secara otomatis dalam periode 5 menit tanpa biaya.

Bekerja dengan metrik gateway dan tape mirip dengan bekerja dengan metrik layanan lainnya. Anda dapat menemukan diskusi tentang beberapa tugas metrik yang paling umum dalam CloudWatch dokumentasi yang tercantum berikut:

- [Melihat Metrik yang Tersedia](#)
- [Mendapatkan Statistik untuk Metrik](#)
- [Membuat CloudWatch Alarm](#)

Memahami Metrik Pita Virtual

Anda dapat menemukan informasi berikut tentang metrik Storage Gateway yang mencakup kaset virtual. Setiap kaset memiliki satu set metrik yang terkait dengannya.

Beberapa metrik khusus rekaman mungkin memiliki nama yang sama dengan metrik khusus gateway tertentu. Metrik ini mewakili jenis pengukuran yang sama tetapi dicakup ke pita alih-alih gateway. Sebelum mulai bekerja, tentukan apakah Anda ingin bekerja dengan metrik gateway atau metrik pita. Saat bekerja dengan metrik pita, tentukan ID pita untuk rekaman yang ingin Anda lihat metrik. Untuk informasi selengkapnya, lihat [Menggunakan Metrik CloudWatch Amazon](#).

Note

Beberapa metrik mengembalikan titik data hanya ketika data baru telah dihasilkan selama periode pemantauan terbaru.

Tabel berikut menjelaskan metrik Storage Gateway yang dapat Anda gunakan untuk mendapatkan informasi tentang kaset Anda.

Metrik	Deskripsi
CachePercentDirty	<p>Kontribusi rekaman terhadap persentase keseluruhan cache gateway yang tidak bertahan AWS. Sampel diambil pada akhir periode pelaporan.</p> <p>Gunakan CachePercentDirty metrik gateway untuk melihat persentase keseluruhan cache gateway yang tidak bertahan AWS. Untuk informasi selengkapnya, lihat Memahami metrik gateway.</p> <p>Unit: Persen</p>
CloudTraffic	<p>Jumlah byte yang diunggah dan diunduh dari cloud ke kaset.</p> <p>Unit: byte</p>
IoWaitPercent	<p>Persentase IoWait unit yang dialokasikan yang saat ini digunakan oleh rekaman itu.</p> <p>Unit: Persen</p>
HealthNotification	<p>Jumlah pemberitahuan kesehatan yang dikirim oleh rekaman itu.</p> <p>Unit: hitung</p>
MemUsedBytes	<p>Persentase memori yang dialokasikan yang saat ini digunakan oleh rekaman itu.</p> <p>Satuan: Byte</p>
MemTotalBytes	<p>Persentase total memori yang saat ini digunakan oleh rekaman itu.</p> <p>Satuan: Byte</p>

Metrik	Deskripsi
ReadBytes	<p>Jumlah total byte yang dibaca dari aplikasi lokal Anda dalam periode pelaporan untuk berbagi file.</p> <p>Gunakan metrik ini dengan Sum statistik untuk mengukur throughput dan dengan Samples statistik untuk mengukur IOPS.</p> <p>Satuan: Byte</p>
UserCpuPercent	<p>Persentase unit komputasi CPU yang dialokasikan untuk pengguna yang saat ini digunakan oleh rekaman.</p> <p>Unit: Persen</p>
WriteBytes	<p>Jumlah total byte yang ditulis ke aplikasi lokal Anda dalam periode pelaporan.</p> <p>Gunakan metrik ini dengan Sum statistik untuk mengukur throughput dan dengan Samples statistik untuk mengukur IOPS.</p> <p>Satuan: Byte</p>

Mengukur Kinerja Antara Tape Gateway Anda dan AWS

Throughput data, latensi data, dan operasi per detik adalah ukuran yang dapat Anda gunakan untuk memahami kinerja penyimpanan aplikasi yang menggunakan Tape Gateway Anda. Bila Anda menggunakan statistik agregasi yang benar, nilai ini dapat diukur dengan menggunakan metrik Storage Gateway yang disediakan untuk Anda.

Statistik adalah agregasi metrik selama periode waktu tertentu. Saat Anda melihat nilai metrik di CloudWatch, gunakan Average statistik untuk latensi data (milidetik), dan gunakan Samples statistik untuk operasi input/output per detik (IOPS). Untuk informasi selengkapnya, lihat [Statistik](#) di Panduan CloudWatch Pengguna Amazon.

Tabel berikut merangkum metrik dan statistik terkait yang dapat Anda gunakan untuk mengukur throughput, latensi, dan IOPS antara Tape Gateway dan AWS

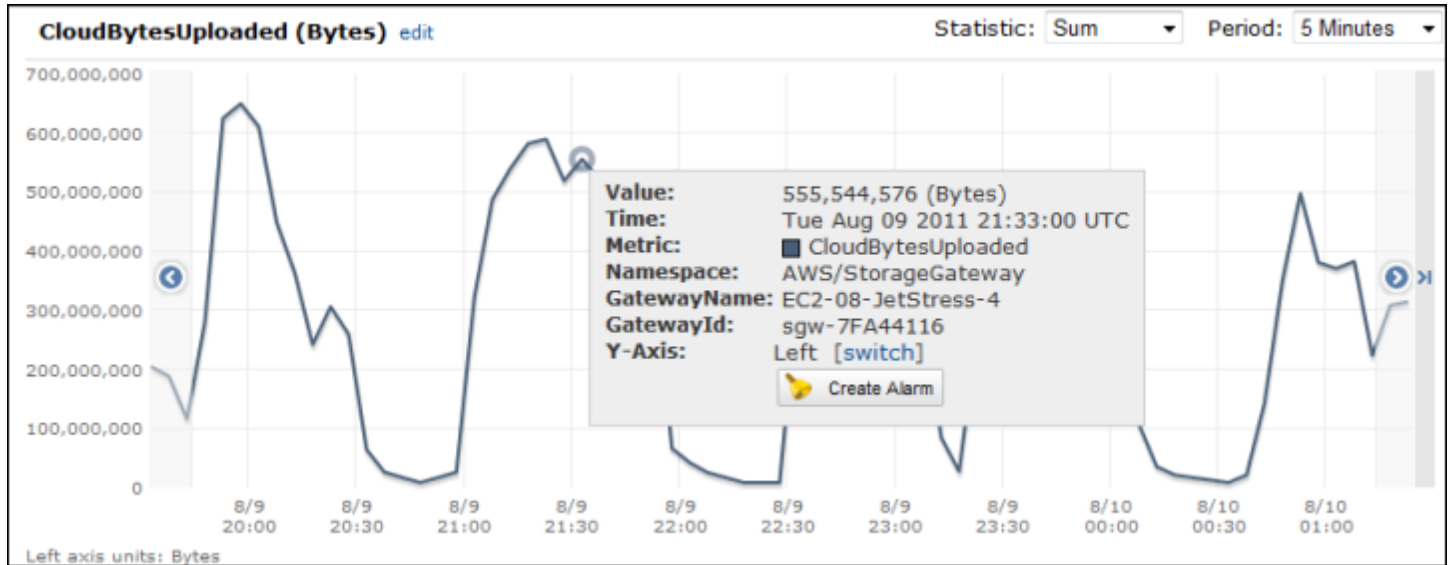
Item yang menarik	Cara Mengukur
Latensi	Gunakan <code>ReadTime</code> dan <code>WriteTime</code> metrik dengan <code>Average</code> CloudWatch statistik. Misalnya, <code>Average</code> nilai <code>ReadTime</code> metrik memberi Anda latensi per operasi selama periode waktu sampel.
Throughput ke AWS	Gunakan <code>CloudBytesDownloaded</code> dan <code>CloudBytesUploaded</code> metrik dengan <code>Sum</code> CloudWatch statistik. Misalnya, <code>Sum</code> nilai <code>CloudBytesDownloaded</code> metrik selama periode sampel 5 menit dibagi 300 detik memberi Anda throughput dari AWS Tape Gateway sebagai laju dalam byte per detik.
Latensi data ke AWS	Gunakan <code>CloudDownloadLatency</code> metrik dengan <code>Average</code> statistik. Misalnya, <code>Average</code> statistik <code>CloudDownloadLatency</code> metrik memberi Anda latensi per operasi.

Untuk mengukur throughput data upload dari Tape Gateway ke AWS

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih tab Metrik.
3. Pilih dimensi StorageGateway: Gateway Metrics, dan temukan Tape Gateway yang ingin Anda gunakan.
4. Pilih `CloudBytesUploaded` metrik.
5. Untuk Rentang Waktu, pilih nilai.
6. Pilih `Sum` statistiknya.
7. Untuk Periode, pilih nilai 5 menit atau lebih.
8. Dalam kumpulan titik data yang diurutkan waktu yang dihasilkan, bagi setiap titik data dengan periode (dalam detik) untuk mendapatkan throughput pada periode sampel tersebut.

Gambar berikut menunjukkan `CloudBytesUploaded` metrik untuk pita gateway dengan `Sum` statistik. Pada gambar, menempatkan kursor di atas titik data menampilkan informasi tentang titik data, termasuk nilainya dan jumlah byte yang diunggah. Bagilah nilai ini dengan nilai Periode (5

menit) untuk mendapatkan throughput pada titik sampel tersebut. Untuk titik yang disorot, throughput dari Tape Gateway ke AWS adalah 555.544.576 byte dibagi 300 detik, yaitu 1,7 megabyte per detik.



Untuk mengukur latensi data dari Tape Gateway ke AWS

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih tab Metrik.
3. Pilih GatewayMetrics dimensi StorageGateway:, dan temukan Tape Gateway yang ingin Anda gunakan.
4. Pilih CloudDownloadLatency metrik.
5. Untuk Rentang Waktu, pilih nilai.
6. Pilih Average statistiknya.
7. Untuk Periode, pilih nilai 5 menit agar sesuai dengan waktu pelaporan default.

Kumpulan titik data yang diurutkan waktu yang dihasilkan berisi latensi dalam milidetik.

Untuk menyetel alarm ambang batas atas untuk throughput Tape Gateway ke AWS

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih Buat Alarm untuk memulai wizard Buat Alarm.
3. Pilih dimensi StorageGateway: Gateway Metrics, dan temukan Tape Gateway yang ingin Anda gunakan.
4. Pilih CloudBytesUploaded metrik.

5. Tentukan alarm dengan menentukan status alarm ketika `CloudBytesUploaded` metrik lebih besar dari atau sama dengan nilai yang ditentukan untuk waktu tertentu. Misalnya, Anda dapat menentukan status alarm ketika `CloudBytesUploaded` metrik lebih besar dari 10 megabita selama 60 menit.
6. Konfigurasi tindakan yang akan diambil untuk status alarm. Misalnya, Anda dapat memiliki pemberitahuan email yang dikirimkan kepada Anda.
7. Pilih Buat Alarm.

Untuk mengatur alarm ambang batas atas untuk membaca data dari AWS

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih Buat Alarm untuk memulai wizard Buat Alarm.
3. Pilih dimensi `StorageGateway: Gateway Metrics`, dan temukan Tape Gateway yang ingin Anda gunakan.
4. Pilih `CloudDownloadLatency` metrik.
5. Tentukan alarm dengan menentukan status alarm ketika `CloudDownloadLatency` metrik lebih besar dari atau sama dengan nilai yang ditentukan untuk waktu tertentu. Misalnya, Anda dapat menentukan status alarm ketika lebih besar dari 60.000 milidetik selama lebih dari 2 jam. `CloudDownloadLatency`
6. Konfigurasi tindakan yang akan diambil untuk status alarm. Misalnya, Anda dapat memiliki pemberitahuan email yang dikirimkan kepada Anda.
7. Pilih Buat Alarm.

Mempertahankan Gateway Anda

Mempertahankan gateway Anda mencakup tugas-tugas seperti mengonfigurasi penyimpanan cache dan mengunggah ruang buffer, dan melakukan pemeliharaan umum kinerja gateway Anda. Tugas-tugas ini umum untuk semua jenis gateway. Jika Anda belum membuat gateway, lihat [Membuat Gateway Anda](#).

Topik

- [Mematikan VM Gateway Anda](#)
- [Mengelola disk lokal untuk Storage Gateway Anda](#)
- [Mengelola Bandwidth untuk Tape Gateway Anda](#)
- [Mengelola Pembaruan Gateway Menggunakan AWS Storage Gateway Konsol](#)
- [Melakukan Tugas Pemeliharaan di Konsol Lokal](#)
- [Menghapus Gateway Anda dengan Menggunakan AWS Storage Gateway Konsol dan Menghapus Sumber Daya Terkait](#)

Mematikan VM Gateway Anda

Anda mungkin perlu mematikan atau me-reboot VM Anda untuk pemeliharaan, seperti saat menerapkan patch ke hypervisor Anda. Sebelum Anda mematikan VM, Anda harus terlebih dahulu menghentikan gateway. Untuk File Gateway, Anda cukup mematikan VM Anda. Meskipun bagian ini berfokus pada memulai dan menghentikan gateway menggunakan Storage Gateway Management Console, Anda juga dapat menghentikan gateway dengan menggunakan konsol lokal VM atau Storage Gateway API. Saat Anda menyalakan VM Anda, ingatlah untuk me-restart gateway Anda.

Important

Jika Anda berhenti dan memulai gateway Amazon EC2 yang menggunakan penyimpanan sementara, gateway akan offline secara permanen. Ini terjadi karena disk penyimpanan fisik diganti. Tidak ada solusi untuk masalah ini. Satu-satunya resolusi adalah menghapus gateway dan mengaktifkan yang baru pada instans EC2 baru.

Note

Jika Anda menghentikan gateway Anda saat perangkat lunak cadangan Anda menulis atau membaca dari rekaman, tugas menulis atau membaca mungkin tidak berhasil. Sebelum Anda menghentikan gateway Anda, Anda harus memeriksa perangkat lunak cadangan Anda dan jadwal cadangan untuk tugas apa pun yang sedang berlangsung.

- [Masuk ke Konsol Lokal Menggunakan Kredensial Default](#) Konsol lokal Gateway VM—lihat.
- Storage Gateway API—Lihat [ShutdownGateway](#)

Untuk File Gateway, Anda cukup mematikan VM Anda. Anda tidak mematikan gateway.

Memulai dan Menghentikan Tape Gateway

Untuk menghentikan Tape Gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway untuk berhenti. Status gateway adalah Running.
3. Untuk Tindakan, pilih Stop gateway dan verifikasi id gateway dari kotak dialog, lalu pilih Stop gateway.

Saat gateway berhenti, Anda mungkin melihat pesan yang menunjukkan status gateway. Ketika gateway dimatikan, pesan dan tombol Start gateway muncul di tab Detail.

Ketika Anda menghentikan gateway Anda, sumber daya penyimpanan tidak akan dapat diakses sampai Anda memulai penyimpanan Anda. Jika gateway mengunggah data saat dihentikan, unggahan akan dilanjutkan saat Anda memulai gateway.

Untuk memulai Tape Gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Gateway dan kemudian pilih gateway untuk memulai. Status gateway adalah Shutdown.
3. Pilih Detail. dan kemudian pilih Start gateway.

Mengelola disk lokal untuk Storage Gateway Anda

Mesin virtual gateway (VM) menggunakan disk lokal yang Anda alokasikan di tempat untuk buffering dan penyimpanan. Gateway yang dibuat di instans Amazon EC2 menggunakan volume Amazon EBS sebagai disk lokal.

Topik

- [Menentukan jumlah penyimpanan disk lokal](#)
- [Mengoptimalkan Kinerja Gateway](#)
- [Menentukan ukuran buffer unggahan yang akan dialokasikan](#)
- [Menentukan ukuran penyimpanan cache yang akan dialokasikan](#)
- [Mengkonfigurasi buffer unggahan tambahan atau penyimpanan cache](#)

Menentukan jumlah penyimpanan disk lokal

Jumlah dan ukuran disk yang ingin Anda alokasikan untuk gateway Anda terserah Anda. Bergantung pada solusi penyimpanan yang Anda terapkan (lihat [Rencanakan penyebaran Storage Gateway](#)), gateway memerlukan penyimpanan tambahan berikut:

- Tape Gateways membutuhkan setidaknya dua disk. Satu untuk digunakan sebagai cache, dan satu untuk digunakan sebagai buffer unggahan.

Tabel berikut merekomendasikan ukuran untuk penyimpanan disk lokal untuk gateway yang Anda gunakan. Anda dapat menambahkan lebih banyak penyimpanan lokal nanti setelah Anda mengatur gateway, dan saat tuntutan beban kerja Anda meningkat.

Penyimpanan lokal	Deskripsi
Unggah buffer	Buffer unggahan menyediakan area pementasan untuk data sebelum gateway mengunggah data ke Amazon S3. Gateway Anda mengunggah data buffer ini melalui koneksi Secure Sockets Layer (SSL) terenkripsi ke. AWS

Penyimpanan lokal	Deskripsi	
Penyimpanan cache	Penyimpanan cache bertindak sebagai penyimpanan tahan lama lokal untuk data yang menunggu unggahan ke Amazon S3 dari buffer unggahan. Saat aplikasi Anda menjalankan I/O pada volume atau tape, gateway menyimpan data ke penyimpanan cache untuk akses latensi rendah. Saat aplikasi Anda meminta data dari volume atau rekaman, gateway terlebih dahulu memeriksa penyimpanan cache untuk data sebelum mengunduh data dari AWS.	

Note

Saat Anda menyediakan disk, kami sangat menyarankan agar Anda tidak menyediakan disk lokal untuk buffer unggahan dan penyimpanan cache jika mereka menggunakan sumber daya fisik yang sama (disk yang sama). Sumber daya penyimpanan fisik yang mendasari direpresentasikan sebagai penyimpanan data di VMware. Saat Anda menyebarkan VM gateway, Anda memilih penyimpanan data untuk menyimpan file VM. Saat Anda menyediakan disk lokal (misalnya, untuk digunakan sebagai penyimpanan cache atau buffer unggah), Anda memiliki opsi untuk menyimpan disk virtual di penyimpanan data yang sama dengan VM atau penyimpanan data yang berbeda.

Jika Anda memiliki lebih dari satu penyimpanan data, kami sangat menyarankan Anda memilih satu penyimpanan data untuk penyimpanan cache dan satu lagi untuk buffer unggahan. Penyimpanan data yang didukung oleh hanya satu disk fisik yang mendasarinya dapat menyebabkan kinerja yang buruk dalam beberapa situasi ketika digunakan untuk mendukung penyimpanan cache dan buffer unggah. Ini juga berlaku jika cadangan adalah konfigurasi RAID yang kurang berkinerja seperti RAID1.

Setelah konfigurasi awal dan penerapan gateway Anda, Anda dapat menyesuaikan penyimpanan lokal dengan menambahkan atau menghapus disk untuk buffer unggahan. Anda juga dapat menambahkan disk untuk penyimpanan cache.

Mengoptimalkan Kinerja Gateway

Untuk mencapai kinerja optimal, gunakan disk SSD throughput tinggi untuk cache dan buffer unggahan

- Gunakan disk yang berbeda untuk cache dan unggah buffer. Jika menggunakan RAID, pastikan cache dan unggah buffer di disks menggunakan pengontrol RAID terpisah di tingkat perangkat keras.
- Tambahkan setidaknya 2 disk buffer unggahan yang berbeda.
- Gunakan konfigurasi raid bergaris RAID 0 untuk perangkat buffer unggahan cache + untuk meningkatkan throughput. Ini sangat penting untuk disk cache.

Menentukan ukuran buffer unggahan yang akan dialokasikan

Anda dapat menentukan ukuran buffer upload yang akan dialokasikan dengan menggunakan rumus buffer upload. Kami sangat menyarankan Anda mengalokasikan setidaknya 150 GiB buffer unggahan. Jika rumus mengembalikan nilai kurang dari 150 GiB, gunakan 150 GiB sebagai jumlah yang Anda alokasikan ke buffer unggahan. Anda dapat mengonfigurasi kapasitas buffer unggahan hingga 2 TiB untuk setiap gateway.

Note

Untuk Tape Gateways, ketika buffer unggahan mencapai kapasitasnya, aplikasi Anda dapat terus membaca dan menulis data ke volume penyimpanan Anda. Namun, Tape Gateway tidak menulis data volume apa pun ke buffer unggahannya dan tidak mengunggah data ini AWS hingga Storage Gateway menyinkronkan data yang disimpan secara lokal dengan salinan data yang disimpan. AWS Sinkronisasi ini terjadi ketika volume berada dalam status BOOTSTRAPPING.

Untuk memperkirakan jumlah buffer unggahan yang akan dialokasikan, Anda dapat menentukan kecepatan data masuk dan keluar yang diharapkan dan menghubungkannya ke rumus berikut.

Tingkat data yang masuk

Tarif ini mengacu pada throughput aplikasi, tingkat di mana aplikasi lokal Anda menulis data ke gateway Anda selama beberapa periode waktu.

Tingkat data keluar

Tarif ini mengacu pada throughput jaringan, tingkat di mana gateway Anda dapat mengunggah data. AWS Tingkat ini tergantung pada kecepatan jaringan Anda, pemanfaatan, dan apakah Anda telah mengaktifkan pembatasan bandwidth. Tingkat ini harus disesuaikan untuk kompresi. Saat mengunggah data ke AWS, gateway menerapkan kompresi data jika memungkinkan. Misalnya, jika data aplikasi Anda hanya teks, Anda mungkin mendapatkan rasio kompresi efektif sekitar 2:1. Namun, jika Anda menulis video, gateway mungkin tidak dapat mencapai kompresi data apa pun dan mungkin memerlukan lebih banyak buffer unggahan untuk gateway.

Kami sangat menyarankan Anda mengalokasikan setidaknya 150 GiB ruang buffer upload jika salah satu dari berikut ini benar:

- Tarif masuk Anda lebih tinggi dari tarif keluar.
- Rumus mengembalikan nilai kurang dari 150 GiB.

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

Misalnya, asumsikan bahwa aplikasi bisnis Anda menulis data teks ke gateway Anda dengan kecepatan 40 MB per detik selama 12 jam per hari dan throughput jaringan Anda adalah 12 MB per detik. Dengan asumsi faktor kompresi 2:1 untuk data teks, Anda akan mengalokasikan sekitar 690 GiB ruang untuk buffer unggahan.

Example

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

Anda awalnya dapat menggunakan perkiraan ini untuk menentukan ukuran disk yang ingin Anda alokasikan ke gateway sebagai ruang buffer unggah. Tambahkan lebih banyak ruang buffer upload sesuai kebutuhan menggunakan konsol Storage Gateway. Selain itu, Anda dapat menggunakan metrik CloudWatch operasional Amazon untuk memantau penggunaan buffer unggahan dan

menentukan persyaratan penyimpanan tambahan. Untuk informasi tentang metrik dan pengaturan alarm, lihat. [Memantau buffer unggahan](#)

Menentukan ukuran penyimpanan cache yang akan dialokasikan

Gateway Anda menggunakan penyimpanan cache untuk menyediakan akses latensi rendah ke data yang baru saja Anda akses. Penyimpanan cache bertindak sebagai penyimpanan tahan lama lokal untuk data yang menunggu unggahan ke Amazon S3 dari buffer unggahan. Secara umum, Anda mengukur penyimpanan cache 1,1 kali ukuran buffer unggah. Untuk informasi selengkapnya tentang cara memperkirakan ukuran penyimpanan cache, lihat [Menentukan ukuran buffer unggahan yang akan dialokasikan](#).

Anda awalnya dapat menggunakan perkiraan ini untuk menyediakan disk untuk penyimpanan cache. Anda kemudian dapat menggunakan metrik CloudWatch operasional Amazon untuk memantau penggunaan penyimpanan cache dan menyediakan lebih banyak penyimpanan sesuai kebutuhan menggunakan konsol. Untuk informasi tentang penggunaan metrik dan pengaturan alarm, lihat. [Memantau penyimpanan cache](#)

Mengkonfigurasi buffer unggahan tambahan atau penyimpanan cache

Saat aplikasi Anda perlu berubah, Anda dapat meningkatkan buffer unggahan gateway atau kapasitas penyimpanan cache. Anda dapat menambahkan kapasitas penyimpanan ke gateway Anda tanpa mengganggu fungsionalitas atau menyebabkan downtime. Saat Anda menambahkan lebih banyak penyimpanan, Anda melakukannya dengan gateway VM dihidupkan.

Important

Saat menambahkan cache atau mengunggah buffer ke gateway yang ada, Anda harus membuat disk baru di hypervisor host gateway atau instans Amazon EC2. Jangan menghapus atau mengubah ukuran disk yang ada yang telah dialokasikan sebagai cache atau upload buffer.

Untuk mengonfigurasi buffer unggahan tambahan atau penyimpanan cache untuk gateway Anda

1. Menyediakan satu atau beberapa disk baru di hypervisor host gateway atau instans Amazon EC2 Anda. Untuk informasi tentang cara menyediakan disk pada hypervisor, lihat dokumentasi hypervisor Anda. Untuk informasi tentang penyediaan volume Amazon EBS untuk instans Amazon EC2, lihat volume Amazon [EBS di Panduan Pengguna Amazon](#) Elastic Compute Cloud

- untuk Instans Linux. Pada langkah-langkah berikut, Anda akan mengonfigurasi disk ini sebagai buffer unggah atau penyimpanan cache.
2. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
 3. Di panel navigasi, pilih Gateway.
 4. Cari gateway Anda dan pilih dari daftar.
 5. Dari menu Tindakan, pilih Konfigurasi penyimpanan.
 6. Di bagian Konfigurasi penyimpanan, identifikasi disk yang Anda sediakan. Jika Anda tidak melihat disk Anda, pilih ikon penyegaran untuk menyegarkan daftar. Untuk setiap disk, pilih UPLOAD BUFFER atau CACHE STORAGE dari menu drop-down yang dialokasikan ke.
 7. Pilih Simpan perubahan untuk menyimpan pengaturan konfigurasi Anda.

Mengelola Bandwidth untuk Tape Gateway Anda

Anda dapat membatasi (atau membatasi) throughput unggahan dari gateway ke AWS atau throughput unduhan dari AWS gateway Anda. Menggunakan bandwidth throttling membantu Anda mengontrol jumlah bandwidth jaringan yang digunakan oleh gateway Anda. Secara default, gateway yang diaktifkan tidak memiliki batas tarif saat mengunggah atau mengunduh.

Anda dapat menentukan batas tarif dengan menggunakan AWS Management Console, atau secara terprogram dengan menggunakan Storage Gateway API (lihat [UpdateBandwidthRateLimit](#)) atau AWS Software Development Kit (SDK). Dengan membatasi bandwidth secara terprogram, Anda dapat mengubah batas secara otomatis sepanjang hari—misalnya, dengan menjadwalkan tugas untuk mengubah bandwidth.

Anda juga dapat menentukan pembatasan bandwidth berbasis jadwal untuk gateway Anda. Anda menjadwalkan pembatasan bandwidth dengan mendefinisikan satu atau lebih interval. `bandwidth-rate-limit` Untuk informasi selengkapnya, lihat [Throttling Bandwidth Berbasis Jadwal Menggunakan Konsol Storage Gateway](#).

Mengkonfigurasi pengaturan tunggal untuk pembatasan bandwidth adalah setara fungsional dengan mendefinisikan jadwal dengan `bandwidth-rate-limit` interval tunggal yang ditetapkan untuk Setiap Hari, dengan waktu Mulai `00:00` dan waktu Akhir. `23:59`

Note

Informasi di bagian ini khusus untuk Tape dan Volume Gateways. Untuk mengelola bandwidth untuk Gateway File Amazon S3, lihat [Mengelola Bandwidth untuk Gateway File](#)

[Amazon S3 Anda](#). Batas tingkat bandwidth saat ini tidak didukung untuk Amazon FSx File Gateway.

Topik

- [Mengubah Bandwidth Throttling Menggunakan Storage Gateway Console](#)
- [Throttling Bandwidth Berbasis Jadwal Menggunakan Konsol Storage Gateway](#)
- [Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for Java](#)
- [Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for .NET](#)
- [Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS Tools for Windows PowerShell](#)

Mengubah Bandwidth Throttling Menggunakan Storage Gateway Console

Prosedur berikut menunjukkan cara mengubah pembatasan bandwidth gateway dari konsol Storage Gateway.

Untuk mengubah pembatasan bandwidth gateway menggunakan konsol

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi kiri, pilih Gateway, lalu pilih gateway yang ingin Anda kelola.
3. Untuk Tindakan, pilih Edit batas bandwidth.
4. Dalam kotak dialog Edit batas laju, masukkan nilai batas baru, lalu pilih Simpan. Perubahan Anda muncul di tab Detail untuk gateway Anda.

Throttling Bandwidth Berbasis Jadwal Menggunakan Konsol Storage Gateway

Prosedur berikut menunjukkan cara menjadwalkan perubahan pada pembatasan bandwidth gateway menggunakan konsol Storage Gateway.

Untuk menambah atau memodifikasi jadwal pelambatan bandwidth gateway


1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi kiri, pilih Gateway, lalu pilih gateway yang ingin Anda kelola.

3. Untuk Tindakan, pilih Edit jadwal batas laju bandwidth.

bandwidth-rate-limit Jadwal gateway ditampilkan di kotak dialog Edit jadwal batas laju bandwidth. Secara default, bandwidth-rate-limit jadwal gateway baru kosong.


4. Dalam kotak dialog Edit jadwal batas laju bandwidth, pilih Tambahkan item baru untuk menambahkan bandwidth-rate-limit interval baru. Masukkan informasi berikut untuk setiap bandwidth-rate-limit interval:

- Hari dalam seminggu — Anda dapat membuat bandwidth-rate-limit interval untuk hari kerja (Senin sampai Jumat), untuk akhir pekan (Sabtu dan Minggu), untuk setiap hari dalam seminggu, atau untuk satu atau lebih hari tertentu dalam seminggu.
- Waktu mulai — Masukkan waktu mulai untuk interval bandwidth di zona waktu lokal gateway, menggunakan format HH: MM.

 Note

bandwidth-rate-limit Interval Anda dimulai pada awal menit yang Anda tentukan di sini.

- Waktu akhir - Masukkan waktu akhir untuk bandwidth-rate-limit interval di zona waktu lokal gateway, menggunakan format HH: MM.

 Important

bandwidth-rate-limit Interval berakhir pada akhir menit yang ditentukan di sini. Untuk menjadwalkan interval yang berakhir pada akhir jam, masukkan **59**.

Untuk menjadwalkan interval kontinu berturut-turut, transisi pada awal jam, tanpa gangguan di antara interval, masukkan **59** untuk menit akhir interval pertama.

Masukkan **00** untuk menit awal interval berikutnya.

- Tingkat unduhan - Masukkan batas kecepatan unduhan, dalam kilobit per detik (Kbps), atau pilih Tidak ada batas untuk menonaktifkan pembatasan bandwidth untuk mengunduh. Nilai minimum untuk tingkat unduhan adalah 100 Kbps.
- Upload rate — Masukkan batas upload rate, di Kbps, atau pilih No limit untuk menonaktifkan bandwidth throttling untuk upload. Nilai minimum untuk tingkat unggah adalah 50 Kbps.

Untuk memodifikasi bandwidth-rate-limit interval, Anda dapat memasukkan nilai yang direvisi untuk parameter interval.

Untuk menghapus bandwidth-rate-limit interval Anda, Anda dapat memilih Hapus di sebelah kanan interval yang akan dihapus.

Setelah perubahan Anda selesai, pilih Simpan.

5. Lanjutkan menambahkan bandwidth-rate-limit interval dengan memilih Tambahkan item baru dan masukkan hari, waktu mulai dan akhir, dan batas kecepatan unduh dan unggah.

 Important

bandwidth-rate-limit Interval B tidak bisa tumpang tindih. Waktu mulai suatu interval harus terjadi setelah waktu akhir dari interval sebelumnya, dan sebelum waktu mulai dari interval berikutnya.

6. Setelah memasukkan semua bandwidth-rate-limit interval, pilih Simpan perubahan untuk menyimpan bandwidth-rate-limit jadwal Anda.

Ketika bandwidth-rate-limit jadwal berhasil diperbarui, Anda dapat melihat batas kecepatan unduh dan unggah saat ini di panel Detail untuk gateway.

Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for Java

Dengan memperbarui batas bandwidth-rate secara terprogram, Anda dapat menyesuaikan batas secara otomatis selama periode waktu—misalnya, dengan menggunakan tugas terjadwal. Contoh berikut menunjukkan cara memperbarui batas bandwidth-rate gateway menggunakan AWS SDK for Java Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan aplikasi konsol Java. Untuk informasi selengkapnya, lihat [Memulai](#) di Panduan AWS SDK for Java Pengembang.

Example : Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for Java

Contoh kode Java berikut memperbarui batas bandwidth-rate gateway. Untuk menggunakan kode contoh ini, Anda harus memberikan titik akhir layanan, gateway Anda Amazon Resource Name (ARN), dan batas upload dan download. Untuk daftar endpoint AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat [AWS Storage Gateway Endpoints dan Quotas](#) di Referensi Umum AWS

```
import java.io.IOException;
```

```
import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;

public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

    // The endpoint
    static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

    // Rates
    static long uploadRate = 51200; // Bits per second, minimum 51200
    static long downloadRate = 102400; // Bits per second, minimum 102400

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

        // Create a Storage Gateway client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
        sgClient.setEndpoint(serviceURL);

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
        long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                    .withGatewayARN(gatewayARN)
                    .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .withAverageUploadRateLimitInBitsPerSec(uploadRate);
```

```
UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
second");
System.out.println("Download bandwidth limit = " + downloadRate + " bits
per second");
}
catch (AmazonClientException ex)
{
System.err.println("Error updating gateway bandwidth.\n" + ex.toString());
}
}
}
```

Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for .NET

Dengan memperbarui batas bandwidth-rate secara terprogram, Anda dapat menyesuaikan batas secara otomatis selama periode waktu—misalnya, dengan menggunakan tugas terjadwal. Contoh berikut menunjukkan cara memperbarui batas bandwidth-rate gateway dengan menggunakan AWS SDK for .NET Untuk menggunakan kode contoh, Anda harus terbiasa menjalankan aplikasi konsol.NET. Untuk informasi selengkapnya, lihat [Memulai](#) di Panduan AWS SDK for .NET Pengembang.

Example : Memperbarui Batas Tingkat Bandwidth Gateway dengan Menggunakan AWS SDK for .NET

Contoh kode C # berikut memperbarui batas kecepatan bandwidth gateway. Untuk menggunakan kode contoh ini, Anda harus memberikan titik akhir layanan, gateway Anda Amazon Resource Name (ARN), dan batas upload dan download. Untuk daftar endpoint AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat [AWS Storage Gateway Endpoints dan Quotas](#) di. Referensi Umum AWS

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Amazon.StorageGateway;
```

```
using Amazon.StorageGateway.Model;

namespace AWSStorageGateway
{
    class UpdateBandwidthExample
    {
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

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

        // The endpoint
        static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

        // Rates
        static long uploadRate = 51200; // Bits per second, minimum 51200
        static long downloadRate = 102400; // Bits per second, minimum 102400

        public static void Main(string[] args)
        {
            // Create a Storage Gateway client
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = serviceURL;
            sgClient = new AmazonStorageGatewayClient(sgConfig);

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

            Console.WriteLine("\nTo continue, press Enter.");
            Console.Read();
        }

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                        .WithGatewayARN(gatewayARN)
                        .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                        .WithAverageUploadRateLimitInBitsPerSec(uploadRate);
            }
        }
    }
}
```

```
UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
per second");
}
catch (AmazonStorageGatewayException ex)
{
Console.WriteLine("Error updating gateway bandwidth.\n" +
ex.ToString());
}
}
}
```

Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS Tools for Windows PowerShell

Dengan memperbarui batas bandwidth-rate secara terprogram, Anda dapat menyesuaikan batas secara otomatis selama periode waktu—misalnya, dengan menggunakan tugas terjadwal. Contoh berikut menunjukkan cara memperbarui batas bandwidth-rate gateway menggunakan AWS Tools for Windows PowerShell Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan PowerShell skrip. Untuk informasi lebih lanjut, lihat [Memulai](#) di AWS Tools for Windows PowerShell Panduan Pengguna.

Example : Memperbarui Batas Tingkat Bandwidth Gateway dengan Menggunakan AWS Tools for Windows PowerShell

Contoh PowerShell skrip berikut memperbarui batas kecepatan bandwidth gateway. Untuk menggunakan skrip contoh ini, Anda harus memberikan gateway Anda Nama Sumber Daya Amazon (ARN), dan batas unggah dan unduhan.

```
<#
.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)
```

Mengelola Pembaruan Gateway Menggunakan AWS Storage Gateway Konsol

Storage Gateway secara berkala merilis pembaruan perangkat lunak penting untuk gateway Anda. Anda dapat menerapkan pembaruan secara manual di Storage Gateway Management Console, atau menunggu hingga pembaruan diterapkan secara otomatis selama jadwal pemeliharaan yang dikonfigurasi. Meskipun Storage Gateway memeriksa pembaruan setiap menit, itu hanya melalui pemeliharaan dan restart jika ada pembaruan.

Rilis perangkat lunak Gateway secara teratur mencakup pembaruan sistem operasi dan tambalan keamanan yang telah divalidasi oleh AWS. Pembaruan ini biasanya dirilis setiap enam bulan, dan diterapkan sebagai bagian dari proses pembaruan gateway normal selama jendela pemeliharaan terjadwal.


 Note

Anda harus memperlakukan alat Storage Gateway sebagai mesin virtual terkelola, dan tidak boleh mencoba mengakses atau memodifikasi pemasangannya dengan cara apa pun. Mencoba menginstal atau memperbarui paket perangkat lunak apa pun menggunakan metode selain mekanisme pembaruan gateway normal (misalnya, SSM atau alat hypervisor) dapat menyebabkan gateway mengalami kerusakan.

Untuk mengubah alamat email yang mengirimkan pemberitahuan pembaruan perangkat lunak, buka halaman [Mengelola AWS akun](#) dan perbarui kontak alternatif untuk “operasi”.

Sebelum pembaruan apa pun diterapkan ke gateway Anda, AWS beri tahu Anda dengan pesan di konsol Storage Gateway dan Anda AWS Health Dashboard. Untuk informasi selengkapnya, lihat [AWS Health Dashboard](#). VM tidak reboot, tetapi gateway tidak tersedia untuk waktu yang singkat saat sedang diperbarui dan dimulai ulang.

Saat Anda menerapkan dan mengaktifkan gateway Anda, jadwal pemeliharaan mingguan default ditetapkan. Anda dapat mengubah jadwal pemeliharaan kapan saja. Saat pembaruan tersedia, tab Detail menampilkan pesan pemeliharaan. Anda dapat melihat tanggal dan waktu pembaruan terakhir yang berhasil diterapkan ke gateway Anda di tab Detail.

 Important


Anda dapat meminimalkan kemungkinan gangguan pada aplikasi Anda karena gateway restart dengan meningkatkan batas waktu inisiator iSCSI Anda. Untuk informasi selengkapnya tentang meningkatkan batas waktu inisiator iSCSI untuk Windows dan Linux, lihat dan. [Menyesuaikan Pengaturan Windows iSCSI Anda](#) [Menyesuaikan Pengaturan iSCSI Linux Anda](#)

Untuk memodifikasi jadwal pemeliharaan

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Pada panel navigasi, pilih Gateway, dan pilih gateway yang ingin Anda ubah jadwal pembaruan.
3. Untuk Tindakan, pilih Edit jendela pemeliharaan untuk menulis kotak dialog Edit waktu mulai pemeliharaan.
4. Untuk Jadwal, pilih Mingguan atau Bulanan untuk menjadwalkan pembaruan.

5. Jika Anda memilih Mingguan, ubah nilai untuk Hari dalam seminggu dan Waktu.

Jika Anda memilih Bulanan, ubah nilai untuk Hari dalam sebulan dan Waktu. Jika Anda memilih opsi ini dan Anda mendapatkan kesalahan, itu berarti gateway Anda adalah versi yang lebih lama dan belum ditingkatkan ke versi yang lebih baru.

 Note

Nilai maksimum yang dapat ditetapkan untuk hari dalam sebulan adalah 28. Jika 28 dipilih, waktu mulai pemeliharaan akan pada hari ke 28 setiap bulan.

Waktu mulai pemeliharaan Anda muncul di tab Detail untuk gateway lain kali Anda membuka tab Detail.

Melakukan Tugas Pemeliharaan di Konsol Lokal

Anda dapat melakukan tugas pemeliharaan berikut menggunakan konsol lokal host. Tugas konsol lokal dapat dilakukan pada host VM atau instans Amazon EC2. Banyak tugas yang umum di antara host yang berbeda, tetapi ada juga beberapa perbedaan.

Melakukan Tugas di Konsol Lokal VM

Untuk gateway yang digunakan di lokasi, Anda dapat melakukan tugas pemeliharaan berikut menggunakan konsol lokal host VM. Tugas-tugas ini umum untuk host VMware, Hyper-V, dan Linux Kernel-based Virtual Machine (KVM).

Topik

- [Masuk ke Konsol Lokal Menggunakan Kredensial Default](#)
- [Mengatur Kata Sandi Konsol Lokal dari Storage Gateway Console](#)
- [Merutekan Gateway Lokal Anda Melalui Proxy](#)
- [Mengkonfigurasi Jaringan Gateway Anda](#)
- [Menguji Koneksi Gateway Anda ke Internet](#)
- [Menyinkronkan Waktu VM Gateway Anda](#)
- [Menjalankan Perintah Storage Gateway di Konsol Lokal](#)
- [Melihat Status Sumber Daya Sistem Gateway Anda](#)

- [Mengkonfigurasi Adaptor Jaringan untuk Gateway Anda](#)

Masuk ke Konsol Lokal Menggunakan Kredensial Default

Ketika VM siap bagi Anda untuk masuk, layar login akan ditampilkan. Jika ini adalah pertama kalinya Anda masuk ke konsol lokal, Anda menggunakan kredensial login default untuk masuk. Kredensial login default ini memberi Anda akses ke menu tempat Anda dapat mengonfigurasi pengaturan jaringan gateway dan mengubah kata sandi dari konsol lokal. Storage Gateway memungkinkan Anda untuk mengatur kata sandi Anda sendiri dari AWS Storage Gateway konsol alih-alih mengubah kata sandi dari konsol lokal. Anda tidak perlu mengetahui kata sandi default untuk mengatur kata sandi baru. Untuk informasi selengkapnya, lihat [Mengatur Kata Sandi Konsol Lokal dari Storage Gateway Console](#).

Untuk masuk ke konsol lokal gateway

1. Jika ini adalah pertama kalinya Anda masuk ke konsol lokal, masuk ke VM dengan kredensial default. Nama pengguna default adalah `admin` dan kata sandi adalah `password`.

Jika tidak, gunakan kredensial Anda untuk masuk.

Note

Sebaiknya ubah kata sandi default dengan memasukkan angka yang sesuai untuk Gateway Console dari menu utama AWS Appliance Activation - Configuration, lalu jalankan `passwd` perintah. Untuk informasi tentang cara menjalankan perintah, lihat [Menjalankan Perintah Storage Gateway di Konsol Lokal](#). Anda juga dapat mengatur kata sandi Anda sendiri dari AWS Storage Gateway konsol. Untuk informasi selengkapnya, lihat [Mengatur Kata Sandi Konsol Lokal dari Storage Gateway Console](#).

Important

Untuk versi volume atau Tape Gateway yang lebih lama, nama pengguna adalah `sguser` dan kata sandinya `sgpassword`. Jika Anda mengatur ulang kata sandi dan gateway Anda diperbarui ke versi yang lebih baru, nama pengguna Anda akan berubah menjadi `admin` tetapi kata sandi akan dipertahankan.

2. Setelah Anda masuk, Anda melihat menu utama AWS Storage Gateway Configuration, dari mana Anda dapat melakukan berbagai tugas.

Untuk mempelajari tentang tugas ini	Lihat Topik Ini
Konfigurasi proxy SOCKS untuk gateway Anda	Merutekan Gateway Lokal Anda Melalui Proxy.
Konfigurasi jaringan Anda	Mengkonfigurasi Jaringan Gateway Anda.
Uji konektivitas jaringan	Menguji Koneksi Gateway Anda ke Internet.
Kelola waktu VM	Menyinkronkan Waktu VM Gateway Anda.
Jalankan perintah konsol Storage Gateway	Menjalankan Perintah Storage Gateway di Konsol Lokal.
Lihat pemeriksaan sumber daya sistem	Melihat Status Sumber Daya Sistem Gateway Anda.

Untuk mematikan gateway, masuk **0**.

Untuk keluar dari sesi konfigurasi, masukkan **X**.


Mengatur Kata Sandi Konsol Lokal dari Storage Gateway Console

Saat Anda masuk ke konsol lokal untuk pertama kalinya, Anda masuk ke VM dengan kredensi default — Nama pengguna adalah `admin` dan kata sandinya. `password` Kami menyarankan agar Anda selalu menetapkan kata sandi baru segera setelah Anda membuat gateway baru Anda. Anda dapat mengatur kata sandi ini dari AWS Storage Gateway konsol daripada konsol lokal jika Anda mau. Anda tidak perlu mengetahui kata sandi default untuk mengatur kata sandi baru.

Untuk mengatur kata sandi konsol lokal di konsol Storage Gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Pada panel navigasi, pilih Gateway lalu pilih gateway yang ingin Anda atur kata sandi baru.
3. Untuk Tindakan, pilih **Setel Kata Sandi Konsol Lokal**.


4. Dalam kotak dialog Setel Kata Sandi Konsol Lokal, ketik kata sandi baru, konfirmasi kata sandi, lalu pilih Simpan. Kata sandi baru Anda menggantikan kata sandi default. Storage Gateway tidak menyimpan kata sandi melainkan mengirimkannya dengan aman ke VM.

 Note

Kata sandi dapat terdiri dari karakter apa pun pada keyboard dan panjangnya bisa 1 hingga 512 karakter.

Merutekan Gateway Lokal Anda Melalui Proxy

Volume Gateways dan Tape Gateways mendukung konfigurasi proxy Socket Secure versi 5 (SOCKS5) antara gateway lokal dan AWS.

 Note

Satu-satunya konfigurasi proxy yang didukung adalah SOCKS5.

Jika gateway Anda harus menggunakan server proxy untuk berkomunikasi ke internet, maka Anda perlu mengonfigurasi pengaturan proxy SOCKS untuk gateway Anda. Anda melakukan ini dengan menentukan alamat IP dan nomor port untuk host yang menjalankan proxy Anda. Setelah Anda melakukannya, Storage Gateway merutekan semua lalu lintas melalui server proxy Anda. Untuk informasi tentang persyaratan jaringan untuk gateway Anda, lihat [Persyaratan jaringan dan firewall](#).

Prosedur berikut menunjukkan cara mengkonfigurasi proxy SOCKS untuk Volume Gateway dan Tape Gateway.

Untuk mengonfigurasi proxy SOCKS5 untuk volume dan Tape Gateways

1. Masuk ke konsol lokal gateway Anda.
 - VMware ESXi - untuk informasi lebih lanjut, lihat. [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
 - Microsoft Hyper-V — untuk informasi selengkapnya, lihat. [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
 - KVM — untuk informasi lebih lanjut, lihat. [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)

2. Dari AWS Storage Gateway - menu utama Konfigurasi, masukkan angka yang sesuai untuk memilih Konfigurasi Proxy SOCKS.
3. Dari menu AWS Storage Gateway SOCKS Proxy Configuration, masukkan angka yang sesuai untuk melakukan salah satu tugas berikut:

Untuk Melakukan Tugas Ini	Lakukan Ini
Konfigurasi proxy SOCKS	<p>Masukkan angka yang sesuai untuk memilih Configure SOCKS Proxy.</p> <p>Anda harus menyediakan nama host dan port untuk menyelesaikan konfigurasi.</p>
Lihat konfigurasi proxy SOCKS saat ini	<p>Masukkan angka yang sesuai untuk memilih Lihat Konfigurasi Proksi SOCKS Saat Ini.</p> <p>Jika proxy SOCKS tidak dikonfigurasi, pesan akan SOCKS Proxy not configured ditampilkan. Jika proxy SOCKS dikonfigurasi, nama host dan port proxy akan ditampilkan.</p>
Hapus konfigurasi proxy SOCKS	<p>Masukkan angka yang sesuai untuk memilih Hapus Konfigurasi Proksi SOCKS.</p> <p>Pesan SOCKS Proxy Configuration Removed ditampilkan.</p>

4. Mulai ulang VM Anda untuk menerapkan konfigurasi HTTP Anda.

Mengkonfigurasi Jaringan Gateway Anda


Konfigurasi jaringan default untuk gateway adalah Dynamic Host Configuration Protocol (DHCP). Dengan DHCP, gateway Anda secara otomatis diberi alamat IP. Dalam beberapa kasus, Anda mungkin perlu menetapkan IP gateway Anda secara manual sebagai alamat IP statis, seperti yang dijelaskan berikut.


Untuk mengkonfigurasi gateway Anda untuk menggunakan alamat IP statis


1. Masuk ke konsol lokal gateway Anda.
 - VMware ESXi - untuk informasi lebih lanjut, lihat. [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
 - Microsoft Hyper-V — untuk informasi selengkapnya, lihat. [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
 - KVM — untuk informasi lebih lanjut, lihat. [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)
2. Dari AWS Storage Gateway - menu utama Konfigurasi, masukkan angka yang sesuai untuk memilih Konfigurasi Jaringan.
3. Dari menu AWS Storage Gateway Network Configuration, lakukan salah satu tugas berikut:

Untuk Melakukan Tugas Ini	Lakukan Ini
Jelaskan adaptor jaringan	<p>Masukkan angka yang sesuai untuk memilih Deskripsi Adaptor.</p> <p>Daftar nama adaptor muncul, dan Anda diminta untuk mengetikkan nama adaptor — misalnya, eth0 Jika adaptor yang Anda tentukan sedang digunakan, informasi berikut tentang adaptor akan ditampilkan:</p> <ul style="list-style-type: none">• Alamat kontrol akses media (MAC)• Alamat IP• Netmask• Alamat IP Gateway• Status diaktifkan DHCP

Untuk Melakukan Tugas Ini	Lakukan Ini
	<p>Anda menggunakan nama adaptor yang tercantum di sini saat Anda mengonfigurasi alamat IP statis atau mengatur adaptor default gateway Anda.</p>
Konfigurasi DHCP	<p>Masukkan angka yang sesuai untuk memilih Konfigurasi DHCP.</p> <p>Anda diminta untuk mengkonfigurasi antarmuka jaringan untuk menggunakan DHCP.</p>

Untuk Melakukan Tugas Ini	Lakukan Ini
<p>Konfigurasi alamat IP statis untuk gateway Anda</p>	<p>Masukkan angka yang sesuai untuk memilih Konfigurasi IP Statis.</p> <p>Anda diminta untuk mengetik informasi berikut untuk mengkonfigurasi IP statis:</p> <ul style="list-style-type: none">• Nama adaptor jaringan• Alamat IP• Netmask• Alamat gateway default• Alamat Layanan Nama Domain Utama (DNS)• Alamat DNS sekunder <div data-bbox="829 1161 1511 1570" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Jika gateway Anda telah diaktifkan, Anda harus mematikannya dan memulai ulang dari konsol Storage Gateway agar pengaturan diterapkan. Untuk informasi selengkapnya, lihat Mematikan VM Gateway Anda.</p></div> <p>Jika gateway Anda menggunakan lebih dari satu antarmuka jaringan, Anda harus mengatur semua antarmuka yang diaktifkan untuk menggunakan DHCP atau alamat IP statis.</p>

Untuk Melakukan Tugas Ini	Lakukan Ini
	<p>Misalnya, VM gateway Anda menggunakan dua antarmuka yang dikonfigurasi sebagai DHCP. Jika Anda kemudian mengatur satu antarmuka ke IP statis, antarmuka lainnya dinonaktifkan. Untuk mengaktifkan antarmuka dalam hal ini, Anda harus mengaturnya ke IP statis.</p> <p>Jika kedua antarmuka awalnya diatur untuk menggunakan alamat IP statis dan Anda kemudian mengatur gateway untuk menggunakan DHCP, kedua antarmuka akan menggunakan DHCP.</p>
Konfigurasi nama host untuk gateway Anda	<p>Masukkan angka yang sesuai untuk memilih Configure Hostname.</p> <p>Anda diminta untuk memilih apakah gateway akan menggunakan nama host statis yang Anda tentukan, atau mendapatkannya secara otomatis melalui DHCP atau RDNS.</p> <div data-bbox="829 1150 1507 1507"><p> Note</p><p>Jika Anda mengonfigurasi nama host statis untuk gateway Anda, Anda harus membuat catatan A di sistem DNS Anda yang mengarahkan alamat IP gateway ke nama host statisnya.</p></div>

Untuk Melakukan Tugas Ini	Lakukan Ini
<p>Setel ulang semua konfigurasi jaringan gateway Anda ke DHCP</p>	<p>Masukkan angka yang sesuai untuk memilih Reset semua ke DHCP.</p> <p>Semua antarmuka jaringan diatur untuk menggunakan DHCP.</p> <div data-bbox="829 541 1507 999" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Jika gateway Anda telah diaktifkan, Anda harus mematikan dan memulai ulang gateway Anda dari konsol Storage Gateway agar pengaturan diterapkan. Untuk informasi selengkapnya, lihat Mematikan VM Gateway Anda.</p></div>
<p>Tetapkan adaptor rute default gateway Anda</p>	<p>Masukkan angka yang sesuai untuk memilih Set Default Adapter.</p> <p>Adaptor yang tersedia untuk gateway Anda ditampilkan, dan Anda diminta untuk memilih salah satu adaptor—misalnya, eth0</p>
<p>Lihat konfigurasi DNS gateway Anda</p>	<p>Masukkan angka yang sesuai untuk memilih Lihat Konfigurasi DNS.</p> <p>Alamat IP server nama DNS primer dan sekunder ditampilkan.</p>

Untuk Melakukan Tugas Ini	Lakukan Ini
Lihat tabel perutean	Masukkan angka yang sesuai untuk memilih Lihat Rute. Rute default gateway Anda ditampilkan.

Menguji Koneksi Gateway Anda ke Internet

Anda dapat menggunakan konsol lokal gateway Anda untuk menguji koneksi internet Anda. Tes ini dapat berguna ketika Anda memecahkan masalah jaringan dengan gateway Anda.

Untuk menguji koneksi gateway Anda ke internet

1. Masuk ke konsol lokal gateway Anda.
 - VMware ESXi - untuk informasi lebih lanjut, lihat. [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
 - Microsoft Hyper-V — untuk informasi selengkapnya, lihat. [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
 - KVM — untuk informasi lebih lanjut, lihat. [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)
2. Dari AWS Storage Gateway - menu utama Konfigurasi, masukkan angka yang sesuai untuk memilih Test Network Connectivity.

Jika gateway Anda telah diaktifkan, tes konektivitas segera dimulai. Untuk gateway yang belum diaktifkan, Anda harus menentukan jenis titik akhir dan Wilayah AWS seperti yang dijelaskan dalam langkah-langkah berikut.

3. Jika gateway Anda belum diaktifkan, masukkan angka yang sesuai untuk memilih jenis titik akhir untuk gateway Anda.
4. Jika Anda memilih jenis titik akhir publik, masukkan angka yang sesuai untuk memilih Wilayah AWS yang ingin Anda uji. Untuk didukung Wilayah AWS dan daftar titik akhir AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat [AWS Storage Gateway titik akhir dan kuota](#) di. Referensi Umum AWS

Saat pengujian berlangsung, setiap titik akhir menampilkan [LULUS] atau [GAGAL], yang menunjukkan status koneksi sebagai berikut:

Pesan	Deskripsi
[LULUS]	Storage Gateway memiliki konektivitas jaringan.
[GAGAL]	Storage Gateway tidak memiliki konektivitas jaringan.

Menyinkronkan Waktu VM Gateway Anda

Setelah gateway Anda digunakan dan dijalankan, dalam beberapa skenario waktu VM gateway dapat melayang. Misalnya, jika ada pemadaman jaringan yang berkepanjangan dan host dan gateway hypervisor Anda tidak mendapatkan pembaruan waktu, maka waktu VM gateway akan berbeda dari waktu sebenarnya. Ketika ada penyimpangan waktu, perbedaan terjadi antara waktu yang dinyatakan saat operasi seperti snapshot terjadi dan waktu sebenarnya saat operasi terjadi.

Untuk gateway yang digunakan pada VMware ESXi, mengatur waktu host hypervisor dan menyinkronkan waktu VM ke host sudah cukup untuk menghindari penyimpangan waktu. Untuk informasi selengkapnya, lihat [Sinkronisasi Waktu VM dengan Waktu Host](#).

Untuk gateway yang digunakan di Microsoft Hyper-V, Anda harus memeriksa waktu VM Anda secara berkala. Untuk informasi selengkapnya, lihat [Menyinkronkan Waktu VM Gateway Anda](#).

Menjalankan Perintah Storage Gateway di Konsol Lokal

Konsol lokal VM di Storage Gateway membantu menyediakan lingkungan yang aman untuk mengonfigurasi dan mendiagnosis masalah dengan gateway Anda. Dengan menggunakan perintah konsol lokal, Anda dapat melakukan tugas pemeliharaan seperti menyimpan tabel perutean, menghubungkan ke AWS Support, dan sebagainya.


Untuk menjalankan konfigurasi atau perintah diagnostik


1. Masuk ke konsol lokal gateway Anda:

- Untuk informasi selengkapnya tentang masuk ke konsol lokal VMware ESXi, lihat [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)

- Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
 - Untuk informasi selengkapnya tentang masuk ke konsol lokal KVM, lihat. [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Gateway Console.
 3. Dari prompt perintah konsol gateway, masukkan **h**.

Konsol menampilkan menu AVAILABLE COMMANDS, yang mencantumkan perintah yang tersedia:

Perintah	Fungsi
menggali	Kumpulkan output dari penggalian untuk pemecahan masalah DNS.
keluar	Kembali ke menu Konfigurasi.
-h	Tampilkan daftar perintah yang tersedia.
ifconfig	Lihat atau konfigurasi antarmuka jaringan. <div data-bbox="836 1165 1510 1575" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus. Untuk petunjuk, lihat Mengonfigurasi Jaringan Gateway Anda Mengonfigurasi Jaringan .</p> </div>
ip	Menampilkan/manipulasi routing, perangkat , dan terowongan.

Perintah	Fungsi
	<p> Note</p> <p>Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus. Untuk petunjuk, lihat Mengonfigurasi Jaringan Gateway Anda Mengonfigurasi Jaringan .</p>
iptables	Alat administrasi untuk penyaringan paket IPv4 dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.
nping	Kumpulkan output dari nping untuk pemecahan masalah jaringan.
open-support-channel	Connect to AWS Support.
passwd	Perbarui token otentikasi.
simpan-iptables	Pertahankan tabel IP.
save-routing-table	Simpan entri tabel routing yang baru ditambahkan.
tcptracert	Kumpulkan output traceroute pada lalu lintas TCP ke tujuan.

4. Dari prompt perintah konsol gateway, masukkan perintah yang sesuai untuk fungsi yang ingin Anda gunakan, dan ikuti petunjuknya.

Untuk mempelajari tentang perintah, masukkan **man + nama perintah** pada prompt perintah.

Melihat Status Sumber Daya Sistem Gateway Anda

Ketika gateway Anda dimulai, ia memeriksa inti CPU virtual, ukuran volume root, dan RAM. Ini kemudian menentukan apakah sumber daya sistem ini cukup untuk gateway Anda berfungsi dengan baik. Anda dapat melihat hasil pemeriksaan ini di konsol lokal gateway.

Untuk melihat status pemeriksaan sumber daya sistem

1. Masuk ke konsol lokal gateway Anda:
 - Untuk informasi selengkapnya tentang masuk ke konsol VMware ESXi, lihat. [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
 - Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
 - Untuk informasi selengkapnya tentang masuk ke konsol lokal KVM, lihat. [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Lihat Pemeriksaan Sumber Daya Sistem.

Setiap sumber daya menampilkan [OK], [PERINGATAN], atau [GAGAL], yang menunjukkan status sumber daya sebagai berikut:

Pesan	Deskripsi
[OK]	Sumber daya telah lulus pemeriksaan sumber daya sistem.
[PERINGATAN]	Sumber daya tidak memenuhi persyaratan yang disarankan, tetapi gateway Anda dapat terus berfungsi. Storage Gateway menampilkan pesan yang menjelaskan hasil pemeriksaan sumber daya.
[GAGAL]	Sumber daya tidak memenuhi persyaratan minimum. Gateway Anda mungkin tidak berfungsi dengan baik. Storage Gateway menampilkan pesan yang menjelaskan hasil pemeriksaan sumber daya.

Konsol juga menampilkan jumlah kesalahan dan peringatan di sebelah opsi menu centang sumber daya.

Mengkonfigurasi Adaptor Jaringan untuk Gateway Anda

Secara default, Storage Gateway dikonfigurasi untuk menggunakan jenis adaptor jaringan E1000, tetapi Anda dapat mengkonfigurasi ulang gateway Anda untuk menggunakan adaptor jaringan VMXNET3 (10 GbE). Anda juga dapat mengkonfigurasi Storage Gateway sehingga dapat diakses oleh lebih dari satu alamat IP. Anda melakukan ini dengan mengonfigurasi gateway Anda untuk menggunakan lebih dari satu adaptor jaringan.

Topik

- [Mengkonfigurasi Gateway Anda untuk Menggunakan Adaptor Jaringan VMXNET3](#)
- [Mengkonfigurasi Gateway Anda untuk Beberapa NIC](#)

Mengkonfigurasi Gateway Anda untuk Menggunakan Adaptor Jaringan VMXNET3

Storage Gateway mendukung jenis adaptor jaringan E1000 di host hypervisor VMware ESXi dan Microsoft Hyper-V. Namun, jenis adaptor jaringan VMXNET3 (10 GbE) hanya didukung di hypervisor VMware ESXi. Jika gateway Anda di-host pada hypervisor VMware ESXi, Anda dapat mengkonfigurasi ulang gateway Anda untuk menggunakan jenis adaptor VMXNET3 (10 GbE). Untuk informasi lebih lanjut tentang adaptor ini, lihat situs web [VMware](#).

Important

Untuk memilih VMXNET3, tipe sistem operasi tamu Anda harus Other Linux64.

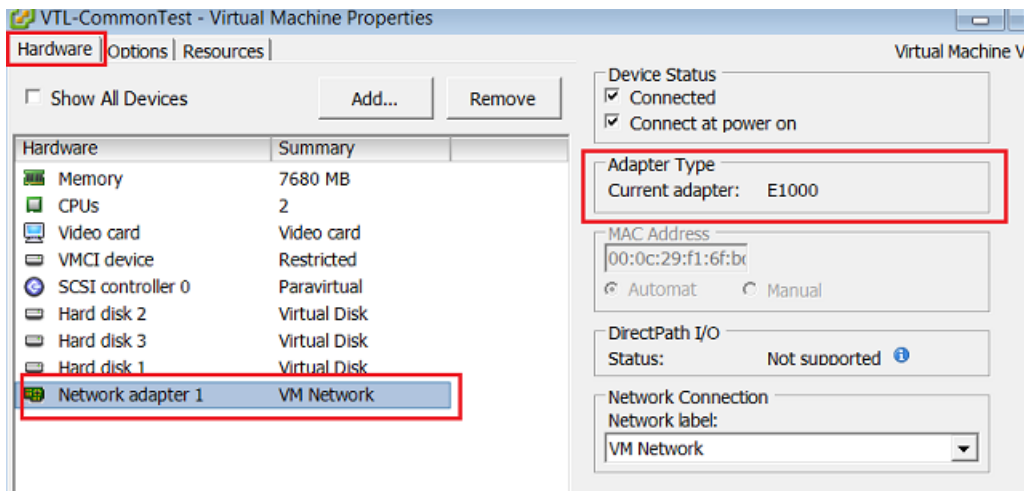
Berikut adalah langkah-langkah yang Anda ambil untuk mengonfigurasi gateway Anda untuk menggunakan adaptor VMXNET3:

1. Hapus adaptor E1000 default.
2. Tambahkan adaptor VMXNET3.
3. Mulai ulang gateway Anda.
4. Konfigurasi adaptor untuk jaringan.

Detail tentang cara melakukan setiap langkah berikut.

Untuk menghapus adaptor E1000 default dan mengkonfigurasi gateway Anda untuk menggunakan adaptor VMXNET3

1. Di VMware, buka menu konteks (klik kanan) untuk gateway Anda dan pilih Edit Pengaturan.
2. Di jendela Virtual Machine Properties, pilih tab Hardware.
3. Untuk Perangkat Keras, pilih Adaptor jaringan. Perhatikan bahwa adaptor saat ini adalah E1000 di bagian Jenis Adaptor. Anda akan mengganti adaptor ini dengan adaptor VMXNET3.



4. Pilih adaptor jaringan E1000, lalu pilih Hapus. Dalam contoh ini, adaptor jaringan E1000 adalah Adaptor jaringan 1.

Note

Meskipun Anda dapat menjalankan adaptor jaringan E1000 dan VMXNET3 di gateway Anda secara bersamaan, kami tidak menyarankan melakukannya karena dapat menyebabkan masalah jaringan.

5. Pilih Tambah untuk membuka wizard Tambah Perangkat Keras.
6. Pilih Adaptor Ethernet, lalu pilih Berikutnya.
7. Di wizard Jenis Jaringan, pilih **VMXNET3** Jenis Adaptor, lalu pilih Berikutnya.
8. Di wizard properti Mesin Virtual, verifikasi di bagian Jenis Adaptor bahwa Adaptor Saat Ini diatur ke VMXNET3, lalu pilih OK.
9. Di klien VMware vSphere, matikan gateway Anda.
10. Di klien VMware vSphere, restart gateway Anda.

Setelah gateway Anda restart, konfigurasi ulang adaptor yang baru saja Anda tambahkan untuk memastikan konektivitas jaringan ke internet terjalin.

Untuk mengkonfigurasi adaptor untuk jaringan

1. Di klien vSphere, pilih tab Konsol untuk memulai konsol lokal. Gunakan kredensial login default untuk masuk ke konsol lokal gateway untuk tugas konfigurasi ini. Untuk selengkapnya tentang cara masuk menggunakan kredensial default, lihat [Masuk ke Konsol Lokal Menggunakan Kredensial Default ke Konsol Lokal Menggunakan Kredensial Default](#).
2. Pada prompt, masukkan angka yang sesuai untuk memilih Konfigurasi Jaringan.
3. Pada prompt, masukkan angka yang sesuai untuk memilih Reset semua ke DHCP, dan kemudian masukkan **y** (untuk ya) pada prompt untuk mengatur semua adaptor untuk menggunakan Dynamic Host Configuration Protocol (DHCP). Semua adaptor yang tersedia diatur untuk menggunakan DHCP.

Jika gateway Anda sudah diaktifkan, Anda harus mematikannya dan memulai ulang dari Storage Gateway Management Console. Setelah gateway restart, Anda harus menguji konektivitas jaringan ke internet. Untuk informasi tentang cara menguji konektivitas jaringan, lihat [Menguji Koneksi Gateway Anda ke Internet](#).

Mengkonfigurasi Gateway Anda untuk Beberapa NIC

Jika Anda mengonfigurasi gateway Anda untuk menggunakan beberapa adaptor jaringan (NIC), itu dapat diakses oleh lebih dari satu alamat IP. Anda mungkin ingin melakukan hal ini dalam situasi berikut:

- Memaksimalkan throughput — Anda mungkin ingin memaksimalkan throughput ke gateway saat adaptor jaringan menjadi hambatan.
- Pemisahan aplikasi — Anda mungkin perlu memisahkan cara aplikasi Anda menulis ke volume gateway. Misalnya, Anda mungkin memilih untuk memiliki aplikasi penyimpanan penting secara eksklusif menggunakan satu adaptor tertentu yang ditentukan untuk gateway Anda.
- Kendala jaringan — Lingkungan aplikasi Anda mungkin mengharuskan Anda menyimpan target iSCSI Anda dan inisiator yang terhubung ke mereka dalam jaringan terisolasi yang berbeda dari jaringan tempat gateway berkomunikasi. AWS

Dalam kasus penggunaan multi-adaptor yang khas, satu adaptor dikonfigurasi sebagai rute yang digunakan gateway untuk berkomunikasi AWS (yaitu, sebagai gateway default). Kecuali untuk adaptor yang satu ini, inisiator harus berada di subnet yang sama dengan adaptor yang berisi target iSCSI yang mereka sambungkan. Jika tidak, komunikasi dengan target yang dituju mungkin tidak mungkin dilakukan. Jika target dikonfigurasi pada adaptor yang sama yang digunakan untuk komunikasi dengan AWS, lalu lintas iSCSI untuk target itu AWS dan lalu lintas akan mengalir melalui adaptor yang sama.

Saat Anda mengonfigurasi satu adaptor untuk terhubung ke konsol Storage Gateway dan kemudian menambahkan adaptor kedua, Storage Gateway secara otomatis mengonfigurasi tabel rute untuk menggunakan adaptor kedua sebagai rute pilihan. Untuk petunjuk tentang cara mengkonfigurasi beberapa adaptor, lihat bagian berikut.

- [Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Host VMware ESXi](#)
- [Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Microsoft Hyper-V Host](#)

Melakukan Tugas di Konsol Lokal Amazon EC2

Beberapa tugas pemeliharaan mengharuskan Anda masuk ke konsol lokal saat menjalankan gateway yang diterapkan pada instans Amazon EC2. Bagian ini menjelaskan cara masuk ke konsol lokal dan melakukan tugas pemeliharaan.

Topik

- [Masuk ke Konsol Lokal Amazon EC2 Gateway](#)
- [Merutekan gateway Anda yang diterapkan di EC2 melalui proxy HTTP](#)
- [Menguji konektivitas jaringan gateway Anda](#)
- [Melihat status sumber daya sistem gateway Anda](#)
- [Menjalankan perintah Storage Gateway di konsol lokal](#)

Masuk ke Konsol Lokal Amazon EC2 Gateway

Anda dapat terhubung ke instans Amazon EC2 menggunakan klien Secure Shell (SSH). Untuk informasi selengkapnya, lihat [Connect to Your Instance](#) di Panduan Pengguna Amazon EC2. Untuk menghubungkan dengan cara ini, Anda akan memerlukan key pair SSH yang Anda tentukan saat meluncurkan instance. Untuk informasi tentang pasangan kunci Amazon EC2, lihat [Pasangan Kunci Amazon EC2 di Panduan Pengguna Amazon EC2](#).

Untuk masuk ke konsol lokal gateway

1. Masuk ke konsol lokal Anda. Jika Anda terhubung ke instans EC2 Anda dari komputer Windows, masuk sebagai admin.
2. Setelah Anda masuk, Anda melihat menu utama AWS Storage Gateway - Configuration, dari mana Anda dapat melakukan berbagai tugas.

Untuk mempelajari tentang tugas ini	Lihat Topik Ini
Konfigurasi proxy SOCKS untuk gateway Anda	Merutekan gateway Anda yang diterapkan di EC2 melalui proxy HTTP
Uji konektivitas jaringan	Menguji konektivitas jaringan gateway Anda
Jalankan perintah konsol Storage Gateway	Menjalankan perintah Storage Gateway di konsol lokal
Lihat pemeriksaan sumber daya sistem	Melihat status sumber daya sistem gateway Anda.

Untuk mematikan gateway, masuk **0**.

Untuk keluar dari sesi konfigurasi, masukkan **X**.

Merutekan gateway Anda yang diterapkan di EC2 melalui proxy HTTP

Storage Gateway mendukung konfigurasi proxy Socket Secure versi 5 (SOCKS5) antara gateway yang digunakan di Amazon EC2 dan AWS.

Jika gateway Anda harus menggunakan server proxy untuk berkomunikasi ke internet, maka Anda perlu mengkonfigurasi pengaturan proxy HTTP untuk gateway Anda. Anda melakukan ini dengan menentukan alamat IP dan nomor port untuk host yang menjalankan proxy Anda. Setelah Anda melakukannya, Storage Gateway merutekan semua lalu lintas AWS endpoint melalui server proxy Anda. Komunikasi antara gateway dan titik akhir dienkripsi, bahkan saat menggunakan proxy HTTP.

Untuk merutekan lalu lintas internet gateway Anda melalui server proxy lokal

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, lihat [Masuk ke Konsol Lokal Amazon EC2 Gateway](#).

2. Dari menu utama AWS Appliance Activation - Configuration, masukkan angka yang sesuai untuk memilih Configure HTTP Proxy.
3. Dari menu AWS Appliance Activation HTTP Proxy Configuration, masukkan angka yang sesuai untuk tugas yang ingin Anda lakukan:
 - Konfigurasi HTTP proxy - Anda akan perlu untuk menyediakan nama host dan port untuk menyelesaikan konfigurasi.
 - Lihat konfigurasi proxy HTTP saat ini - Jika proxy HTTP tidak dikonfigurasi, pesan akan HTTP Proxy not configured ditampilkan. Jika proxy HTTP dikonfigurasi, nama host dan port proxy akan ditampilkan.
 - Hapus konfigurasi proxy HTTP - Pesan HTTP Proxy Configuration Removed ditampilkan.

Menguji konektivitas jaringan gateway Anda

Anda dapat menggunakan konsol lokal gateway Anda untuk menguji konektivitas jaringan Anda. Tes ini dapat berguna ketika Anda memecahkan masalah jaringan dengan gateway Anda.

Untuk menguji konektivitas gateway Anda

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, lihat [Masuk ke Konsol Lokal Amazon EC2 Gateway](#).
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Uji Konektivitas Jaringan.

Jika gateway Anda telah diaktifkan, tes konektivitas segera dimulai. Untuk gateway yang belum diaktifkan, Anda harus menentukan jenis titik akhir dan Wilayah AWS seperti yang dijelaskan dalam langkah-langkah berikut.

3. Jika gateway Anda belum diaktifkan, masukkan angka yang sesuai untuk memilih jenis titik akhir untuk gateway Anda.
4. Jika Anda memilih jenis titik akhir publik, masukkan angka yang sesuai untuk memilih Wilayah AWS yang ingin Anda uji. Untuk didukung Wilayah AWS dan daftar titik akhir AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat [AWS Storage Gateway titik akhir dan kuota](#) di Referensi Umum AWS

Saat pengujian berlangsung, setiap titik akhir menampilkan [LULUS] atau [GAGAL], yang menunjukkan status koneksi sebagai berikut:

Pesan	Deskripsi
[LULUS]	Storage Gateway memiliki konektivitas jaringan.
[GAGAL]	Storage Gateway tidak memiliki konektivitas jaringan.

Melihat status sumber daya sistem gateway Anda

Ketika gateway Anda dimulai, ia memeriksa inti CPU virtual, ukuran volume root, dan RAM. Ini kemudian menentukan apakah sumber daya sistem ini cukup untuk gateway Anda berfungsi dengan baik. Anda dapat melihat hasil pemeriksaan ini di konsol lokal gateway.

Untuk melihat status pemeriksaan sumber daya sistem

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, lihat [Masuk ke Konsol Lokal Amazon EC2 Gateway](#).
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Lihat Pemeriksaan Sumber Daya Sistem.

Setiap sumber daya menampilkan [OK], [PERINGATAN], atau [GAGAL], yang menunjukkan status sumber daya sebagai berikut:

Pesan	Deskripsi
[Oke]	Sumber daya telah lulus pemeriksaan sumber daya sistem.
[PERINGATAN]	Sumber daya tidak memenuhi persyaratan yang disarankan, tetapi gateway Anda dapat terus berfungsi. Storage Gateway menampilkan pesan yang menjelaskan hasil pemeriksaan sumber daya.

Pesan	Deskripsi
[GAGAL]	Sumber daya tidak memenuhi persyaratan minimum. Gateway Anda mungkin tidak berfungsi dengan baik. Storage Gateway menampilkan pesan yang menjelaskan hasil pemeriksaan sumber daya.

Konsol juga menampilkan jumlah kesalahan dan peringatan di sebelah opsi menu centang sumber daya.

Menjalankan perintah Storage Gateway di konsol lokal



AWS Storage Gateway Konsol membantu menyediakan lingkungan yang aman untuk mengonfigurasi dan mendiagnosis masalah dengan gateway Anda. Dengan menggunakan perintah konsol, Anda dapat melakukan tugas pemeliharaan seperti menyimpan tabel perutean atau menghubungkan ke AWS Support.

Untuk menjalankan konfigurasi atau perintah diagnostik

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, lihat [Masuk ke Konsol Lokal Amazon EC2 Gateway](#).
2. Dari menu utama AWS Appliance Activation - Configuration, masukkan angka yang sesuai untuk memilih Gateway Console.
3. Dari prompt perintah konsol gateway, masukkanh.

Konsol menampilkan menu AVAILABLE COMMANDS, yang mencantumkan perintah yang tersedia:

Perintah	Fungsi
menggali	Kumpulkan output dari penggalian untuk pemecahan masalah DNS.
keluar	Kembali ke menu Konfigurasi.

Perintah	Fungsi
-h	Tampilkan daftar perintah yang tersedia.
ifconfig	Lihat atau konfigurasi antarmuka jaringan. <div data-bbox="834 386 1507 701" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus.</p> </div>
ip	Menampilkan/memanipulasi routing, perangkat, dan terowongan. <div data-bbox="834 863 1507 1178" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus.</p> </div>
iptables	Alat administrasi untuk penyaringan paket IPv4 dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.
nping	Kumpulkan output dari nping untuk pemecahan masalah jaringan.
open-support-channel	Connect to AWS Support
simpan-iptables	Pertahankan tabel IP.
save-routing-table	Simpan entri tabel routing yang baru ditambahkan.

Perintah	Fungsi
sslcheck	Periksa validitas SSL untuk pemecahan masalah jaringan.
tcptraceroute	Kumpulkan output traceroute pada lalu lintas TCP ke tujuan.

4. Dari prompt perintah konsol gateway, masukkan perintah yang sesuai untuk fungsi yang ingin Anda gunakan, dan ikuti petunjuknya.

Untuk mempelajari tentang perintah, masukkan nama perintah diikuti dengan `-h` opsi, misalnya: `sslcheck -h`.

Mengakses Konsol Lokal Gateway

Cara Anda mengakses konsol lokal VM Anda tergantung pada jenis Hypervisor tempat Anda menerapkan VM gateway Anda. Di bagian ini, Anda dapat menemukan informasi tentang cara mengakses konsol lokal VM menggunakan Linux Kernel-based Virtual Machine (KVM), VMware ESXi, dan Microsoft Hyper-V Manager.

Topik

- [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)
- [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
- [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)

Mengakses Konsol Lokal Gateway dengan Linux KVM

Ada berbagai cara untuk mengkonfigurasi mesin virtual yang berjalan di KVM, tergantung pada distribusi Linux yang digunakan. Petunjuk untuk mengakses opsi konfigurasi KVM dari baris perintah ikuti. Instruksi mungkin berbeda tergantung pada implementasi KVM Anda.

Untuk mengakses konsol lokal gateway Anda dengan KVM

1. Gunakan perintah berikut untuk membuat daftar VM yang saat ini tersedia di KVM.

```
# virsh list
```

Anda dapat memilih VM yang tersedia dengan `Id`.

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

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

- Gunakan perintah berikut untuk mengakses konsol lokal.

```
# virsh console VM_Id
```

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

AWS Appliance

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

- Untuk mendapatkan kredensial default untuk masuk ke konsol lokal, lihat. [Masuk ke Konsol Lokal Menggunakan Kredensial Default](#)
- Setelah Anda masuk, Anda dapat mengaktifkan dan mengkonfigurasi gateway Anda.

```
AWS Appliance Activation - Configuration

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

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

0: Get activation key

Press "x" to exit session

Enter command: _
```

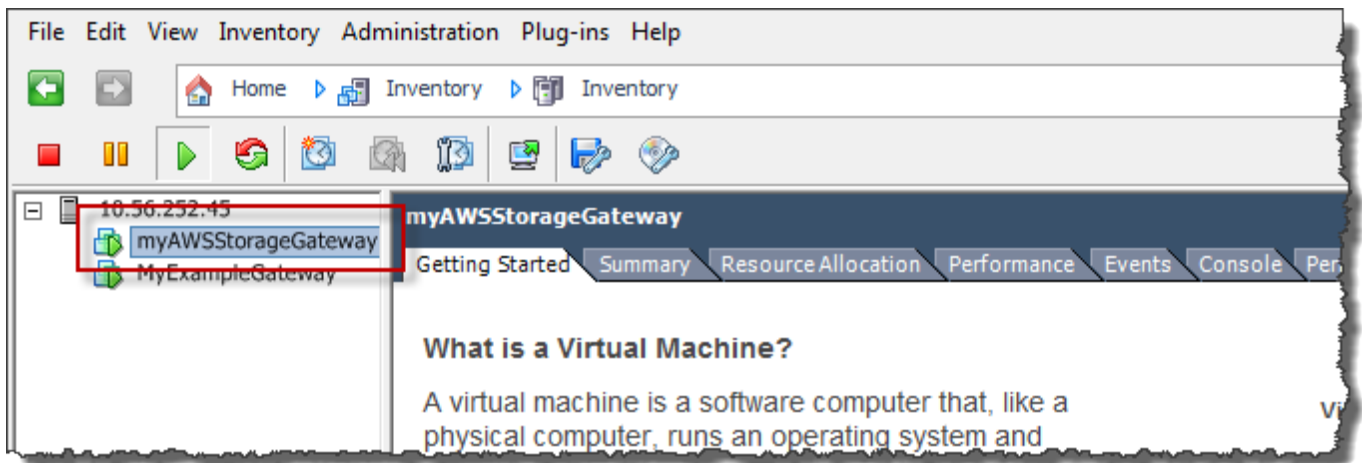
Mengakses Konsol Lokal Gateway dengan VMware ESXi

Untuk mengakses konsol lokal gateway Anda dengan VMware ESXi

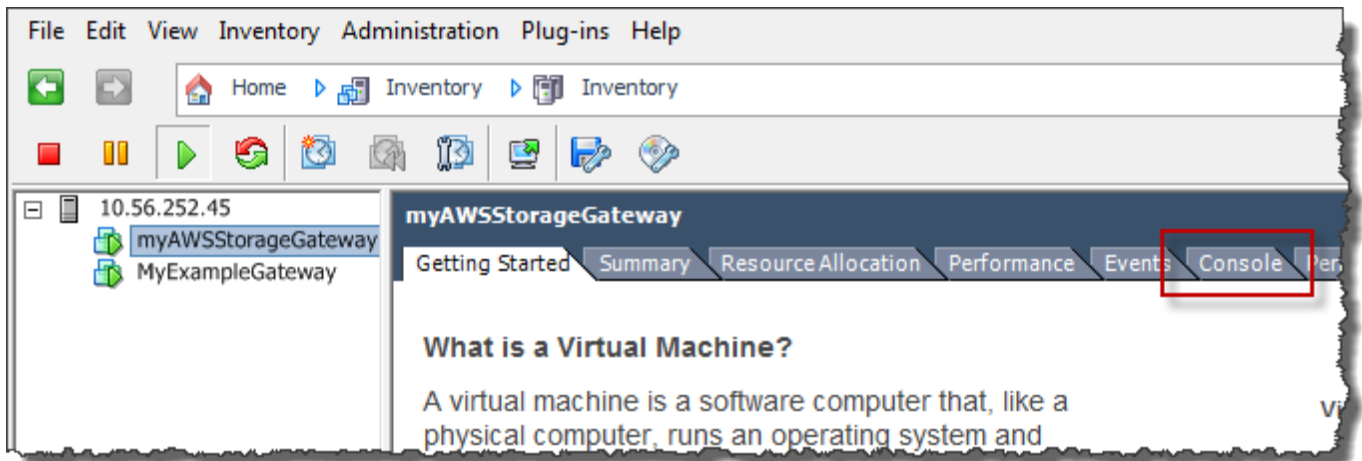
1. Di klien VMware vSphere, pilih VM gateway Anda.
2. Pastikan gateway dihidupkan.

Note

Jika VM gateway Anda dihidupkan, ikon panah hijau muncul dengan ikon VM, seperti yang ditunjukkan pada gambar berikut. Jika VM gateway Anda tidak dihidupkan, Anda dapat menyalakannya dengan memilih ikon Power On hijau pada menu Toolbar.



3. Pilih tab Konsol.



Setelah beberapa saat, VM siap untuk Anda masuk.

Note

Untuk melepaskan kursor dari jendela konsol, tekan Ctrl+Alt.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

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

localhost login: _
```

4. Untuk masuk menggunakan kredensial default, lanjutkan ke prosedur. [Masuk ke Konsol Lokal Menggunakan Kredensial Default](#)

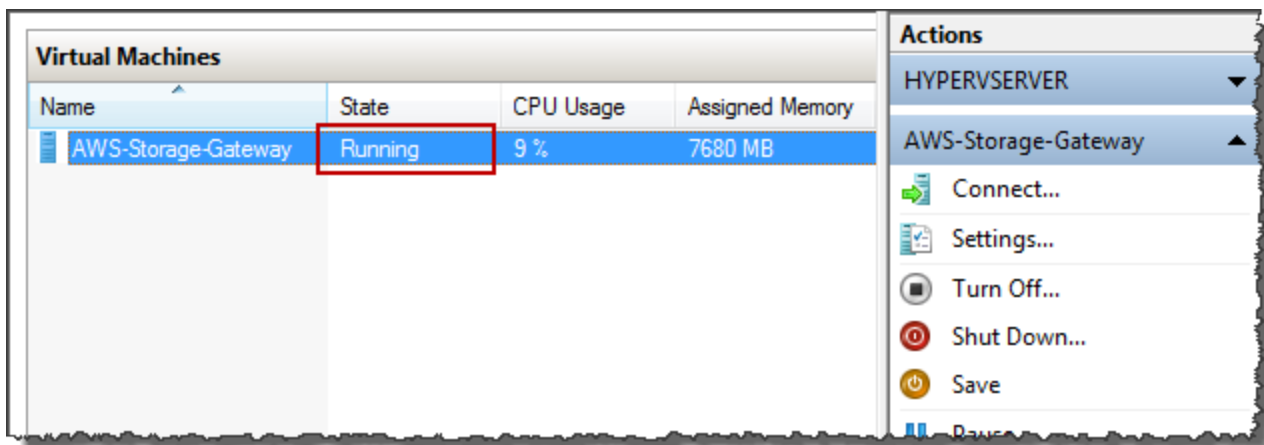
Akses Konsol Lokal Gateway dengan Microsoft Hyper-V

Untuk mengakses konsol lokal gateway Anda (Microsoft Hyper-V)

1. Dalam daftar Mesin Virtual Microsoft Hyper-V Manager, pilih VM gateway Anda.
2. Pastikan gateway dihidupkan.

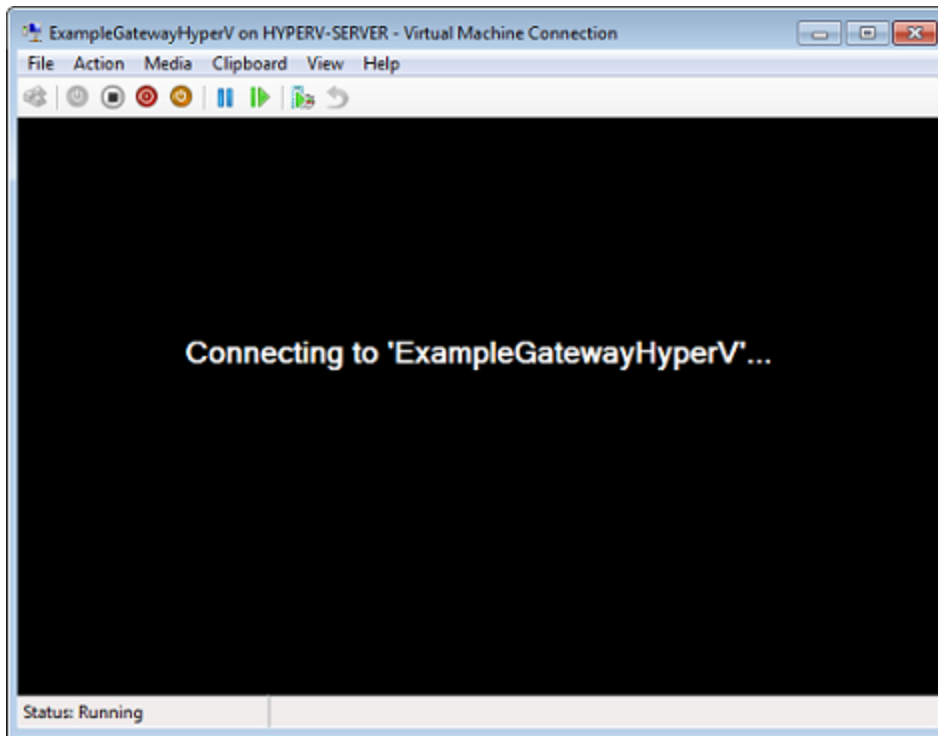
Note

Jika VM gateway Anda dihidupkan, Running ditampilkan sebagai Status VM, seperti yang ditunjukkan pada gambar berikut. Jika VM gateway Anda tidak diaktifkan, Anda dapat menyalakannya dengan memilih Mulai di panel Tindakan.



3. Di panel Actions, pilih Connect.

Jendela Virtual Machine Connection muncul. Jika jendela otentikasi muncul, ketikkan kredensial masuk yang diberikan kepada Anda oleh administrator hypervisor.



Setelah beberapa saat, VM siap untuk Anda masuk.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

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

localhost login: _
```

4. Untuk masuk menggunakan kredensial default, lanjutkan ke prosedur. [Masuk ke Konsol Lokal Menggunakan Kredensial Default](#)

Mengkonfigurasi Adaptor Jaringan untuk Gateway Anda

Di bagian ini Anda dapat menemukan informasi tentang caranya konfigurasi beberapa adapter jaringan untuk gateway Anda.

Topik

- [Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Host VMware ESXi](#)
- [Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Microsoft Hyper-V Host](#)

Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Host VMware ESXi

Prosedur berikut mengasumsikan bahwa VM gateway Anda sudah memiliki satu adaptor jaringan yang ditentukan, dan menjelaskan cara menambahkan adaptor pada VMware ESXi.

Untuk mengkonfigurasi gateway Anda untuk menggunakan adaptor jaringan tambahan di host VMware ESXi

1. Matikan pintu gerbangnya.
2. Di klien VMware vSphere, pilih VM gateway Anda.

VM dapat tetap dihidupkan untuk prosedur ini.

3. Di klien, buka menu konteks (klik kanan) untuk VM gateway Anda, dan pilih Edit Pengaturan.
4. Pada tab Hardware pada kotak dialog Virtual Machine Properties, pilih Tambah untuk menambahkan perangkat.
5. Ikuti panduan Add Hardware untuk menambahkan adaptor jaringan.
 - a. Di panel Jenis Perangkat, pilih Adaptor Ethernet untuk menambahkan adaptor, lalu pilih Berikutnya.
 - b. Di panel Network Type, pastikan Connect at power on dipilih untuk Type, lalu pilih Next.

Kami menyarankan Anda menggunakan adaptor jaringan VMXNET3 dengan Storage Gateway. Untuk informasi selengkapnya tentang jenis adaptor yang mungkin muncul di daftar adaptor, lihat Jenis Adaptor Jaringan di Dokumentasi Server [ESXi dan vCenter](#).

- c. Di panel Siap Selesai, tinjau informasinya, lalu pilih Selesai.
6. Pilih tab Ringkasan untuk VM, dan pilih Lihat Semua di sebelah kotak Alamat IP. Jendela Alamat IP Mesin Virtual menampilkan semua alamat IP yang dapat Anda gunakan untuk mengakses gateway. Konfirmasikan bahwa alamat IP kedua terdaftar untuk gateway.

Note

Mungkin perlu beberapa saat agar perubahan adaptor diterapkan dan informasi ringkasan VM disegarkan.

7. Di konsol Storage Gateway, nyalakan gateway.
8. Di panel Navigasi konsol Storage Gateway, pilih Gateways dan pilih gateway tempat Anda menambahkan adaptor. Konfirmasikan bahwa alamat IP kedua tercantum di tab Detail.

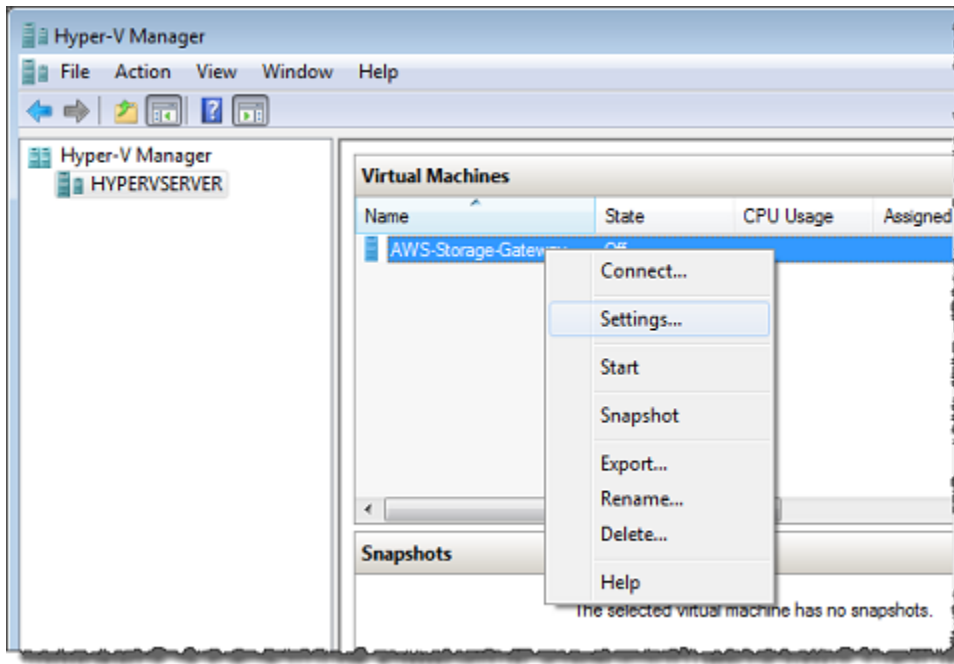
Untuk informasi tentang tugas konsol lokal yang umum untuk host VMware, Hyper-V, dan KVM, lihat [Melakukan Tugas di Konsol Lokal VM](#)

Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Microsoft Hyper-V Host

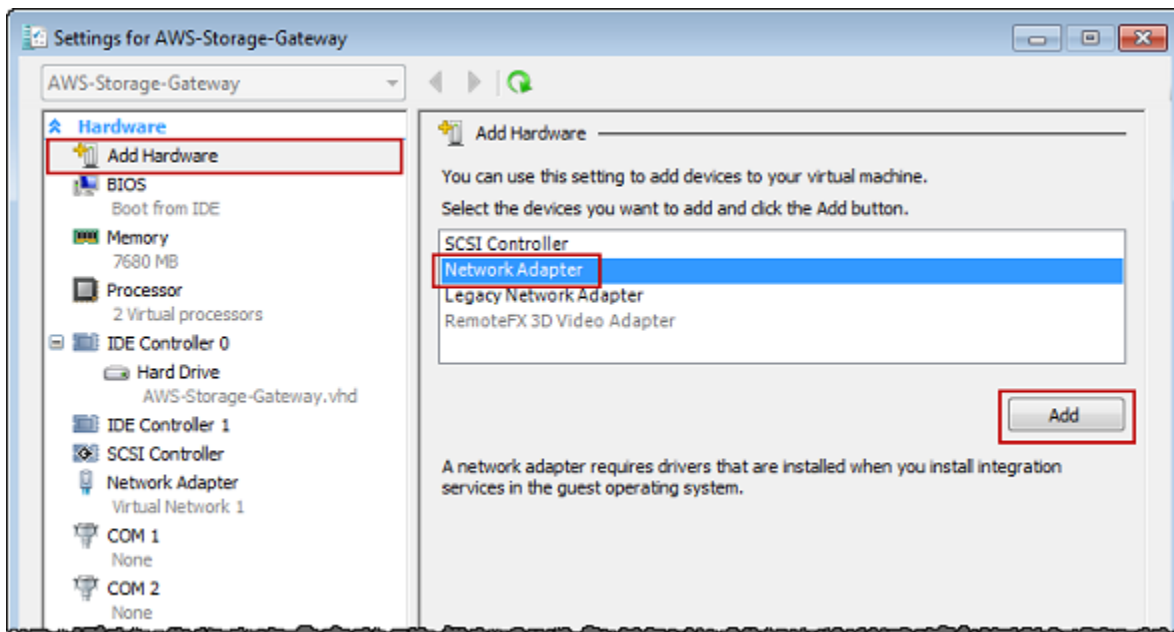
Prosedur berikut mengasumsikan bahwa VM gateway Anda sudah memiliki satu adaptor jaringan yang ditentukan dan Anda menambahkan adaptor kedua. Prosedur ini menunjukkan cara menambahkan adaptor untuk host Microsoft Hyper-V.

Untuk mengonfigurasi gateway Anda untuk menggunakan adaptor jaringan tambahan di Microsoft Hyper-V Host

1. Pada konsol Storage Gateway, matikan gateway. Untuk petunjuk, lihat [Untuk menghentikan Tape Gateway](#).
2. Di Microsoft Hyper-V Manager, pilih VM gateway Anda.
3. Jika VM belum dimatikan, buka menu konteks (klik kanan) untuk gateway Anda dan pilih Matikan.
4. Di klien, buka menu konteks untuk VM gateway Anda dan pilih Pengaturan.

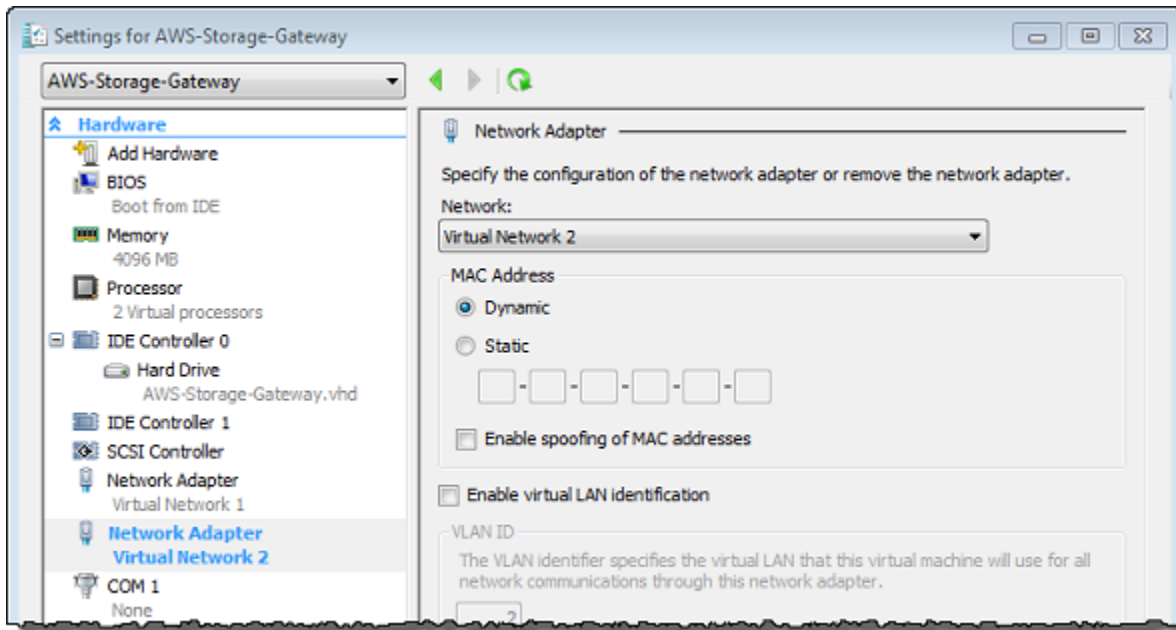


5. Di kotak dialog Pengaturan untuk VM, untuk Perangkat Keras, pilih Tambahkan Perangkat Keras.
6. Di panel Tambahkan Perangkat Keras, pilih Adaptor Jaringan, lalu pilih Tambah untuk menambahkan perangkat.



7. Konfigurasi adaptor jaringan, lalu pilih Terapkan untuk menerapkan pengaturan.

Dalam contoh berikut, Virtual Network 2 dipilih untuk adaptor baru.



8. Di kotak dialog Pengaturan, untuk Perangkat Keras, konfirmasi bahwa adaptor kedua telah ditambahkan, lalu pilih OK.
9. Pada konsol Storage Gateway, nyalakan gateway. Untuk petunjuk, lihat [Untuk memulai Tape Gateway](#).
10. Di panel Navigasi pilih Gateway, lalu pilih gateway tempat Anda menambahkan adaptor. Konfirmasi bahwa alamat IP kedua tercantum di tab Detail.

Note

Contoh perintah pemasangan yang disediakan pada halaman info untuk berbagi file di konsol Storage Gateway akan selalu menyertakan alamat IP adaptor jaringan yang terbaru ditambahkan ke gateway terkait berbagi file.

Untuk informasi tentang tugas konsol lokal yang umum untuk host VMware, Hyper-V, dan KVM, lihat [Melakukan Tugas di Konsol Lokal VM](#)

Menghapus Gateway Anda dengan Menggunakan AWS Storage Gateway Konsol dan Menghapus Sumber Daya Terkait

Jika Anda tidak berencana untuk terus menggunakan gateway Anda, pertimbangkan untuk menghapus gateway dan sumber daya yang terkait. Menghapus sumber daya menghindari biaya untuk sumber daya yang tidak Anda rencanakan untuk terus digunakan dan membantu mengurangi tagihan bulanan Anda.

Saat Anda menghapus gateway, gateway tidak lagi muncul di AWS Storage Gateway Management Console dan koneksi iSCSI ke inisiator ditutup. Prosedur untuk menghapus gateway adalah sama untuk semua jenis gateway; Namun, tergantung pada jenis gateway yang ingin Anda hapus dan host yang digunakan, Anda mengikuti instruksi khusus untuk menghapus sumber daya terkait.

Note

Saat Anda menghapus Gateway Tape, kaset apa pun yang saat ini dalam AVAILABLE status juga akan dihapus, dan data apa pun pada kaset tersebut akan hilang. Jika Anda ingin menyimpan data dari kaset yang digunakan oleh gateway yang ingin Anda hapus, Anda harus mengarsipkan kaset sebelum menghapus gateway. Untuk informasi selengkapnya, lihat [Mengarsipkan Kaset Virtual](#).

Anda dapat menghapus gateway menggunakan konsol Storage Gateway atau secara terprogram. Anda dapat menemukan informasi berikut tentang cara menghapus gateway menggunakan konsol Storage Gateway. Jika Anda ingin menghapus gateway secara terprogram, lihat Referensi [AWS Storage Gateway API](#).

Topik

- [Menghapus Gateway Anda dengan Menggunakan Storage Gateway Console](#)
- [Menghapus Sumber Daya dari Gateway yang Diterapkan di Tempat](#)
- [Menghapus Sumber Daya dari Gateway yang Diterapkan di Instans Amazon EC2](#)

Menghapus Gateway Anda dengan Menggunakan Storage Gateway Console

Prosedur untuk menghapus gateway adalah sama untuk semua jenis gateway. Namun, tergantung pada jenis gateway yang ingin Anda hapus dan host tempat gateway digunakan, Anda mungkin harus melakukan tugas tambahan untuk menghapus sumber daya yang terkait dengan gateway. Menghapus sumber daya ini membantu Anda menghindari membayar sumber daya yang tidak Anda rencanakan untuk digunakan.

Note

Untuk gateway yang digunakan pada instans Amazon EC2, instans akan tetap ada hingga Anda menghapusnya.

Untuk gateway yang digunakan pada mesin virtual (VM), setelah Anda menghapus gateway, VM gateway masih ada di lingkungan virtualisasi Anda. Untuk menghapus VM, gunakan klien VMware vSphere, Microsoft Hyper-V Manager, atau klien Linux Kernel-based Virtual Machine (KVM) untuk terhubung ke host dan menghapus VM. Perhatikan bahwa Anda tidak dapat menggunakan kembali VM gateway yang dihapus untuk mengaktifkan gateway baru.

Untuk menghapus gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Pilih Gateway, lalu pilih satu atau beberapa gateway untuk dihapus.
3. Untuk Tindakan, pilih Hapus gateway. Kotak dialog konfirmasi muncul.

Warning

Sebelum Anda melakukan langkah ini, pastikan bahwa tidak ada aplikasi yang saat ini menulis ke volume gateway. Jika Anda menghapus gateway saat sedang digunakan, kehilangan data dapat terjadi. Ketika gateway dihapus, tidak ada cara untuk mendapatkannya kembali.

4. Pastikan Anda ingin menghapus gateway yang ditentukan, lalu ketik kata hapus di kotak konfirmasi, dan pilih Hapus.
5. (Opsional) Jika Anda ingin memberikan umpan balik tentang gateway yang dihapus, lengkapi kotak dialog umpan balik, lalu pilih Kirim. Jika tidak, pilih Lewati.

⚠ Important

Anda tidak lagi membayar biaya perangkat lunak setelah menghapus gateway, tetapi sumber daya seperti kaset virtual, snapshot Amazon Elastic Block Store (Amazon EBS), dan instans Amazon EC2 tetap ada. Anda akan terus ditagih untuk sumber daya ini. Anda dapat memilih untuk menghapus instans Amazon EC2 dan snapshot Amazon EBS dengan membatalkan langganan Amazon EC2 Anda. Jika Anda ingin mempertahankan langganan Amazon EC2, Anda dapat menghapus snapshot Amazon EBS menggunakan konsol Amazon EC2.

Menghapus Sumber Daya dari Gateway yang Diterapkan di Tempat

Anda dapat menggunakan petunjuk berikut untuk menghapus sumber daya dari gateway yang digunakan di lokasi.

Menghapus Sumber Daya dari Tape Gateway yang Digunakan di VM

Saat menghapus gateway—virtual tape library (VTL), Anda melakukan langkah pembersihan tambahan sebelum dan sesudah menghapus gateway. Langkah-langkah tambahan ini membantu Anda menghapus sumber daya yang tidak Anda butuhkan sehingga Anda tidak terus membayarnya.

Jika Tape Gateway yang ingin Anda hapus digunakan pada mesin virtual (VM), kami sarankan Anda mengambil tindakan berikut untuk membersihkan sumber daya.

⚠ Important

Sebelum menghapus Tape Gateway, Anda harus membatalkan semua operasi pengambilan tape dan mengeluarkan semua kaset yang diambil.

Setelah menghapus Tape Gateway, Anda harus menghapus sumber daya apa pun yang terkait dengan Tape Gateway yang tidak perlu Anda hindari untuk membayar sumber daya tersebut.

Saat Anda menghapus Tape Gateway, Anda dapat menemukan salah satu dari dua skenario.

- Tape Gateway terhubung ke AWS - Jika Tape Gateway terhubung AWS dan Anda menghapus gateway, target iSCSI yang terkait dengan gateway (yaitu, drive pita virtual dan pengubah media) tidak akan lagi tersedia.

- Tape Gateway tidak terhubung ke AWS - Jika Tape Gateway tidak terhubung AWS, misalnya jika VM yang mendasarinya dimatikan atau jaringan Anda mati, maka Anda tidak dapat menghapus gateway. Jika Anda mencoba melakukannya, setelah lingkungan Anda di-back up dan berjalan, Anda mungkin memiliki Tape Gateway yang berjalan di lokasi dengan target iSCSI yang tersedia. Namun, tidak ada data Tape Gateway yang akan diunggah ke, atau diunduh dari, AWS.

Jika Tape Gateway yang ingin Anda hapus tidak berfungsi, Anda harus menonaktifkannya terlebih dahulu sebelum menghapusnya, seperti yang dijelaskan berikut:

- Untuk menghapus kaset yang memiliki status RETRIEVED dari perpustakaan, keluarkan kaset menggunakan perangkat lunak cadangan Anda. Untuk petunjuk, lihat [Mengarsipkan Rekaman](#).

Setelah menonaktifkan Tape Gateway dan menghapus kaset, Anda dapat menghapus Tape Gateway. Untuk petunjuk tentang cara menghapus gateway, lihat [Menghapus Gateway Anda dengan Menggunakan Storage Gateway Console](#).

Jika Anda memiliki kaset yang diarsipkan, kaset itu tetap ada dan Anda terus membayar penyimpanan sampai Anda menghapusnya. Untuk instruksi tentang cara menghapus kaset dari arsip, lihat [Menghapus Kaset](#)

Important

Anda dikenakan biaya untuk penyimpanan minimal 90 hari untuk kaset virtual dalam arsip. Jika Anda mengambil rekaman virtual yang telah disimpan dalam arsip selama kurang dari 90 hari, Anda masih dikenakan biaya untuk penyimpanan 90 hari.

Menghapus Sumber Daya dari Gateway yang Diterapkan di Instans Amazon EC2

Jika Anda ingin menghapus gateway yang Anda gunakan pada instans Amazon EC2, sebaiknya Anda membersihkan AWS sumber daya yang digunakan dengan gateway, khususnya instans Amazon EC2, volume Amazon EBS apa pun, dan juga kaset jika Anda menggunakan Tape Gateway. Melakukannya membantu menghindari biaya penggunaan yang tidak diinginkan.

Menghapus Sumber Daya dari Tape Gateway Anda yang Digunakan di Amazon EC2

Jika Anda menggunakan Tape Gateway, kami sarankan Anda mengambil tindakan berikut untuk menghapus gateway dan membersihkan sumber dayanya:

1. Hapus semua kaset virtual yang telah Anda ambil ke Tape Gateway Anda. Untuk informasi selengkapnya, lihat [Menghapus Kaset](#).
2. Hapus semua kaset virtual dari perpustakaan kaset. Untuk informasi selengkapnya, lihat [Menghapus Kaset](#).
3. Hapus Tape Gateway. Untuk informasi selengkapnya, lihat [Menghapus Gateway Anda dengan Menggunakan Storage Gateway Console](#).
4. Hentikan semua instans Amazon EC2, dan hapus semua volume Amazon EBS. Untuk informasi selengkapnya, lihat [Membersihkan Instans dan Volume Anda](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.
5. Hapus semua kaset virtual yang diarsipkan. Untuk informasi selengkapnya, lihat [Menghapus Kaset](#).

Important

Anda dikenakan biaya untuk penyimpanan minimal 90 hari untuk kaset virtual di arsip. Jika Anda mengambil rekaman virtual yang telah disimpan dalam arsip selama kurang dari 90 hari, Anda masih dikenakan biaya untuk penyimpanan 90 hari.

Performa

Bagian ini menjelaskan kinerja Storage Gateway.

Topik

- [Panduan kinerja untuk Tape Gateways](#)
- [Mengoptimalkan Kinerja Gateway](#)
- [Menggunakan VMware vSphere Ketersediaan Tinggi dengan Storage Gateway](#)

Panduan kinerja untuk Tape Gateways

Di bagian ini, Anda dapat menemukan panduan konfigurasi untuk penyediaan perangkat keras untuk Tape Gateway VM Anda. Ukuran dan jenis instans Amazon EC2 yang tercantum dalam tabel adalah contoh, dan disediakan untuk referensi.

Konfigurasi	Tulis Throughput Gbps	Baca dari Cache Throughput Gbps	Baca dari Amazon Web Services Cloud Throughput Gbps
Platform Host: Contoh Amazon EC2— c5.4xlarge CPU: 16 vCPU RAM: 32 GB Disk root: 80 GB, io1 SSD, 4.000 IOPS Disk cache: RAID bergaris (2 x 500 GB, io1 EBS SSD, 25000 IOP) Unggah disk buffer: 450 GB, io1 SSD, 2000 IOPS Bandwidth jaringan ke cloud: 10 Gbps	2.3	4.0	2.2

Konfigurasi	Tulis Throughput Gbps	Baca dari Cache Throughput Gbps	Baca dari Amazon Web Services Cloud Throughput Gbps
Platform host: Alat Perangkat Keras Storage Gateway Disk cache: 2,5 TB Unggah disk penyangga: 2 TB Bandwidth jaringan ke cloud: 10 Gbps	2.3	8.8	3.8
Platform host: Amazon EC2Instance— c5d.9xlarge CPU: 36 vCPU RAM: 72 GB Disk root: 80 GB, io1 SSD, 4.000 IOPS Disk cache: Disk NVMe 900 GB Unggah disk buffer: 900 GB NVMe disk Bandwidth jaringan ke cloud: 10 Gbps	5.2	11.6	5.2

Konfigurasi	Tulis Throughput Gbps	Baca dari Cache Throughput Gbps	Baca dari Amazon Web Services Cloud Throughput Gbps
Platform host: Amazon EC2 Instance— c5d.metal CPU: 96 vCPU RAM: 192 GB Disk root: 80 GB, io1 SSD, 4.000 IOPS Disk cache: RAID bergaris (disk NVMe 2 x 900 GB) Unggah disk buffer: 900 GB NVMe disk Bandwidth jaringan ke cloud: 10 Gbps	5.2	11.6	7.2

Note

Kinerja ini dicapai dengan menggunakan ukuran blok 1 MB dan sepuluh tape drive secara bersamaan.

Konfigurasi EC2 pada tabel di atas hanya dimaksudkan untuk mewakili kinerja yang mungkin Anda capai di server fisik Anda sendiri dengan sumber daya serupa. Misalnya, konfigurasi EC2 menggunakan RAID bergaris dilakukan melalui mekanisme khusus yang umumnya tidak didukung oleh gateway kami di EC2. Untuk mencapai kinerja yang sama, Anda sebaiknya menggunakan pengontrol RAID perangkat keras yang terpasang ke server on-premise yang menjalankan gateway Anda.

Kinerja Anda mungkin bervariasi berdasarkan konfigurasi platform host dan bandwidth jaringan Anda.

Untuk meningkatkan kinerja throughput tulis dan baca Tape Gateway Anda, lihat [Optimalkan Pengaturan iSCSI](#), [Gunakan Ukuran Blok yang Lebih Besar untuk Tape Drives](#), dan [Optimalkan Kinerja Virtual Tape Drive di Perangkat Lunak Backup](#).

Mengoptimalkan Kinerja Gateway

Konfigurasi Server Gateway yang Direkomendasikan

Untuk mendapatkan performa terbaik dari gateway Anda, Storage Gateway merekomendasikan konfigurasi gateway berikut untuk server host gateway Anda:

- Setidaknya 64 core CPU fisik khusus
- Untuk Tape Gateway , perangkat keras Anda harus mendedikasikan jumlah RAM berikut:
 - Setidaknya 16 GiB RAM cadangan untuk gateway dengan ukuran cache hingga 16 TiB
 - Setidaknya 32 GiB RAM cadangan untuk gateway dengan ukuran cache 16 TiB hingga 32 TiB
 - Setidaknya 48 GiB RAM cadangan untuk gateway dengan ukuran cache 32 TiB hingga 64 TiB

Note

Untuk kinerja gateway yang optimal, Anda harus menyediakan setidaknya 32 GiB RAM.

- Disk 1, untuk digunakan sebagai cache gateway sebagai berikut:
 - Striped RAID (array redundan disk independen) yang terdiri dari SSD NVMe.
- Disk 2, untuk digunakan sebagai buffer upload gateway sebagai berikut:
 - Striped RAID terdiri dari NVMe SSD.
- Disk 3, untuk digunakan sebagai buffer upload gateway sebagai berikut:
 - Striped RAID terdiri dari NVMe SSD.
- Adaptor jaringan 1 dikonfigurasi pada jaringan VM 1:
 - Gunakan jaringan VM 1 dan tambahkan VMxNet3 (10 Gbps) untuk digunakan untuk konsumsi.
- Adaptor jaringan 2 dikonfigurasi pada jaringan VM 2:
 - Gunakan jaringan VM 2 dan tambahkan VMxNet3 (10 Gbps) yang akan digunakan untuk terhubung. AWS

Tambahkan Sumber Daya ke Gateway Anda

Hambatan berikut dapat mengurangi kinerja Tape Gateway Gateway Anda di bawah throughput berkelanjutan maksimum teoritis (bandwidth Anda ke cloud): AWS

- Jumlah inti CPU
- Cache/Unggah throughput disk buffer
- Jumlah RAM total
- Bandwidth jaringan untuk AWS
- Bandwidth jaringan dari inisiator ke gateway

Bagian ini berisi langkah-langkah yang dapat Anda ambil untuk mengoptimalkan kinerja gateway Anda. Panduan ini didasarkan pada penambahan sumber daya ke gateway atau server aplikasi Anda.

Anda dapat mengoptimalkan kinerja gateway dengan menambahkan sumber daya ke gateway Anda dengan satu atau beberapa cara berikut.

Gunakan disk berkinerja lebih tinggi

Cache dan upload buffer disk throughput dapat membatasi kinerja upload dan download gateway Anda. Jika gateway Anda menunjukkan kinerja secara signifikan di bawah yang diharapkan, pertimbangkan untuk meningkatkan cache dan mengunggah throughput disk buffer dengan:

- Menggunakan RAID bergaris seperti RAID 10 untuk meningkatkan throughput disk, idealnya dengan pengontrol RAID perangkat keras.


Note

RAID (redundan array disk independen) atau konfigurasi RAID bergaris disk khusus seperti RAID 10, adalah proses membagi badan data menjadi blok dan menyebarkan blok data di beberapa perangkat penyimpanan. Level RAID yang Anda gunakan memengaruhi kecepatan dan toleransi kesalahan yang tepat yang dapat Anda capai. Dengan menghapus beban kerja IO di beberapa disk, throughput keseluruhan perangkat RAID jauh lebih tinggi daripada disk anggota tunggal mana pun.

- Menggunakan disk berkinerja tinggi yang terpasang langsung

Untuk mengoptimalkan kinerja gateway, Anda dapat menambahkan disk berkinerja tinggi seperti solid-state drive (SSD) dan pengontrol NVMe. Anda juga dapat melampirkan disk virtual ke VM Anda langsung dari jaringan area penyimpanan (SAN) alih-alih Microsoft Hyper-V NTFS. Peningkatan kinerja disk umumnya menghasilkan throughput yang lebih baik dan lebih banyak operasi input/output per detik (IOPS).

Untuk mengukur throughput, gunakan `ReadBytes` dan `WriteBytes` metrik dengan statistik `Samples` Amazon CloudWatch. Misalnya, `Samples` statistik `ReadBytes` metrik selama periode sampel 5 menit dibagi 300 detik memberi Anda IOPS. Sebagai aturan umum, saat Anda meninjau metrik ini untuk gateway, cari throughput rendah dan tren IOPS rendah untuk menunjukkan kemacetan terkait disk. Untuk informasi selengkapnya tentang metrik gateway, lihat [Mengukur Kinerja Antara Tape Gateway Anda dan AWS](#).

 Note

CloudWatch metrik tidak tersedia untuk semua gateway. Untuk informasi tentang metrik gateway, lihat [Memantau Storage Gateway](#).

Tambahkan lebih banyak disk buffer unggah

Untuk mencapai throughput penulisan yang lebih tinggi, tambahkan setidaknya dua disk buffer unggah. Ketika data ditulis ke gateway, itu ditulis dan disimpan secara lokal pada disk buffer upload. Setelah itu, data lokal yang disimpan dibaca secara asinkron dari disk yang akan diproses dan diunggah. AWS Menambahkan lebih banyak disk buffer upload dapat mengurangi jumlah operasi I/O bersamaan yang dilakukan untuk setiap disk individu. Hal ini dapat mengakibatkan peningkatan throughput tulis ke gateway.

Back gateway virtual disk dengan disk fisik terpisah

Saat Anda menyediakan disk gateway, kami sangat menyarankan agar Anda tidak menyediakan disk lokal untuk buffer unggahan dan penyimpanan cache yang menggunakan disk penyimpanan fisik dasar yang sama. Misalnya, untuk VMware ESXi, sumber daya penyimpanan fisik yang mendasarinya direpresentasikan sebagai penyimpanan data. Saat Anda menyebarkan VM gateway, Anda memilih penyimpanan data untuk menyimpan file VM. Saat Anda menyediakan disk virtual (misalnya, sebagai buffer unggahan), Anda dapat menyimpan disk virtual di penyimpanan data yang sama dengan VM atau penyimpanan data yang berbeda.

Jika Anda memiliki lebih dari satu penyimpanan data, maka kami sangat menyarankan Anda memilih satu penyimpanan data untuk setiap jenis penyimpanan lokal yang Anda

buat. Penyimpanan data yang didukung oleh hanya satu disk fisik yang mendasarinya dapat menyebabkan kinerja yang buruk. Contohnya adalah ketika Anda menggunakan disk seperti itu untuk mendukung penyimpanan cache dan mengunggah buffer dalam pengaturan gateway. Demikian pula, penyimpanan data yang didukung oleh konfigurasi RAID yang kurang berkinerja tinggi seperti RAID 1 atau RAID 6 dapat menyebabkan kinerja yang buruk.

Tambahkan sumber daya CPU ke host gateway Anda

Persyaratan minimum untuk server host gateway adalah empat prosesor virtual. Untuk mengoptimalkan kinerja gateway, konfirmasi bahwa setiap prosesor virtual yang ditetapkan ke VM gateway didukung oleh inti CPU khusus. Selain itu, konfirmasi bahwa Anda tidak kelebihan langganan CPU server host.

Ketika Anda menambahkan CPU tambahan ke server host gateway Anda, Anda meningkatkan kemampuan pemrosesan gateway. Melakukan hal ini memungkinkan gateway Anda untuk menangani, secara paralel, baik menyimpan data dari aplikasi Anda ke penyimpanan lokal Anda dan mengunggah data ini ke Amazon S3. CPU tambahan juga membantu memastikan bahwa gateway Anda mendapatkan sumber daya CPU yang cukup saat host dibagikan dengan VM lain. Menyediakan sumber daya CPU yang cukup memiliki efek umum meningkatkan throughput.

Tingkatkan bandwidth antara gateway dan AWS cloud Anda

Meningkatkan bandwidth Anda ke dan dari AWS akan meningkatkan tingkat maksimum masuknya data ke gateway dan jalan keluar Anda ke cloud. AWS Ini dapat meningkatkan kinerja gateway Anda jika kecepatan jaringan adalah faktor pembatas dalam konfigurasi gateway Anda, daripada faktor lain seperti disk lambat atau bandwidth koneksi inisiator gateway yang buruk.

Bandwidth jaringan ke dan dari AWS menentukan kinerja rata-rata maksimum teoritis dari Tape Gateway Anda selama beban kerja berkelanjutan.

- Tingkat rata-rata di mana Anda dapat menulis data ke Tape Gateway Anda dalam interval yang lama tidak akan melebihi bandwidth unggahan Anda AWS.
- Tingkat rata-rata di mana Anda dapat membaca data dari Tape Gateway Anda dalam interval yang lama tidak akan melebihi bandwidth unduhan Anda AWS.

Note

Kinerja gateway yang Anda amati kemungkinan akan lebih rendah daripada bandwidth jaringan Anda karena faktor pembatas lain yang tercantum di sini, seperti throughput disk buffer cache/upload, jumlah inti CPU, jumlah RAM total, atau bandwidth antara inisiator

dan gateway Anda. Selain itu, operasi normal gateway Anda melibatkan banyak tindakan yang diambil untuk melindungi data Anda, yang dapat menyebabkan kinerja yang diamati kurang dari bandwidth jaringan Anda.

Optimalkan Pengaturan iSCSI

Anda dapat mengoptimalkan pengaturan iSCSI pada inisiator iSCSI Anda untuk mencapai kinerja I/O yang lebih tinggi. Kami merekomendasikan memilih 256 KiB untuk `MaxReceiveDataSegmentLength` dan `FirstBurstLength`, dan 1 MiB untuk `MaxBurstLength`. Untuk informasi selengkapnya tentang mengonfigurasi setelan iSCSI, lihat [Menyesuaikan Pengaturan iSCSI](#).

Note

Pengaturan yang direkomendasikan ini dapat memfasilitasi kinerja yang lebih baik secara keseluruhan. Namun, pengaturan iSCSI spesifik yang diperlukan untuk mengoptimalkan kinerja bervariasi tergantung pada perangkat lunak cadangan yang Anda gunakan. Untuk detailnya, lihat dokumentasi perangkat lunak cadangan Anda.

Gunakan Ukuran Blok yang Lebih Besar untuk Tape Drives

Untuk Tape Gateway, ukuran blok default untuk tape drive adalah 64 KB. Namun, Anda dapat meningkatkan ukuran blok hingga 1 MB untuk meningkatkan kinerja I/O.

Ukuran blok yang Anda pilih tergantung pada ukuran blok maksimum yang didukung perangkat lunak cadangan Anda. Kami menyarankan Anda mengatur ukuran blok tape drive di perangkat lunak cadangan Anda ke ukuran yang sebesar mungkin. Namun, ukuran blok ini tidak boleh lebih besar dari ukuran maksimum 1 MB yang didukung gateway.

Tape Gateways menegosiasikan ukuran blok untuk drive tape virtual agar secara otomatis cocok dengan apa yang diatur pada perangkat lunak cadangan. Ketika Anda meningkatkan ukuran blok pada perangkat lunak cadangan, kami sarankan Anda juga memeriksa pengaturan untuk memastikan bahwa inisiator host mendukung ukuran blok baru. Untuk informasi selengkapnya, lihat dokumentasi untuk perangkat lunak cadangan Anda. Untuk informasi selengkapnya tentang panduan kinerja gateway tertentu, lihat [Performa](#).

Optimalkan Kinerja Virtual Tape Drive di Perangkat Lunak Backup

Perangkat lunak cadangan Anda dapat mencadangkan data hingga 10 drive pita virtual pada Tape Gateway secara bersamaan. Kami menyarankan Anda mengonfigurasi pekerjaan pencadangan dalam perangkat lunak cadangan Anda untuk menggunakan setidaknya 4 drive tape virtual secara bersamaan di Tape Gateway. Anda dapat mencapai throughput penulisan yang lebih baik ketika perangkat lunak cadangan mencadangkan data ke lebih dari satu rekaman virtual pada saat yang bersamaan.

Sebagai aturan umum, Anda dapat mencapai throughput maksimum yang lebih tinggi dengan mengoperasikan (membaca atau menulis dari) lebih banyak kaset virtual pada saat yang bersamaan. Dengan menggunakan lebih banyak tape drive, Anda mengizinkan gateway Anda untuk melayani lebih banyak permintaan secara bersamaan, berpotensi meningkatkan kinerja.

Tambahkan Sumber Daya ke Lingkungan Aplikasi Anda

Tingkatkan bandwidth antara server aplikasi dan gateway Anda

Koneksi antara inisiator iSCSI dan gateway Anda dapat membatasi kinerja unggahan dan unduhan Anda. Jika gateway Anda menunjukkan kinerja yang jauh lebih buruk dari yang diharapkan dan Anda telah meningkatkan jumlah inti CPU dan throughput disk Anda, pertimbangkan:

- Upgrade kabel jaringan Anda untuk memiliki bandwidth yang lebih tinggi antara inisiator dan gateway Anda.
- Menggunakan sebanyak mungkin tape drive secara bersamaan. iSCSI tidak mendukung antrian beberapa permintaan untuk target yang sama, artinya semakin banyak tape drive yang Anda gunakan, semakin banyak permintaan yang dapat dilayani gateway Anda secara bersamaan. Ini akan memungkinkan Anda untuk lebih memanfaatkan bandwidth antara gateway dan inisiator Anda, meningkatkan throughput nyata gateway Anda.

Untuk mengoptimalkan kinerja gateway, pastikan bandwidth jaringan antara aplikasi Anda dan gateway dapat mempertahankan kebutuhan aplikasi Anda. Anda dapat menggunakan `ReadBytes` dan `WriteBytes` metrik gateway untuk mengukur total throughput data. Untuk informasi selengkapnya tentang metrik ini, lihat [Mengukur Kinerja Antara Tape Gateway Anda dan AWS](#).

Untuk aplikasi Anda, bandingkan throughput yang diukur dengan throughput yang diinginkan. Jika throughput yang diukur kurang dari throughput yang diinginkan, maka meningkatkan bandwidth

antara aplikasi dan gateway Anda dapat meningkatkan kinerja jika jaringan adalah hambatan. Demikian pula, Anda dapat meningkatkan bandwidth antara VM dan disk lokal Anda, jika tidak terpasang langsung.

Tambahkan sumber daya CPU ke lingkungan aplikasi Anda

Jika aplikasi Anda dapat menggunakan sumber daya CPU tambahan, menambahkan lebih banyak CPU dapat membantu aplikasi Anda untuk menskalakan beban I/O-nya.

Menggunakan VMware vSphere Ketersediaan Tinggi dengan Storage Gateway

Storage Gateway menyediakan ketersediaan tinggi pada VMware melalui serangkaian pemeriksaan kesehatan tingkat aplikasi yang terintegrasi dengan VMware vSphere High Availability (VMware HA). Pendekatan ini membantu melindungi beban kerja penyimpanan terhadap kegagalan perangkat keras, hypervisor, atau jaringan. Ini juga membantu melindungi terhadap kesalahan perangkat lunak, seperti batas waktu koneksi dan berbagi file atau tidak tersedianya volume.

vSphere HA bekerja dengan menyatukan mesin virtual dan host tempat mereka tinggal ke dalam cluster untuk redundansi. Host di cluster dipantau dan jika terjadi kegagalan, mesin virtual pada host yang gagal dimulai ulang pada host alternatif. Umumnya, pemulihan ini terjadi dengan cepat dan tanpa kehilangan data. Untuk informasi selengkapnya tentang vSphere HA, lihat Cara [kerja vSphere HA dalam dokumentasi VMware](#).

Note

Waktu yang diperlukan untuk me-restart mesin virtual yang gagal dan membangun kembali koneksi iSCSI pada host baru tergantung pada banyak faktor, seperti sistem operasi host dan beban sumber daya, kecepatan disk, koneksi jaringan, dan infrastruktur SAN/penyimpanan. [Untuk meminimalkan downtime failover, terapkan rekomendasi yang diuraikan dalam Mengoptimalkan .](#)

Untuk menggunakan VMware HA dengan Storage Gateway, lakukan langkah-langkah berikut ini.

Topik

- [Konfigurasi Cluster VSphere VMware HA Anda](#)

- [Unduh Image .ova dari konsol Storage Gateway](#)
- [Menyebarkan Gateway](#)
- [\(Opsional\) Tambahkan Opsi Override untuk VM Lain di Cluster Anda](#)
- [Aktifkan Gateway Anda](#)
- [Uji Konfigurasi Ketersediaan Tinggi VMware Anda](#)

Konfigurasi Cluster VSphere VMware HA Anda

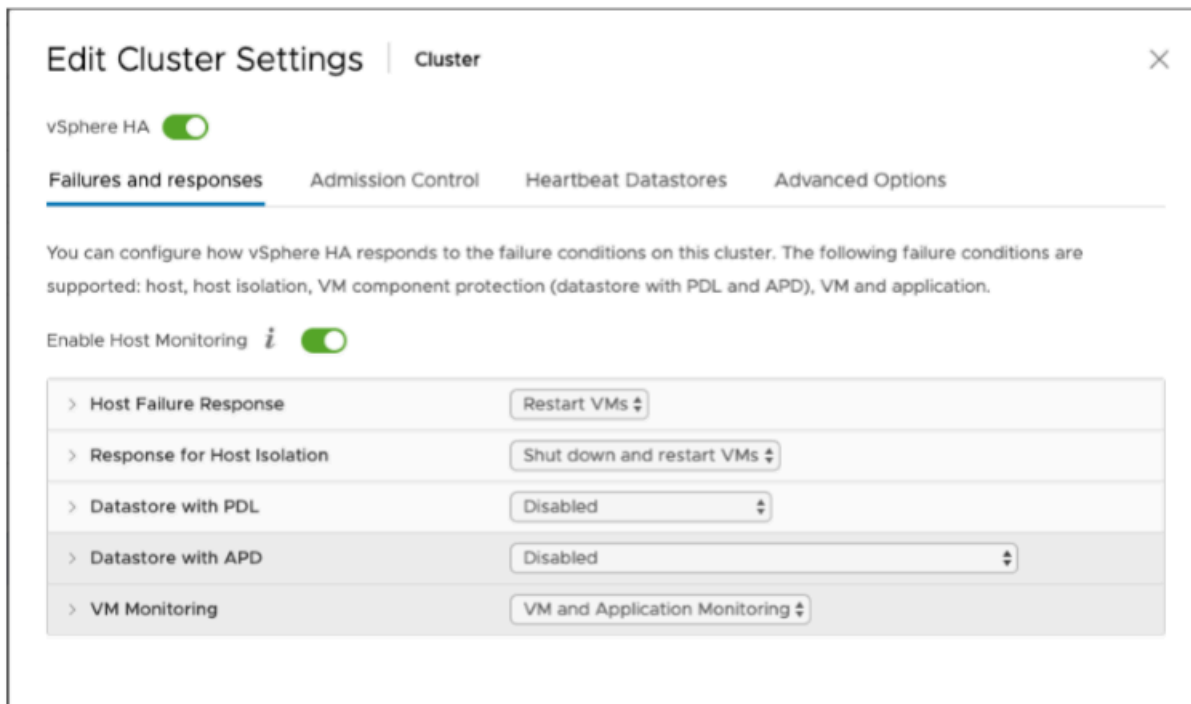
Pertama, jika Anda belum membuat cluster VMware, buat satu. Untuk informasi tentang cara membuat cluster VMware, lihat [Membuat Cluster VSphere HA di dokumentasi VMware](#).

Selanjutnya, konfigurasi cluster VMware Anda untuk bekerja dengan Storage Gateway.

Untuk mengkonfigurasi cluster VMware Anda

1. Pada halaman Edit Pengaturan Cluster di VMware vSphere, pastikan bahwa pemantauan VM dikonfigurasi untuk VM dan pemantauan aplikasi. Untuk melakukannya, atur opsi berikut seperti yang tercantum:
 - Respon Kegagalan Host: Mulai Ulang VM
 - Respons untuk Isolasi Host: Matikan dan restart VM
 - Datastore dengan PDL: Dinonaktifkan
 - Datastore dengan APD: Dinonaktifkan
 - Pemantauan VM: VM dan Pemantauan Aplikasi

Sebagai contoh, lihat tangkapan layar berikut.



2. Sempurnakan sensitivitas cluster dengan menyesuaikan nilai-nilai berikut:

- Interval kegagalan — Setelah interval ini, VM dimulai ulang jika detak jantung VM tidak diterima.
- Waktu aktif minimum - Cluster menunggu selama ini setelah VM mulai memantau detak jantung alat VM.
- Reset per-VM maksimum - Cluster me-restart VM maksimal ini berkali-kali dalam jendela waktu reset maksimum.
- Jendela waktu reset maksimum — Jendela waktu untuk menghitung reset maksimum per VM reset.

Jika Anda tidak yakin nilai apa yang akan ditetapkan, gunakan contoh pengaturan ini:

- Interval kegagalan: **30** detik
- Waktu aktif minimum: detik **120**
- Reset per VM maksimum: **3**
- Jendela waktu reset maksimum: jam **1**

Jika Anda memiliki VM lain yang berjalan di cluster, Anda mungkin ingin menetapkan nilai-nilai ini secara khusus untuk VM Anda. Anda tidak dapat melakukan ini sampai Anda menerapkan VM

dari .ova. Untuk informasi selengkapnya tentang pengaturan nilai-nilai ini, lihat [\(Opsional\) Tambahkan Opsi Override untuk VM Lain di Cluster Anda](#).

Unduh Image .ova dari konsol Storage Gateway

Untuk mengunduh gambar.ova untuk gateway Anda

- Pada halaman Siapkan gateway di konsol Storage Gateway, pilih jenis gateway dan platform host Anda, lalu gunakan tautan yang disediakan di konsol untuk mendownload.ova seperti yang diuraikan dalam [Mengatur Gateway Tape Siapkan Gateway](#).

Menyebarkan Gateway

Di cluster Anda yang dikonfigurasi, terapkan gambar.ova ke salah satu host cluster.

Untuk menyebarkan image gateway .ova

1. Terapkan gambar.ova ke salah satu host di cluster.
2. Pastikan penyimpanan data yang Anda pilih untuk disk root dan cache tersedia untuk semua host di cluster. Saat menerapkan file Storage Gateway .ova di lingkungan VMware atau on-prem, disk digambarkan sebagai disk SCSI paravirtualisasi. Paravirtualisasi adalah mode di mana gateway VM bekerja dengan sistem operasi host sehingga konsol dapat mengidentifikasi disk virtual yang Anda tambahkan ke VM Anda.

Untuk mengonfigurasi VM Anda untuk menggunakan pengontrol paravirtualisasi

1. Di klien VMware vSphere, buka menu konteks (klik kanan) untuk VM gateway Anda, lalu pilih Edit Pengaturan.
2. Di kotak dialog Virtual Machine Properties, pilih tab Hardware, pilih SCSI controller 0, lalu pilih Change Type.
3. Dalam kotak dialog Ubah Jenis Pengontrol SCSI, pilih jenis pengontrol SCSI Paravirtual VMware, lalu pilih OK.

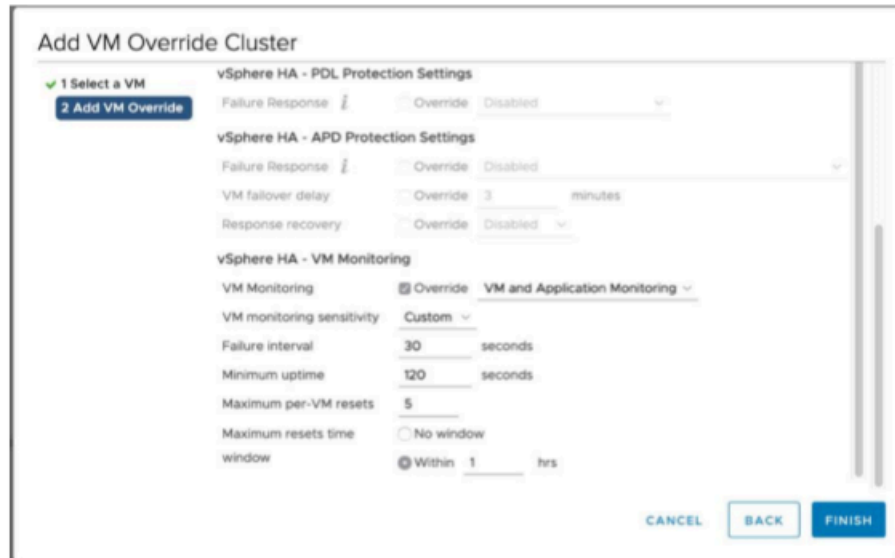
(Opsional) Tambahkan Opsi Override untuk VM Lain di Cluster Anda

Jika Anda memiliki VM lain yang berjalan di cluster Anda, Anda mungkin ingin menetapkan nilai cluster khusus untuk setiap VM.

Untuk menambahkan opsi penggantian untuk VM lain di cluster Anda

1. Pada halaman Ringkasan di VMware vSphere, pilih cluster Anda untuk membuka halaman cluster, lalu pilih Configure.
2. Pilih tab Configuration, lalu pilih VM Overrides.
3. Tambahkan opsi penggantian VM baru untuk mengubah setiap nilai.

Untuk opsi penggantian, lihat tangkapan layar berikut.



Aktifkan Gateway Anda

Setelah .ova untuk gateway Anda diterapkan, aktifkan gateway Anda. Petunjuk tentang bagaimana perbedaan untuk setiap jenis gateway.

Untuk mengaktifkan gateway Anda

- Ikuti prosedur yang diuraikan dalam topik berikut:
 - a. [Hubungkan Tape Gateway Anda ke AWS](#)
 - b. [Tinjau pengaturan dan aktifkan Tape Gateway Anda](#)
 - c. [Konfigurasi Tape Gateway Anda](#)

Uji Konfigurasi Ketersediaan Tinggi VMware Anda

Setelah Anda mengaktifkan gateway Anda, uji konfigurasi Anda.

Untuk menguji konfigurasi HA VMware Anda

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Pada panel navigasi, pilih Gateways, lalu pilih gateway yang ingin Anda uji untuk VMware HA.
3. Untuk Tindakan, pilih Verifikasi VMware HA.
4. Di kotak Verifikasi Konfigurasi Ketersediaan Tinggi VMware yang muncul, pilih OK.

Note

Menguji konfigurasi VMware HA Anda me-reboot VM gateway Anda dan mengganggu konektivitas ke gateway Anda. Tes mungkin memakan waktu beberapa menit untuk menyelesaikannya.

Jika tes berhasil, status Verified muncul di tab detail gateway di konsol.

5. Pilih Keluar.

Anda dapat menemukan informasi tentang peristiwa VMware HA di grup CloudWatch log Amazon. Untuk informasi selengkapnya, lihat [Mendapatkan Log Kesehatan Gateway Tape dengan Grup CloudWatch Log](#).

Keamanan di AWS Storage Gateway

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di Amazon Web Services Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan Program AWS Kepatuhan](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS Storage Gateway, lihat [AWS Layanan dalam Lingkup menurut AWS Layanan Program Kepatuhan](#) .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Storage Gateway. Topik berikut menunjukkan cara mengonfigurasi Storage Gateway untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Storage Gateway Anda.

Topik

- [Perlindungan data di AWS Storage Gateway](#)
- [Identity and Access Management untuk AWS Storage Gateway](#)
- [Logging dan Monitoring di AWS Storage Gateway](#)
- [Validasi kepatuhan untuk AWS Storage Gateway](#)
- [Ketahanan di Storage Gateway AWS](#)
- [Keamanan Infrastruktur di AWS Storage Gateway](#)
- [AWS Praktik Terbaik Keamanan](#)

Perlindungan data di AWS Storage Gateway

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di AWS Storage Gateway. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk memelihara kendali atas isi yang dihost pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Storage Gateway atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data menggunakan AWS KMS

Storage Gateway menggunakan SSL/TLS (Secure Socket Layers/Transport Layer Security) untuk mengenkripsi data yang ditransfer antara alat gateway dan penyimpanan Anda. AWS Secara default, Storage Gateway menggunakan Amazon S3-Managed Encryption Keys (SSE-S3) untuk mengenkripsi sisi server semua data yang disimpan di Amazon S3. Anda memiliki opsi untuk menggunakan Storage Gateway API untuk mengonfigurasi gateway Anda untuk mengenkripsi data yang disimpan di cloud menggunakan enkripsi sisi server dengan kunci AWS Key Management Service (SSE-KMS).

Important

Bila Anda menggunakan AWS KMS kunci untuk enkripsi sisi server, Anda harus memilih kunci simetris. Storage Gateway tidak mendukung kunci asimetris. Untuk informasi selengkapnya, lihat [Menggunakan kunci simetri dan asimetrik](#) di Panduan Developer AWS Key Management Service .

Mengenkripsi berbagi file

Untuk berbagi file, Anda dapat mengonfigurasi gateway untuk mengenkripsi objek Anda dengan kunci yang AWS KMS dikelola menggunakan SSE-KMS. Untuk informasi tentang penggunaan Storage Gateway API untuk mengenkripsi data yang ditulis ke berbagi file, lihat [CreateNFS FileShare di Referensi](#) API.AWS Storage Gateway

Mengenkripsi volume

Untuk volume cache dan tersimpan, Anda dapat mengonfigurasi gateway untuk mengenkripsi data volume yang disimpan di cloud dengan kunci yang AWS KMS dikelola menggunakan Storage Gateway API. Anda dapat menentukan salah satu kunci yang dikelola sebagai kunci KMS. Kunci yang Anda gunakan untuk mengenkripsi volume Anda tidak dapat diubah setelah volume dibuat. Untuk informasi tentang penggunaan Storage Gateway API untuk mengenkripsi data yang ditulis ke volume yang di-cache atau disimpan, lihat [CreateCachediscsiVolume atau scsiVolume di CreateStorediReferensi](#) API.AWS Storage Gateway

Mengenkripsi kaset

Untuk rekaman virtual, Anda dapat mengonfigurasi gateway untuk mengenkripsi data tape yang disimpan di cloud dengan kunci yang AWS KMS dikelola menggunakan Storage Gateway API. Anda dapat menentukan salah satu kunci yang dikelola sebagai kunci KMS. Kunci yang Anda gunakan untuk mengenkripsi data rekaman Anda tidak dapat diubah setelah rekaman dibuat. Untuk informasi tentang penggunaan Storage Gateway API untuk mengenkripsi data yang ditulis ke pita virtual, lihat [CreateTapes](#) di Referensi AWS Storage Gateway API.

Saat menggunakan AWS KMS untuk mengenkripsi data Anda, ingatlah hal berikut:

- Data Anda dienkripsi saat istirahat di cloud. Artinya, data dienkripsi di Amazon S3.
- Pengguna IAM harus memiliki izin yang diperlukan untuk memanggil operasi AWS KMS API. Untuk informasi selengkapnya, lihat [Menggunakan kebijakan IAM dengan AWS KMS](#) Panduan AWS Key Management Service Pengembang.
- Jika Anda menghapus atau menonaktifkan AWS KMS kunci atau mencabut token hibah, Anda tidak dapat mengakses data pada volume atau rekaman. Untuk informasi selengkapnya, lihat [Menghapus kunci KMS](#) di Panduan AWS Key Management Service Pengembang.
- Jika Anda membuat snapshot dari volume yang dienkripsi KMS, snapshot dienkripsi. Snapshot mewarisi tombol KMS volume.
- Jika Anda membuat volume baru dari snapshot yang dienkripsi KMS, volume dienkripsi. Anda dapat menentukan kunci KMS yang berbeda untuk volume baru.

Note

Storage Gateway tidak mendukung pembuatan volume yang tidak terenkripsi dari titik pemulihan volume terenkripsi KMS atau snapshot terenkripsi KMS.

Untuk informasi lebih lanjut tentang AWS KMS, lihat [Apa itu AWS Key Management Service?](#)

Identity and Access Management untuk AWS Storage Gateway

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya SGW. AWS IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS Storage Gateway bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Storage Gateway AWS](#)
- [Memecahkan masalah identitas dan AWS akses Storage Gateway](#)

Audiens

Bagaimana Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di AWS SGW.

Pengguna layanan — Jika Anda menggunakan layanan AWS SGW untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensial dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur AWS SGW untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS SGW, lihat.

[Memecahkan masalah identitas dan AWS akses Storage Gateway](#)

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya AWS SGW di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS SGW. Tugas Anda adalah menentukan fitur dan sumber daya AWS SGW mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan AWS SGW, lihat.

[Bagaimana AWS Storage Gateway bekerja dengan IAM](#)

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke AWS SGW. Untuk melihat contoh kebijakan berbasis identitas AWS SGW yang dapat Anda gunakan di IAM, lihat. [Contoh kebijakan berbasis identitas untuk Storage Gateway AWS](#)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensial identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani permintaan AWS API](#) di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat [Autentikasi multi-faktor](#) dalam Panduan Pengguna AWS IAM Identity Center dan [Menggunakan autentikasi multi-faktor \(MFA\) di AWS](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar tugas lengkap

yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensial sementara.

Untuk pengelolaan akses terpusat, sebaiknya Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat [Apa yang dimaksud Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial temporer, dan bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, sebaiknya rotasikan kunci akses. Untuk informasi selengkapnya, lihat [Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) dalam Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran tersebut dimaksudkan untuk dapat diambil oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk

mempelajari selengkapnya, silakan lihat [Kapan harus membuat pengguna IAM \(bukan peran\)](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan [beralih peran](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang metode untuk menggunakan peran, lihat [Menggunakan peran IAM](#) dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi diautentikasi, identitas tersebut dikaitkan dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Membuat peran untuk Penyedia Identitas pihak ketiga](#) dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi sekumpulan izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengaitkan izin yang ditetapkan ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat [Rangkaian izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya](#) dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Contoh, ketika Anda melakukan panggilan dalam layanan, umumnya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran terkait layanan.

- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna IAM atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Meneruskan sesi akses](#).
- Peran IAM – Peran layanan adalah [peran IAM](#) yang diambil layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat mengambil peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensial sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2](#) dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat [Kapan harus membuat peran IAM \(bukan pengguna\)](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan

diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat [Ikhtisar kebijakan JSON](#) dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam Akun AWS. Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat [Memilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu.

Untuk sumber daya yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya.

Anda harus [menentukan pengguna utama](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat [Gambaran umum daftar kontrol akses \(ACL\)](#) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang Principal tidak dibatasi oleh batasan izin. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke sebagian atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat [Cara kerja SCP](#) dalam Panduan Pengguna AWS Organizations .

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit di salah satu kebijakan ini akan membatalkan izin tersebut. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Jika beberapa jenis kebijakan diberlakukan untuk satu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana AWS Storage Gateway bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke AWS SGW, pelajari fitur IAM apa yang tersedia untuk digunakan dengan SGW. AWS

Fitur IAM yang dapat Anda gunakan dengan AWS Storage Gateway

Fitur IAM	AWS Dukungan SGW
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya

Fitur IAM	AWS Dukungan SGW
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja AWS SGW dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Kebijakan berbasis identitas untuk SGW AWS

Mendukung kebijakan berbasis identitas	Ya
--	----

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta ketentuan terkait jenis tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan pengguna utama dalam kebijakan berbasis identitas karena kebijakan ini berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat digunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk SGW AWS

Untuk melihat contoh kebijakan berbasis identitas AWS SGW, lihat. [Contoh kebijakan berbasis identitas untuk Storage Gateway AWS](#)

Kebijakan berbasis sumber daya dalam SGW AWS

Mendukung kebijakan berbasis sumber daya	Tidak
--	-------

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus [menentukan pengguna utama](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama lintas akun ke kebijakan berbasis sumber daya bagian dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, kebijakan berbasis identitas lainnya tidak diperlukan. Untuk informasi selengkapnya, lihat [Perbedaan peran IAM dengan kebijakan berbasis sumber daya](#) di Panduan Pengguna IAM.

Tindakan kebijakan untuk AWS SGW

Mendukung tindakan kebijakan

Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin melakukan operasi terkait.

Untuk melihat daftar tindakan AWS SGW, lihat [Tindakan yang Ditetapkan oleh AWS Storage Gateway](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan di AWS SGW menggunakan awalan berikut sebelum tindakan:

```
sgw
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma.

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

Untuk melihat contoh kebijakan berbasis identitas AWS SGW, lihat. [Contoh kebijakan berbasis identitas untuk Storage Gateway AWS](#)

Sumber daya kebijakan untuk AWS SGW

Mendukung sumber daya kebijakan

Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek atau beberapa objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk mengindikasikan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar tipe resource AWS SGW dan ARNnya, lihat [Resources Defined by AWS Storage Gateway](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang Ditentukan oleh AWS Storage Gateway](#).

Untuk melihat contoh kebijakan berbasis identitas AWS SGW, lihat. [Contoh kebijakan berbasis identitas untuk Storage Gateway AWS](#)

Kunci kondisi kebijakan untuk AWS SGW

Mendukung kunci kondisi kebijakan spesifik layanan	Ya
--	----

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen Condition (atau blok Condition) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen Condition bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen Condition dalam satu pernyataan, atau beberapa kunci dalam satu elemen Condition, AWS akan mengevaluasinya dengan menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat [Elemen kebijakan IAM: variabel dan tanda](#) di Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi AWS SGW, lihat Kunci Kondisi [untuk AWS Storage Gateway](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang Ditentukan oleh AWS Storage Gateway](#).

Untuk melihat contoh kebijakan berbasis identitas AWS SGW, lihat. [Contoh kebijakan berbasis identitas untuk Storage Gateway AWS](#)

ACL dalam SGW AWS

Mendukung ACL

Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan SGW AWS

Mendukung ABAC (tanda dalam kebijakan)

Parsial

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tanda milik pengguna utama cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna dalam situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tanda di [elemen syarat](#) dari sebuah kebijakan dengan menggunakan kunci-kunci persyaratan `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat [Apa itu ABAC?](#) di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) di Panduan Pengguna IAM.

Menggunakan kredensial sementara dengan SGW AWS

Mendukung kredensial sementara	Ya
--------------------------------	----

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensial sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensial sementara, lihat [Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Anda menggunakan kredensial sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensial sementara. Anda juga akan membuat kredensial sementara secara otomatis saat masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang cara beralih peran, lihat [Beralih peran \(konsol\)](#) di Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda menghasilkan kredensial sementara secara dinamis alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#).

Teruskan sesi akses untuk AWS SGW

Mendukung sesi akses maju (FAS)	Ya
---------------------------------	----

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk

menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Meneruskan sesi akses](#).

Peran layanan untuk AWS SGW

Mendukung peran layanan	Ya
-------------------------	----

Peran layanan adalah [peran IAM](#) yang diambil oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas AWS SGW. Edit peran layanan hanya jika AWS SGW memberikan panduan untuk melakukannya.

Peran terkait layanan untuk SGW AWS

Mendukung peran yang terkait layanan	Ya
--------------------------------------	----

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat mengambil peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau pengelolaan peran terkait layanan, lihat [Layanan AWS yang berfungsi dengan IAM](#). Temukan sebuah layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Storage Gateway AWS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya AWS SGW. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS

Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS SGW, termasuk format ARN untuk setiap jenis sumber daya, lihat [Tindakan, Sumber Daya, dan Kunci Kondisi untuk AWS Storage Gateway](#) di Referensi Otorisasi Layanan.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol AWS SGW](#)
- [Izinkan pengguna melihat izin mereka sendiri](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya AWS SGW di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Akun AWS Anda. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [kebijakan yang dikelola AWS](#) atau [kebijakan yang dikelola AWS untuk fungsi pekerjaan](#) di Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat [Kebijakan dan izin di IAM](#) di Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Syarat](#) di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [validasi kebijakan Analizer Akses IAM](#) di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Mengonfigurasi akses API yang dilindungi MFA](#) di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) di Panduan Pengguna IAM.

Menggunakan konsol AWS SGW

Untuk mengakses konsol AWS Storage Gateway, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya AWS SGW di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol AWS SGW, lampirkan juga AWS SGW *ConsoleAccess* atau kebijakan *ReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambahkan izin ke pengguna](#) di Panduan Pengguna IAM.

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Memecahkan masalah identitas dan AWS akses Storage Gateway

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS SGW dan IAM.

Topik

- [Saya tidak berwenang untuk melakukan tindakan di AWS SGW](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya AWS SGW saya](#)

Saya tidak berwenang untuk melakukan tindakan di AWS SGW

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya `my-example-widget` rekaan, tetapi tidak memiliki izin `sgw:GetWidget` rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
sgw:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan `sgw:GetWidget`.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke AWS SGW.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan dalam AWS SGW. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya AWS SGW saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah AWS SGW mendukung fitur-fitur ini, lihat [Bagaimana AWS Storage Gateway bekerja dengan IAM](#)
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Memberikan akses kepada pengguna eksternal yang sah \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Perbedaan antara peran IAM dan kebijakan berbasis sumber daya](#) di Panduan Pengguna IAM.

Logging dan Monitoring di AWS Storage Gateway

Storage Gateway terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Storage Gateway. CloudTrail menangkap semua panggilan API untuk Storage Gateway sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Storage Gateway dan panggilan kode ke operasi Storage Gateway API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Storage Gateway. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Storage Gateway, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Informasi Storage Gateway di CloudTrail

CloudTrail diaktifkan di akun Amazon Web Services Anda saat Anda membuat akun. Ketika aktivitas terjadi di Storage Gateway, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh kejadian terbaru di akun Amazon Web Services Anda. Untuk informasi selengkapnya, lihat [Melihat Acara dengan Riwayat CloudTrail Acara](#).

Untuk catatan peristiwa yang sedang berlangsung di akun Amazon Web Services Anda, termasuk peristiwa untuk Storage Gateway, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua AWS Wilayah. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran umum untuk Membuat Jejak](#)
- [CloudTrail Layanan dan Integrasi yang Didukung](#)
- [Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima File CloudTrail Log dari Beberapa Wilayah](#) dan [Menerima File CloudTrail Log dari Beberapa Akun](#)

Semua tindakan Storage Gateway dicatat dan didokumentasikan dalam topik [Tindakan](#). Misalnya, panggilan ke `ActivateGateway`, `ListGateways`, dan `ShutdownGateway` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan itu dibuat dengan kredensial pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk suatu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi lain, lihat [Elemen userIdentity CloudTrail](#).

Memahami Entri File Log Storage Gateway

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan tindakan.

```
{ "Records": [{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAI15AUEPBH2M7JTNVC",
    "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-04T16:19:00Z",
  "eventSource": "storagegateway.amazonaws.com",
  "eventName": "ActivateGateway",
  "awsRegion": "us-east-2",
```



```

    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "gatewayTimezone": "GMT-5:00",
        "gatewayName": "cloudtrailgatewayv1",
        "gatewayRegion": "us-east-2",
        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
        "gatewayType": "VTL"
    },
    "responseElements": {
        "gatewayARN":
"arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayv1"
    },
    "requestID":
"54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
    "eventType": "AwsApiCall",
    "apiVersion": "20130630",
    "recipientAccountId": "444455556666"
    }
}

```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan ListGateways tindakan.

```

{
  "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAI5AUEPBH2M7JTNVC",
      "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",
  }
]
}

```

```
Linux / 2.6.18 - 164.el5 ",
    " sourceIPAddress ":" 192.0.2.0 ",
    " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
    " requestParameters ":null,
    " responseElements ":null,
    "requestID ":"
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
    " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
d203a189ec8d ",
    " eventType ":" AwsApiCall ",
    " apiVersion ":" 20130630 ",
    " recipientAccountId ":" 444455556666"
    }
}
```

Validasi kepatuhan untuk AWS Storage Gateway

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS Storage Gateway sebagai bagian dari beberapa program AWS kepatuhan. Ini termasuk SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR, dan HITRUST CSF.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan](#) . Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#) .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#) .

Tanggung jawab kepatuhan Anda saat menggunakan Storage Gateway ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan Memulai Cepat Keamanan dan Kepatuhan Panduan](#) Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- [Arsitektur untuk Whitepaper Keamanan dan Kepatuhan HIPAA — Whitepaper](#) ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi yang sesuai dengan HIPAA. AWS
- [AWS Sumber Daya AWS](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.

- [Mengevaluasi sumber daya dengan aturan](#) dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#)— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di Storage Gateway AWS

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Selain infrastruktur AWS global, Storage Gateway menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda:

- Gunakan VMware vSphere High Availability (VMware HA) untuk membantu melindungi beban kerja penyimpanan terhadap kegagalan perangkat keras, hypervisor, atau jaringan. Untuk informasi selengkapnya, lihat [Menggunakan VMware vSphere Ketersediaan Tinggi dengan Storage Gateway](#).
- Arsipkan kaset virtual di S3 Glacier Flexible Retrieval. Lihat informasi yang lebih lengkap di [Pengarsipan Kaset Virtual](#).

Keamanan Infrastruktur di AWS Storage Gateway

Sebagai layanan terkelola, AWS Storage Gateway dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper [Amazon Web Services: Overview of Security Processes](#).

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Storage Gateway melalui jaringan. Klien harus support Keamanan Lapisan Pengangkutan (TLS) 1.2. Klien juga harus

support suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

AWS Praktik Terbaik Keamanan

AWS menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik ini adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik-praktik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, perlakukan mereka sebagai pertimbangan yang bermanfaat daripada resep. Untuk informasi selengkapnya, lihat [Praktik Terbaik AWS Keamanan](#).

Pemecahan masalah gateway

Setelah itu, Anda dapat menemukan informasi tentang masalah pemecahan masalah yang terkait dengan gateway, berbagi file, volume, kaset virtual, dan snapshot. Informasi pemecahan masalah gateway lokal mencakup gateway yang digunakan pada klien VMware ESXi dan Microsoft Hyper-V. Informasi pemecahan masalah untuk berbagi file berlaku untuk jenis File Gateway. Informasi pemecahan masalah untuk volume berlaku untuk tipe Volume Gateway. Informasi pemecahan masalah untuk kaset berlaku untuk tipe Tape Gateway. Informasi pemecahan masalah untuk masalah gateway berlaku untuk menggunakan CloudWatch metrik. Informasi pemecahan masalah untuk masalah ketersediaan tinggi mencakup gateway yang berjalan pada platform VMware vSphere High Availability (HA).

Topik

- [Pemecahan masalah: status gateway ditampilkan offline di konsol AWS Storage Gateway](#)
- [Pemecahan masalah: kesalahan internal diterima selama aktivasi Storage Gateway](#)
- [Memecahkan masalah gateway lokal](#)
- [Memecahkan masalah pengaturan Microsoft Hyper-V](#)
- [Memecahkan masalah gateway Amazon EC2](#)
- [Memecahkan masalah alat perangkat keras](#)
- [Memecahkan masalah rekaman virtual](#)
- [Memecahkan masalah ketersediaan tinggi](#)
- [Praktik terbaik untuk memulihkan data Anda](#)

Pemecahan masalah: status gateway ditampilkan offline di konsol AWS Storage Gateway

Gunakan informasi pemecahan masalah berikut untuk menentukan apa yang harus dilakukan jika AWS Storage Gateway konsol menunjukkan bahwa gateway Anda sedang offline.

Gateway Anda mungkin ditampilkan sebagai offline karena satu atau beberapa alasan berikut:

- Gateway tidak dapat mencapai titik akhir layanan Storage Gateway.
- Pintu gerbang ditutup secara tak terduga.

- Disk cache yang terkait dengan gateway telah terputus atau dimodifikasi, atau gagal.

Untuk mengembalikan gateway Anda secara online, identifikasi dan selesaikan masalah yang menyebabkan gateway Anda offline.

Periksa firewall atau proxy terkait

Jika Anda mengonfigurasi gateway Anda untuk menggunakan proxy, atau Anda menempatkan gateway Anda di belakang firewall, maka tinjau aturan akses proxy atau firewall. Proxy atau firewall harus mengizinkan lalu lintas ke dan dari port jaringan dan titik akhir layanan yang diperlukan oleh Storage Gateway. Untuk informasi selengkapnya, lihat [jaringan dan firewall Persyaratan](#) .

Periksa SSL atau inspeksi paket mendalam yang sedang berlangsung dari lalu lintas gateway Anda

Jika inspeksi SSL atau deep-packet saat ini sedang dilakukan pada lalu lintas jaringan antara gateway Anda dan AWS, maka gateway Anda mungkin tidak dapat berkomunikasi dengan titik akhir layanan yang diperlukan. Untuk membawa gateway Anda kembali online, Anda harus menonaktifkan inspeksi.

Periksa pemadaman listrik atau kegagalan perangkat keras pada host hypervisor

Pemadaman listrik atau kegagalan perangkat keras pada host hypervisor gateway Anda dapat menyebabkan gateway Anda mati secara tak terduga dan menjadi tidak terjangkau. Setelah Anda memulihkan daya dan konektivitas jaringan, gateway Anda akan dapat dijangkau lagi.

Setelah gateway Anda kembali online, pastikan untuk mengambil langkah-langkah untuk memulihkan data Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik untuk memulihkan data Anda data Anda](#).

Periksa masalah dengan disk cache terkait

Gateway Anda dapat offline jika setidaknya salah satu disk cache yang terkait dengan gateway Anda telah dihapus, diubah, atau diubah ukurannya, atau jika rusak.

Jika disk cache yang berfungsi dihapus dari host hypervisor:

1. Matikan pintu gerbangnya.

2. Tambahkan kembali disk.

Note

Pastikan Anda menambahkan disk ke node disk yang sama.

3. Mulai ulang gateway.

Jika disk cache rusak, diganti, atau diubah ukurannya:

1. Matikan pintu gerbangnya.
2. Setel ulang disk cache.
3. Konfigurasi ulang disk untuk penyimpanan cache.
4. Mulai ulang gateway.

Untuk informasi selengkapnya tentang pemecahan masalah disk cache yang rusak untuk gateway tape, lihat [Anda perlu memulihkan rekaman virtual dari disk cache yang tidak berfungsi](#).

Pemecahan masalah: kesalahan internal diterima selama aktivasi Storage Gateway

Permintaan aktivasi Storage Gateway melintasi dua jalur jaringan. Permintaan aktivasi masuk yang dikirim oleh klien terhubung ke mesin virtual gateway (VM) atau instans Amazon Elastic Compute Cloud (Amazon EC2) melalui port 80. Jika gateway berhasil menerima permintaan aktivasi, maka gateway berkomunikasi dengan titik akhir Storage Gateway untuk menerima kunci aktivasi. Jika gateway tidak dapat mencapai titik akhir Storage Gateway, maka gateway merespons klien dengan pesan kesalahan internal.

Gunakan informasi pemecahan masalah berikut untuk menentukan apa yang harus dilakukan jika Anda menerima pesan galat internal saat mencoba mengaktifkan pesan Anda. AWS Storage Gateway

Note

- Pastikan Anda menerapkan gateway baru menggunakan file gambar mesin virtual terbaru atau versi Amazon Machine Image (AMI). Anda akan menerima kesalahan internal jika

Anda mencoba mengaktifkan gateway yang menggunakan AMI yang sudah ketinggalan zaman.

- Pastikan Anda memilih jenis gateway yang benar yang ingin Anda gunakan sebelum mengunduh AMI. File.ova dan AMI untuk setiap jenis gateway berbeda, dan mereka tidak dapat dipertukarkan.

Mengatasi kesalahan saat mengaktifkan gateway Anda menggunakan titik akhir publik

Untuk mengatasi kesalahan aktivasi saat mengaktifkan gateway menggunakan titik akhir publik, lakukan pemeriksaan dan konfigurasi berikut.

Periksa port yang diperlukan

Untuk gateway yang digunakan di lokasi, periksa apakah port terbuka di firewall lokal Anda. Untuk gateway yang digunakan pada instans Amazon EC2, periksa apakah port terbuka di grup keamanan instans. Untuk mengonfirmasi bahwa port terbuka, jalankan perintah telnet pada titik akhir publik dari server. Server ini harus berada di subnet yang sama dengan gateway. Misalnya, perintah telnet berikut menguji koneksi ke port 443:

```
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
```

Untuk mengonfirmasi bahwa gateway itu sendiri dapat mencapai titik akhir, akses konsol VM lokal gateway (untuk gateway yang digunakan di lokasi). Atau, Anda dapat SSH ke instance gateway (untuk gateway yang digunakan di Amazon EC2). Kemudian, jalankan tes konektivitas jaringan. Konfirmasikan bahwa tes kembali[PASSED]. Untuk informasi selengkapnya, lihat [Anda Menguji Koneksi Gateway Anda ke Internet](#) .

Note

Nama pengguna login default untuk konsol gateway adalah `admin`, dan kata sandi defaultnya adalah `password`.

Pastikan keamanan firewall tidak mengubah paket yang dikirim dari gateway ke titik akhir publik

Inspeksi SSL, inspeksi paket mendalam, atau bentuk keamanan firewall lainnya dapat mengganggu paket yang dikirim dari gateway. Jabat tangan SSL gagal jika sertifikat SSL dimodifikasi dari apa yang diharapkan titik akhir aktivasi. Untuk mengonfirmasi bahwa tidak ada inspeksi SSL yang sedang berlangsung, jalankan perintah OpenSSL pada endpoint anon-cp.storagegateway.region.amazonaws.com aktivasi utama () pada port 443. Anda harus menjalankan perintah ini dari mesin yang berada di subnet yang sama dengan gateway:

```
$ openssl s_client -connect anon-cp.storagegateway.region.amazonaws.com:443 -  
servername anon-cp.storagegateway.region.amazonaws.com
```

Note

Ganti *wilayah* dengan Anda Wilayah AWS.

Jika tidak ada inspeksi SSL yang sedang berlangsung, maka perintah mengembalikan respons yang mirip dengan berikut ini:

```
$ 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, 0 = Amazon, CN = Amazon Root CA 1  
verify return:1  
depth=1 C = US, 0 = 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
---
```

Jika ada inspeksi SSL yang sedang berlangsung, maka responsnya menunjukkan rantai sertifikat yang diubah, mirip dengan yang berikut:

```
$ 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
---
```

Titik akhir aktivasi menerima jabat tangan SSL hanya jika mengenali sertifikat SSL. Ini berarti bahwa lalu lintas keluar gateway ke titik akhir harus dibebaskan dari inspeksi yang dilakukan oleh firewall di jaringan Anda. Inspeksi ini mungkin inspeksi SSL atau inspeksi paket mendalam.

Periksa sinkronisasi waktu gateway

Kemiringan waktu yang berlebihan dapat menyebabkan kesalahan jabat tangan SSL. Untuk gateway lokal, Anda dapat menggunakan konsol VM lokal gateway untuk memeriksa sinkronisasi waktu gateway Anda. Kemiringan waktu tidak boleh lebih dari 60 detik.

Opsi Manajemen Waktu Sistem tidak tersedia di gateway yang di-host di instans Amazon EC2. Untuk memastikan gateway Amazon EC2 dapat menyinkronkan waktu dengan benar, konfirmasi bahwa instans Amazon EC2 dapat terhubung ke daftar kumpulan server NTP berikut melalui port UDP dan TCP 123:

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

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

Mengatasi kesalahan saat mengaktifkan gateway menggunakan endpoint Amazon VPC

Untuk mengatasi kesalahan aktivasi saat mengaktifkan gateway menggunakan titik akhir Amazon Virtual Private Cloud (Amazon VPC), lakukan pemeriksaan dan konfigurasi berikut.

Periksa port yang diperlukan

Pastikan port yang diperlukan dalam firewall lokal Anda (untuk gateway yang digunakan di lokasi) atau grup keamanan (untuk gateway yang digunakan di Amazon EC2) terbuka. Port yang diperlukan untuk menghubungkan gateway ke titik akhir VPC Storage Gateway berbeda dari yang diperlukan saat menghubungkan gateway ke titik akhir publik. Port berikut diperlukan untuk menghubungkan ke titik akhir VPC Storage Gateway:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Selain itu, periksa grup keamanan yang dilampirkan ke titik akhir VPC Storage Gateway Anda. Grup keamanan default yang dilampirkan ke titik akhir mungkin tidak mengizinkan port yang diperlukan. Buat grup keamanan baru yang memungkinkan lalu lintas dari rentang alamat IP gateway Anda melalui port yang diperlukan. Kemudian, lampirkan grup keamanan itu ke titik akhir VPC.

Note

Gunakan [konsol VPC Amazon](#) untuk memverifikasi grup keamanan yang dilampirkan ke titik akhir VPC. Lihat titik akhir VPC Storage Gateway Anda dari konsol, lalu pilih tab Grup Keamanan.

Untuk mengonfirmasi bahwa port yang diperlukan terbuka, Anda dapat menjalankan perintah telnet pada Storage Gateway VPC Endpoint. Anda harus menjalankan perintah ini dari server yang berada di subnet yang sama dengan gateway. Anda dapat menjalankan pengujian pada nama DNS pertama yang tidak menentukan Availability Zone. Misalnya, perintah telnet berikut menguji koneksi port yang diperlukan menggunakan nama DNS `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`:

```
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
```

Pastikan keamanan firewall tidak mengubah paket yang dikirim dari gateway ke titik akhir Storage Gateway Amazon VPC

Inspeksi SSL, inspeksi paket mendalam, atau bentuk keamanan firewall lainnya dapat mengganggu paket yang dikirim dari gateway. Jabat tangan SSL gagal jika sertifikat SSL dimodifikasi dari apa yang diharapkan titik akhir aktivasi. Untuk mengonfirmasi bahwa tidak ada pemeriksaan SSL yang sedang berlangsung, jalankan perintah OpenSSL di titik akhir VPC Storage Gateway Anda. Anda harus menjalankan perintah ini dari mesin yang berada di subnet yang sama dengan gateway. Jalankan perintah untuk setiap port yang diperlukan:

```
$ 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
```

Jika tidak ada inspeksi SSL yang sedang berlangsung, maka perintah mengembalikan respons yang mirip dengan berikut ini:

```
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, 0 = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, 0 = 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, 0 = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, 0 = Amazon, OU = Server CA 1B, CN = Amazon
  i:C = US, 0 = Amazon, CN = Amazon Root CA 1
 2 s:C = US, 0 = 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, 0 = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
Authority
---
```

Jika ada inspeksi SSL yang sedang berlangsung, maka responsnya menunjukkan rantai sertifikat yang diubah, mirip dengan yang berikut:

```
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
---
```

Titik akhir aktivasi menerima jabat tangan SSL hanya jika mengenali sertifikat SSL. Ini berarti bahwa lalu lintas keluar gateway ke titik akhir VPC Anda melalui port yang diperlukan dibebaskan dari inspeksi yang dilakukan oleh firewall jaringan Anda. Inspeksi ini mungkin inspeksi SSL atau inspeksi paket mendalam.

Periksa sinkronisasi waktu gateway

Kemiringan waktu yang berlebihan dapat menyebabkan kesalahan jabat tangan SSL. Untuk gateway lokal, Anda dapat menggunakan konsol VM lokal gateway untuk memeriksa sinkronisasi waktu gateway Anda. Kemiringan waktu tidak boleh lebih dari 60 detik.

Opsi Manajemen Waktu Sistem tidak tersedia di gateway yang di-host di instans Amazon EC2. Untuk memastikan gateway Amazon EC2 dapat menyinkronkan waktu dengan benar, konfirmasi bahwa instans Amazon EC2 dapat terhubung ke daftar kumpulan server NTP berikut melalui port UDP dan TCP 123:

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

Periksa proxy HTTP dan konfirmasi pengaturan grup keamanan terkait

Sebelum aktivasi, periksa apakah Anda memiliki proxy HTTP di Amazon EC2 yang dikonfigurasi di VM gateway lokal sebagai proxy Squid di port 3128. Dalam hal ini, konfirmasi hal berikut:

- Grup keamanan yang dilampirkan ke proxy HTTP di Amazon EC2 harus memiliki aturan masuk. Aturan masuk ini harus mengizinkan lalu lintas proxy Squid pada port 3128 dari alamat IP gateway VM.
- Grup keamanan yang dilampirkan pada titik akhir VPC Amazon EC2 harus memiliki aturan masuk. Aturan masuk ini harus mengizinkan lalu lintas pada port 1026-1028, 1031, 2222, dan 443 dari alamat IP proxy HTTP di Amazon EC2.

Mengatasi kesalahan saat mengaktifkan gateway Anda menggunakan titik akhir publik dan ada titik akhir VPC Storage Gateway di VPC yang sama

Untuk mengatasi kesalahan saat mengaktifkan gateway menggunakan titik akhir publik saat ada endpoint Amazon Virtual Private Cloud (Amazon VPC) di VPC yang sama, lakukan pemeriksaan dan konfigurasi berikut.

Konfirmasikan bahwa pengaturan Aktifkan Nama DNS Pribadi tidak diaktifkan pada titik akhir VPC Storage Gateway

Jika Aktifkan Nama DNS Pribadi diaktifkan, Anda tidak dapat mengaktifkan gateway apa pun dari VPC tersebut ke titik akhir publik.

Untuk menonaktifkan opsi nama DNS pribadi:

1. Buka konsol [Amazon VPC](#).
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir VPC Storage Gateway Anda.
4. Pilih Tindakan.
5. Pilih Kelola Nama DNS Pribadi.
6. Untuk Aktifkan Nama DNS Pribadi, hapus Aktifkan untuk Titik Akhir ini.
7. Pilih Ubah Nama DNS Pribadi untuk menyimpan pengaturan.

Memecahkan masalah gateway lokal

Anda dapat menemukan informasi berikut tentang masalah umum yang mungkin Anda temui saat bekerja dengan gateway lokal, dan cara mengaktifkan AWS Support untuk membantu memecahkan masalah gateway.

Tabel berikut mencantumkan masalah umum yang mungkin Anda temui saat bekerja dengan gateway lokal.

Isu	Tindakan yang Harus Dilakukan
<p>Anda tidak dapat menemukan alamat IP gateway Anda.</p>	<p>Gunakan klien hypervisor untuk terhubung ke host Anda untuk menemukan alamat IP gateway.</p> <ul style="list-style-type: none"> • Untuk VMware ESXi, alamat IP VM dapat ditemukan di klien vSphere pada tab Ringkasan. • Untuk Microsoft Hyper-V, alamat IP VM dapat ditemukan dengan masuk ke konsol lokal. <p>Jika Anda masih mengalami kesulitan menemukan alamat IP gateway:</p> <ul style="list-style-type: none"> • Periksa apakah VM dihidupkan. Hanya ketika VM dihidupkan, alamat IP ditetapkan ke gateway Anda. • Tunggu VM menyelesaikan startup. Jika Anda baru saja menyalakan VM Anda, maka mungkin perlu beberapa menit bagi gateway untuk menyelesaikan urutan boot-nya.
<p>Anda mengalami masalah jaringan atau firewall.</p>	<ul style="list-style-type: none"> • Izinkan port yang sesuai untuk gateway Anda. • Validasi/inspeksi sertifikat SSL tidak boleh diaktifkan. Storage Gateway menggunakan otentikasi TLS timbal balik yang akan gagal jika ada aplikasi pihak ketiga yang mencoba mencegat/ menandatangani salah satu sertifikat. • Jika Anda menggunakan firewall atau router untuk memfilter atau membatasi lalu lintas jaringan, Anda harus mengonfigurasi firewall dan router Anda untuk mengizinkan titik akhir layanan ini untuk komunikasi keluar. AWS Untuk informasi selengkapnya tentang persyaratan jaringan dan firewall, lihat Persyaratan jaringan dan firewall.
<p>Aktivasi gateway Anda gagal ketika Anda mengklik tombol Lanjutkan ke</p>	<ul style="list-style-type: none"> • Periksa apakah VM gateway dapat diakses dengan melakukan ping VM dari klien Anda.

Isu	Tindakan yang Harus Dilakukan
Aktivasi di Storage Gateway Management Console.	<ul style="list-style-type: none">• Periksa apakah VM Anda memiliki konektivitas jaringan ke internet. Jika tidak, Anda harus mengonfigurasi proxy SOCKS. Untuk informasi selengkapnya tentang cara melakukannya, lihat Merutekan Gateway Lokal Anda Melalui Proxy.• Periksa apakah host memiliki waktu yang tepat, bahwa host dikonfigurasi untuk menyinkronkan waktunya secara otomatis ke server Network Time Protocol (NTP), dan bahwa gateway VM memiliki waktu yang tepat. Untuk informasi tentang sinkronisasi waktu host hypervisor dan VM, lihat Menyinkronkan Waktu VM Gateway Anda• Setelah melakukan langkah-langkah ini, Anda dapat mencoba kembali penerapan gateway menggunakan konsol Storage Gateway dan wizard Setup and Activate Gateway.• Validasi/inspeksi sertifikat SSL tidak boleh diaktifkan. Storage Gateway menggunakan otentikasi TLS timbal balik yang akan gagal jika ada aplikasi pihak ketiga yang mencoba mencegat/menandatangani salah satu sertifikat.• Periksa apakah VM Anda memiliki setidaknya 7,5 GB RAM. Alokasi gateway gagal jika ada kurang dari 7,5 GB RAM. Untuk informasi selengkapnya, lihat Persyaratan.
Anda perlu menghapus disk yang dialokasikan sebagai ruang buffer unggah. Misalnya, Anda mungkin ingin mengurangi jumlah ruang buffer upload untuk gateway, atau Anda mungkin perlu mengganti disk yang digunakan sebagai buffer unggahan yang gagal.	Untuk petunjuk tentang menghapus disk yang dialokasikan sebagai ruang buffer upload, lihat Menghapus Disk dari Gateway Anda

Isu	Tindakan yang Harus Dilakukan
<p>Anda perlu meningkatkan bandwidth antara gateway Anda dan AWS.</p>	<p>Anda dapat meningkatkan bandwidth dari gateway Anda ke AWS dengan mengatur koneksi internet Anda ke AWS pada adaptor jaringan (NIC) terpisah dari yang menghubungkan aplikasi Anda dan VM gateway. Mengambil pendekatan ini berguna jika Anda memiliki koneksi bandwidth tinggi AWS dan Anda ingin menghindari pertenggaran bandwidth, terutama selama pemulihan snapshot. Untuk kebutuhan beban kerja throughput tinggi, Anda dapat menggunakannya AWS Direct Connect untuk membuat koneksi jaringan khusus antara gateway lokal dan gateway. AWS Untuk mengukur bandwidth koneksi dari gateway Anda ke AWS, gunakan <code>CloudBytesDownloaded</code> dan <code>CloudBytesUploaded</code> metrik gateway. Untuk lebih lanjut tentang hal ini, lihat Mengukur Kinerja Antara Tape Gateway Anda dan AWS. Meningkatkan konektivitas internet Anda membantu memastikan bahwa buffer unggahan Anda tidak terisi.</p>

Isu	Tindakan yang Harus Dilakukan
Throughput ke atau dari gateway Anda turun ke nol.	<ul style="list-style-type: none">• Pada tab Gateway dari konsol Storage Gateway, verifikasi bahwa alamat IP untuk VM gateway Anda sama dengan yang Anda lihat menggunakan perangkat lunak klien hypervisor Anda (yaitu, klien VMware vSphere atau Microsoft Hyper-V Manager). Jika Anda menemukan ketidakcocokan, mulai ulang gateway Anda dari konsol Storage Gateway, seperti yang ditunjukkan pada Mematikan VM Gateway Anda. Setelah restart, alamat dalam daftar Alamat IP di tab Gateway konsol Storage Gateway harus cocok dengan alamat IP untuk gateway Anda, yang Anda tentukan dari klien hypervisor.• Untuk VMware ESXi, alamat IP VM dapat ditemukan di klien vSphere pada tab Ringkasan.• Untuk Microsoft Hyper-V, alamat IP VM dapat ditemukan dengan masuk ke konsol lokal.• Periksa konektivitas gateway Anda AWS seperti yang dijelaskan dalam Menguji Koneksi Gateway Anda ke Internet.• Periksa konfigurasi adaptor jaringan gateway Anda, dan pastikan bahwa semua antarmuka yang Anda inginkan untuk diaktifkan untuk gateway diaktifkan. Untuk melihat konfigurasi adaptor jaringan untuk gateway Anda, ikuti petunjuk Mengkonfigurasi Jaringan Gateway Anda dan pilih opsi untuk melihat konfigurasi jaringan gateway Anda. <p>Anda dapat melihat throughput ke dan dari gateway Anda dari CloudWatch konsol Amazon. Untuk informasi selengkapnya tentang mengukur throughput ke dan dari gateway Anda dan AWS, lihat Mengukur Kinerja Antara Tape Gateway Anda dan AWS.</p>
Anda mengalami masalah dalam mengimpor (menerapkan) Storage Gateway di Microsoft Hyper-V.	Lihat Memecahkan masalah pengaturan Microsoft Hyper-V , yang membahas beberapa masalah umum penerapan gateway di Microsoft Hyper-V.

Isu	Tindakan yang Harus Dilakukan
Anda menerima pesan yang mengatakan: “Data yang telah ditulis ke volume di gateway Anda tidak disimpan dengan aman di AWS”.	Anda menerima pesan ini jika VM gateway Anda dibuat dari klon atau snapshot dari VM gateway lain. Jika ini tidak terjadi, hubungi AWS Support.

Memungkinkan AWS Support untuk membantu memecahkan masalah gateway Anda yang dihosting di lokasi

Storage Gateway menyediakan konsol lokal yang dapat Anda gunakan untuk melakukan beberapa tugas pemeliharaan, termasuk mengaktifkan AWS Support untuk mengakses gateway Anda untuk membantu Anda mengatasi masalah gateway. Secara default, AWS Support akses ke gateway Anda dinonaktifkan. Anda menyediakan akses ini melalui konsol lokal host. Untuk memberikan AWS Support akses ke gateway Anda, pertama-tama Anda masuk ke konsol lokal untuk host, navigasikan ke konsol Storage Gateway, dan kemudian sambungkan ke server dukungan.

Untuk mengizinkan AWS Support akses ke gateway Anda

1. Masuk ke konsol lokal host Anda.
 - VMware ESXi - untuk informasi lebih lanjut, lihat. [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
 - Microsoft Hyper-V — untuk informasi selengkapnya, lihat. [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
2. Pada prompt, masukkan angka yang sesuai untuk memilih Gateway Console.
3. Masukkan **h** untuk membuka daftar perintah yang tersedia.
4. Lakukan salah satu dari cara berikut:
 - Jika gateway Anda menggunakan titik akhir publik, di jendela AVAILABLE COMMANDS, masukkan **open-support-channel** untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.

- Jika gateway Anda menggunakan titik akhir VPC, di jendela AVAILABLE COMMANDS, masukkan **open-support-channel**. Jika gateway Anda tidak diaktifkan, berikan titik akhir VPC atau alamat IP untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.

Note

Nomor saluran bukan nomor port Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Sebagai gantinya, gateway membuat koneksi Secure Shell (SSH) (TCP 22) ke server Storage Gateway dan menyediakan saluran dukungan untuk koneksi.

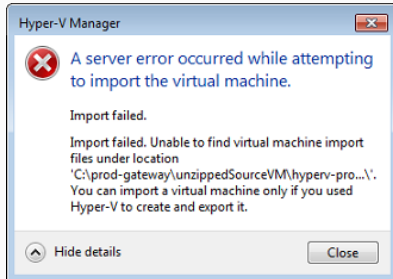
5. Setelah saluran dukungan dibuat, berikan nomor layanan dukungan Anda AWS Support sehingga AWS Support dapat memberikan bantuan pemecahan masalah.
6. Ketika sesi dukungan selesai, masukkan **q** untuk mengakhirinya. Jangan menutup sesi sampai Amazon Web Services Support memberi tahu Anda bahwa sesi dukungan telah selesai.
7. Masuk **exit** untuk keluar dari konsol konsol gateway.
8. Ikuti petunjuk untuk keluar dari konsol lokal.

Memecahkan masalah pengaturan Microsoft Hyper-V

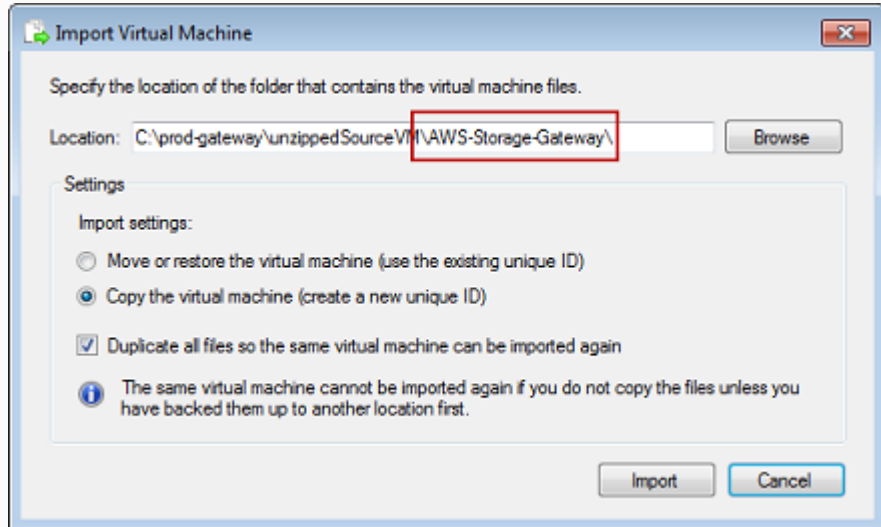
Tabel berikut mencantumkan masalah umum yang mungkin Anda temui saat menerapkan Storage Gateway di platform Microsoft Hyper-V.

Isu	Tindakan yang Harus Dilakukan
<p>Anda mencoba mengimpor gateway dan menerima pesan galat: "Impor gagal. Tidak dapat menemukan file impor mesin virtual di bawah lokasi..."</p>	<p>Kesalahan ini dapat terjadi karena alasan berikut:</p> <ul style="list-style-type: none"> • Jika Anda tidak menunjuk ke root dari file sumber gateway yang tidak di-zip. Bagian terakhir dari lokasi yang Anda tentukan dalam kotak dialog Impor Mesin Virtual seharusnya <code>AWS-Storage-Gateway</code>, seperti yang ditunjukkan contoh berikut:

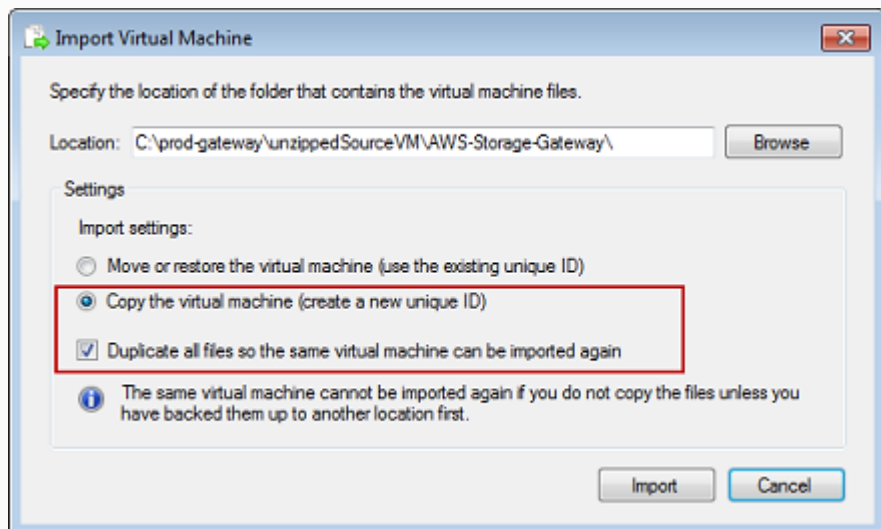
Isu

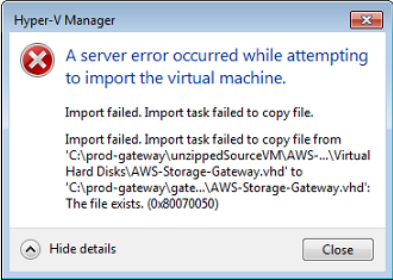
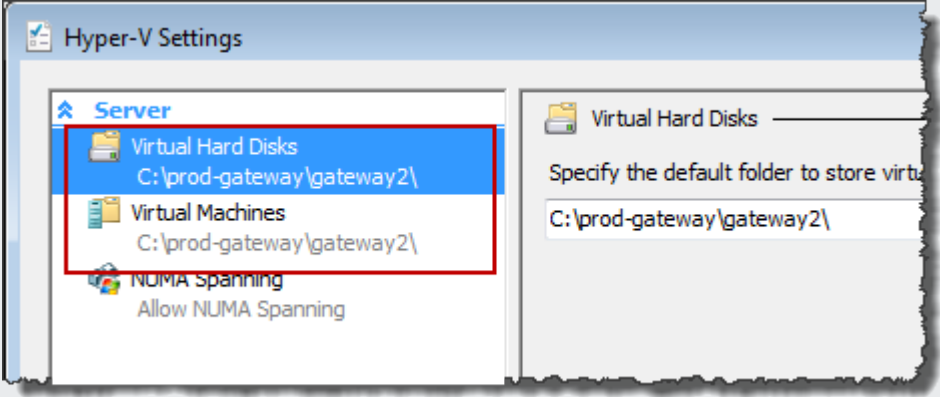


Tindakan yang Harus Dilakukan

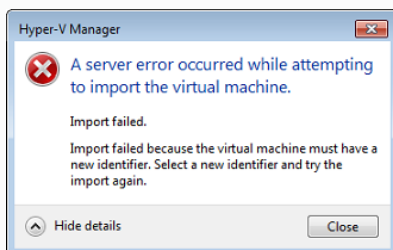


- Jika Anda telah menerapkan gateway dan Anda tidak memilih opsi Salin mesin virtual dan centang opsi Duplikat semua file di kotak dialog Impor Mesin Virtual, maka VM dibuat di lokasi di mana Anda memiliki file gateway yang tidak di-zip dan Anda tidak dapat mengimpor dari lokasi ini lagi. Untuk memperbaiki masalah ini, dapatkan salinan baru dari file sumber gateway yang tidak di-zip dan salin ke lokasi baru. Gunakan lokasi baru sebagai sumber impor. Contoh berikut menunjukkan opsi yang harus Anda periksa apakah Anda berencana membuat beberapa gateway dari satu lokasi file sumber yang tidak di-zip.

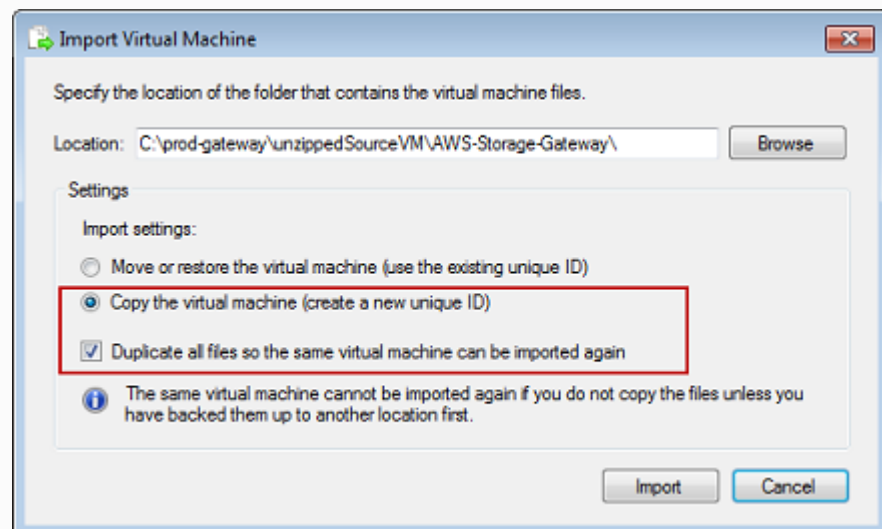


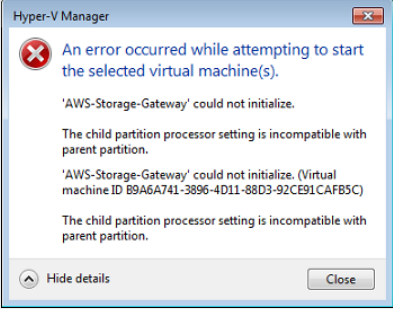
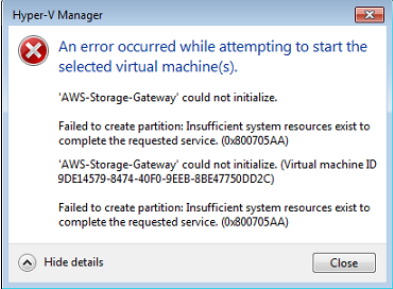
Isu	Tindakan yang Harus Dilakukan
<p>Anda mencoba mengimpor gateway dan menerima pesan galat: “Impor gagal. Tugas impor gagal menyalin file.”</p> 	<p>Jika Anda telah menggunakan gateway dan Anda mencoba menggunakan kembali folder default yang menyimpan file hard disk virtual dan file konfigurasi mesin virtual, maka kesalahan ini akan terjadi. Untuk memperbaiki masalah ini, tentukan lokasi baru di kotak dialog Pengaturan Hyper-V.</p> 

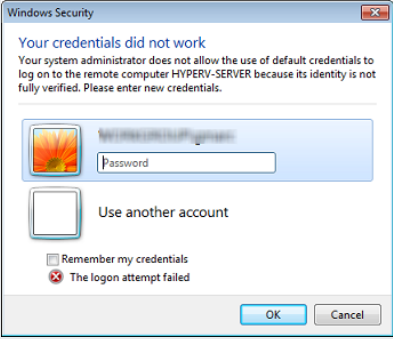
Anda mencoba mengimpor gateway dan menerima pesan galat: “Impor gagal. Impor gagal karena mesin virtual harus memiliki pengenal baru. Pilih pengenal baru dan coba impor lagi.



Saat Anda mengimpor gateway, pastikan Anda memilih opsi Salin mesin virtual dan centang Duplikat semua file pilihan di kotak dialog Impor Mesin Virtual untuk membuat ID unik baru untuk VM. Contoh berikut menunjukkan opsi di kotak dialog Impor Mesin Virtual yang harus Anda gunakan.



Isu	Tindakan yang Harus Dilakukan
<p>Anda mencoba memulai VM gateway dan menerima pesan kesalahan “Pengaturan prosesor partisi anak tidak kompatibel dengan partisi induk.”</p> 	<p>Kesalahan ini kemungkinan disebabkan oleh perbedaan CPU antara CPU yang diperlukan untuk gateway dan CPU yang tersedia di host. Pastikan jumlah CPU VM didukung oleh hypervisor yang mendasarinya.</p> <p>Untuk informasi selengkapnya tentang persyaratan Storage Gateway, lihat Persyaratan.</p>
<p>Anda mencoba memulai VM gateway dan menerima pesan kesalahan “Gagal membuat partisi: Sumber daya tidak cukup ada untuk menyelesaikan layanan yang diminta.”</p> 	<p>Kesalahan ini kemungkinan disebabkan oleh perbedaan RAM antara RAM yang diperlukan untuk gateway dan RAM yang tersedia di host.</p> <p>Untuk informasi selengkapnya tentang persyaratan Storage Gateway, lihat Persyaratan.</p>
<p>Snapshot dan pembaruan perangkat lunak gateway Anda terjadi pada waktu yang sedikit berbeda dari yang diharapkan.</p>	<p>Jam gerbang VM mungkin diimbangi dari waktu aktual, yang dikenal sebagai penyimpangan jam. Periksa dan perbaiki waktu VM menggunakan opsi sinkronisasi waktu konsol gateway lokal. Untuk informasi selengkapnya, lihat Menyinkronkan Waktu VM Gateway Anda.</p>

Isu	Tindakan yang Harus Dilakukan
<p>Anda harus meletakkan file Microsoft Hyper-V Storage Gateway yang tidak di-zip pada sistem file host.</p>	<p>Akses host saat Anda melakukan server Microsoft Windows biasa. Misalnya, jika host hypervisor adalah <code>namahyperv-server</code>, maka Anda dapat menggunakan jalur UNC berikut <code>\\hyperv-server\c\$</code>, yang mengasumsikan bahwa nama tersebut <code>hyperv-server</code> dapat diselesaikan atau didefinisikan dalam file host lokal Anda.</p>
<p>Anda diminta untuk kredensial saat menghubungkan ke hypervisor.</p> 	<p>Tambahkan kredensi pengguna Anda sebagai administrator lokal untuk host hypervisor dengan menggunakan alat <code>sconfig.cmd</code>.</p>
<p>Anda mungkin melihat kinerja jaringan yang buruk jika Anda mengaktifkan antrian mesin virtual (VMQ) pada host Hyper-V yang menggunakan adaptor jaringan Broadcom.</p>	<p>Untuk informasi tentang solusi, lihat dokumentasi Microsoft, lihat Kinerja jaringan yang buruk pada mesin virtual pada host Windows Server 2012 Hyper-V jika VMQ diaktifkan.</p>

Memecahkan masalah gateway Amazon EC2

Di bagian berikut, Anda dapat menemukan masalah umum yang mungkin Anda temui saat bekerja dengan gateway yang diterapkan di Amazon EC2. Untuk informasi selengkapnya tentang perbedaan antara gateway lokal dan gateway yang digunakan di Amazon EC2, lihat. [Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway](#)

Topik

- [Aktivasi gateway Anda tidak terjadi setelah beberapa saat](#)
- [Anda tidak dapat menemukan instans gateway EC2 di daftar instans](#)
- [Anda membuat volume Amazon EBS tetapi tidak dapat melampirkannya ke instans gateway EC2](#)
- [Anda mendapatkan pesan bahwa Anda tidak memiliki disk yang tersedia saat Anda mencoba menambahkan volume penyimpanan](#)
- [Anda ingin menghapus disk yang dialokasikan sebagai ruang buffer unggah untuk mengurangi ruang buffer unggah](#)
- [Throughput ke atau dari gateway EC2 Anda turun ke nol](#)
- [Anda AWS Support ingin membantu memecahkan masalah gateway EC2 Anda](#)
- [Anda ingin terhubung ke instans gateway menggunakan konsol serial Amazon EC2](#)

Aktivasi gateway Anda tidak terjadi setelah beberapa saat

Periksa hal berikut di konsol Amazon EC2:

- Port 80 diaktifkan di grup keamanan yang Anda kaitkan dengan instans. Untuk informasi selengkapnya tentang menambahkan aturan grup keamanan, lihat [Menambahkan aturan grup keamanan](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.
- Instance gateway ditandai sebagai berjalan. Di konsol Amazon EC2, nilai Status untuk instance harus RUNNING.
- Pastikan jenis instans Amazon EC2 Anda memenuhi persyaratan minimum, seperti yang dijelaskan dalam [Persyaratan penyimpanan](#)

Setelah memperbaiki masalah, coba aktifkan gateway lagi. Untuk melakukannya, buka konsol Storage Gateway, pilih Deploy Gateway baru di Amazon EC2, dan masukkan kembali alamat IP instans.

Anda tidak dapat menemukan instans gateway EC2 di daftar instans

Jika Anda tidak memberikan tag sumber daya pada instans Anda dan memiliki banyak instance yang berjalan, mungkin sulit untuk mengetahui instance mana yang Anda luncurkan. Dalam hal ini, Anda dapat mengambil tindakan berikut untuk menemukan instance gateway:

- Periksa nama Amazon Machine Image (AMI) pada tab Deskripsi instance. Sebuah instance berdasarkan Storage Gateway AMI harus dimulai dengan teks **saws-storage-gateway-ami**.
- Jika Anda memiliki beberapa instance berdasarkan Storage Gateway AMI, periksa waktu peluncuran instans untuk menemukan instance yang benar.

Anda membuat volume Amazon EBS tetapi tidak dapat melampirkannya ke instans gateway EC2

Periksa apakah volume Amazon EBS yang dimaksud berada di Availability Zone yang sama dengan instance gateway. Jika terdapat perbedaan dalam Availability Zones, buat volume Amazon EBS baru di Availability Zone yang sama dengan instans Anda.

Anda mendapatkan pesan bahwa Anda tidak memiliki disk yang tersedia saat Anda mencoba menambahkan volume penyimpanan

Untuk gateway yang baru diaktifkan, tidak ada penyimpanan volume yang ditentukan. Sebelum Anda dapat menentukan penyimpanan volume, Anda harus mengalokasikan disk lokal ke gateway untuk digunakan sebagai buffer unggahan dan penyimpanan cache. Untuk gateway yang digunakan ke Amazon EC2, disk lokal adalah volume Amazon EBS yang dilampirkan ke instans. Pesan kesalahan ini kemungkinan terjadi karena tidak ada volume Amazon EBS yang ditentukan untuk instance tersebut.

Periksa perangkat blok yang ditentukan untuk instance yang menjalankan gateway. Jika hanya ada dua perangkat blok (perangkat default yang disertakan dengan AMI), maka Anda harus menambahkan penyimpanan. Untuk informasi selengkapnya tentang cara melakukannya, lihat [Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway](#). Setelah melampirkan dua atau lebih volume Amazon EBS, coba buat penyimpanan volume di gateway.

Anda ingin menghapus disk yang dialokasikan sebagai ruang buffer unggah untuk mengurangi ruang buffer unggah

Ikuti langkah-langkahnya di [Menentukan ukuran buffer unggahan yang akan dialokasikan](#).

Throughput ke atau dari gateway EC2 Anda turun ke nol

Verifikasi bahwa instance gateway sedang berjalan. Jika instance dimulai karena reboot, misalnya, tunggu instance dimulai ulang.

Juga, verifikasi bahwa IP gateway tidak berubah. Jika instance dihentikan dan kemudian dimulai ulang, alamat IP instance mungkin telah berubah. Dalam hal ini, Anda perlu mengaktifkan gateway baru.

Anda dapat melihat throughput ke dan dari gateway Anda dari CloudWatch konsol Amazon. Untuk informasi selengkapnya tentang mengukur throughput ke dan dari gateway Anda dan AWS, lihat [Mengukur Kinerja Antara Tape Gateway Anda dan AWS](#).

Anda AWS Support ingin membantu memecahkan masalah gateway EC2 Anda

Storage Gateway menyediakan konsol lokal yang dapat Anda gunakan untuk melakukan beberapa tugas pemeliharaan, termasuk mengaktifkan AWS Support untuk mengakses gateway Anda untuk membantu Anda mengatasi masalah gateway. Secara default, AWS Support akses ke gateway Anda dinonaktifkan. Anda menyediakan akses ini melalui konsol lokal Amazon EC2. Anda masuk ke konsol lokal Amazon EC2 melalui Secure Shell (SSH). Untuk berhasil masuk melalui SSH, grup keamanan instans Anda harus memiliki aturan yang membuka port TCP 22.

Note

Jika Anda menambahkan aturan baru ke grup keamanan yang sudah ada, aturan baru berlaku untuk semua instans yang menggunakan grup keamanan tersebut. Untuk informasi selengkapnya tentang grup keamanan dan cara menambahkan aturan grup keamanan, lihat [Grup keamanan Amazon EC2 di Panduan Pengguna Amazon EC2](#).

Untuk mengizinkan AWS Support koneksi ke gateway, pertama-tama Anda masuk ke konsol lokal untuk instans Amazon EC2, navigasikan ke konsol Storage Gateway, lalu berikan akses.

Untuk mengaktifkan AWS Support akses ke gateway yang digunakan pada instans Amazon EC2

1. Masuk ke konsol lokal untuk instans Amazon EC2 Anda. Untuk petunjuk, buka [Connect to your instance](#) di Panduan Pengguna Amazon EC2.

Anda dapat menggunakan perintah berikut ini untuk masuk ke konsol lokal instans EC2.

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

Note

PRIVATE-KEY adalah .pem file yang berisi sertifikat pribadi dari key pair EC2 yang Anda gunakan untuk meluncurkan instans Amazon EC2. Untuk informasi selengkapnya, lihat [Mengambil kunci publik untuk key pair Anda](#) di Panduan Pengguna Amazon EC2.

INSTANCE-PUBLIC-DNS-NAME adalah nama Public Domain Name System (DNS) dari instans Amazon EC2 tempat gateway Anda berjalan. Anda mendapatkan nama DNS publik ini dengan memilih instans Amazon EC2 di konsol EC2 dan mengklik tab Deskripsi.

2. Pada prompt, masuk **6 - Command Prompt** untuk membuka konsol AWS Support Saluran.
3. Masukkan **h** Untuk membuka kotak dialog PERINTAH YANG TERSEDIA jendela.
4. Lakukan salah satu dari cara berikut:
 - Jika gateway Anda menggunakan titik akhir publik, di jendela AVAILABLE COMMANDS, masukkan **open-support-channel** untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.
 - Jika gateway Anda menggunakan titik akhir VPC, di jendela AVAILABLE COMMANDS, masukkan. **open-support-channel** Jika gateway Anda tidak diaktifkan, berikan titik akhir VPC atau alamat IP untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.

Note

Nomor saluran bukan nomor port Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Sebagai gantinya, gateway membuat koneksi Secure Shell (SSH) (TCP 22) ke server Storage Gateway dan menyediakan saluran dukungan untuk koneksi.

5. Setelah saluran dukungan dibuat, berikan nomor layanan dukungan Anda AWS Support sehingga AWS Support dapat memberikan bantuan pemecahan masalah.

6. Ketika sesi dukungan selesai, masukkan **q** untuk mengakhirinya. Jangan menutup sesi sampai AWS Support memberi tahu Anda bahwa sesi dukungan telah selesai.
7. Masuk **exit** untuk keluar dari konsol Storage Gateway.
8. Ikuti menu konsol untuk keluar dari instance Storage Gateway.

Anda ingin terhubung ke instans gateway menggunakan konsol serial Amazon EC2

Anda dapat menggunakan konsol serial Amazon EC2 untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya. Untuk petunjuk dan tips pemecahan masalah, lihat Konsol [Serial Amazon EC2](#) di Panduan Pengguna Amazon Elastic Compute Cloud.

Memecahkan masalah alat perangkat keras

Topik berikut membahas masalah yang mungkin Anda temui dengan Storage Gateway Hardware Appliance, dan saran tentang pemecahan masalah ini.

Anda tidak dapat menentukan alamat IP layanan

Ketika mencoba untuk terhubung ke layanan Anda, pastikan bahwa Anda menggunakan alamat IP layanan dan bukan alamat IP host. Konfigurasikan alamat IP layanan di konsol layanan, dan alamat IP host di konsol perangkat keras. Anda melihat konsol perangkat keras saat Anda memulai alat perangkat keras. Untuk pergi ke konsol layanan dari konsol perangkat keras, pilih Open Service Console.

Bagaimana Anda melakukan reset pabrik?

Jika Anda perlu melakukan reset pabrik pada alat Anda, hubungi tim Storage Gateway Hardware Appliance untuk mendapatkan dukungan, seperti yang dijelaskan di bagian Support berikut.

Bagaimana Anda melakukan restart jarak jauh?

Jika Anda perlu melakukan restart alat dari jarak jauh, Anda dapat melakukannya menggunakan antarmuka manajemen Dell iDRAC. Untuk informasi selengkapnya, lihat [Siklus Daya Virtual iDRAC9: Siklus daya jarak jauh PowerEdge Server EMC Dell di situs web](#) Dell Technologies. InfoHub

Di mana Anda mendapatkan dukungan Dell iDRac?

Server Dell PowerEdge R640 dilengkapi dengan antarmuka manajemen Dell iDRac. Sebaiknya lakukan hal berikut:

- Jika Anda menggunakan antarmuka manajemen iDRac, Anda harus mengubah kata sandi default. Untuk informasi selengkapnya tentang kredensial iDRac, [lihat PowerEdge Dell - Apa kredensial login default untuk iDRac?](#) .
- Pastikan firmware tersebut up-to-date untuk mencegah pelanggaran keamanan.
- Memindahkan antarmuka jaringan iDRac ke port normal em () dapat menyebabkan masalah kinerja atau mencegah fungsi normal alat.

Anda tidak dapat menemukan nomor seri alat perangkat keras

Untuk menemukan nomor seri alat perangkat keras, buka halaman ikhtisar perangkat keras di konsol Storage Gateway, seperti yang ditunjukkan berikut.

Tab perangkat keras konsol Storage Gateway dengan alat yang dipilih dan detail ditampilkan.

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

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

Below the table, the "Details" tab is active, showing the following information:

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

Tab perangkat keras konsol Storage Gateway dengan alat yang dipilih dan detail ditampilkan.

Di mana mendapatkan dukungan alat perangkat keras

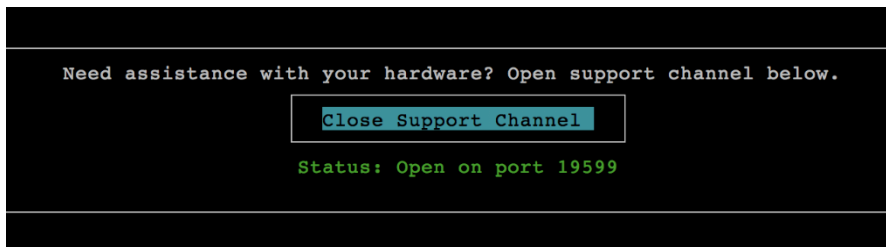
Untuk menghubungi dukungan Storage Gateway Hardware Appliance, lihat [AWS Support](#).

AWS Support Tim mungkin meminta Anda untuk mengaktifkan saluran dukungan untuk memecahkan masalah gateway Anda dari jarak jauh. Anda tidak perlu port ini terbuka untuk operasi normal

gateway Anda, tetapi diperlukan untuk pemecahan masalah. Anda dapat mengaktifkan saluran dukungan dari konsol perangkat keras seperti yang ditunjukkan pada prosedur berikut.

Untuk membuka saluran dukungan untuk AWS

1. Buka konsol perangkat keras.
2. Pilih Open Support Channel seperti yang ditunjukkan berikut.
konsol alat perangkat keras dengan status saluran dukungan ditampilkan.



konsol alat perangkat keras dengan status saluran dukungan ditampilkan.

Nomor port yang ditetapkan akan muncul dalam 30 detik, jika tidak ada konektivitas jaringan atau masalah firewall.

3. Perhatikan nomor port dan berikan ke AWS Support.

Memecahkan masalah rekaman virtual

Anda dapat menemukan informasi berikut tentang tindakan yang harus diambil jika Anda mengalami masalah tak terduga dengan kaset virtual Anda.

Topik

- [Memulihkan Pita Virtual Dari Gateway yang Tidak Dapat Dipulihkan](#)
- [Memecahkan Masalah Kaset yang Tidak Dapat Dipulihkan](#)
- [Pemberitahuan Kesehatan Ketersediaan Tinggi](#)

Memulihkan Pita Virtual Dari Gateway yang Tidak Dapat Dipulihkan

Meskipun jarang terjadi, Tape Gateway Anda mungkin mengalami kegagalan yang tidak dapat dipulihkan. Kegagalan seperti itu dapat terjadi di host hypervisor Anda, gateway itu sendiri, atau disk cache. Jika terjadi kegagalan, Anda dapat memulihkan kaset Anda dengan mengikuti petunjuk pemecahan masalah di bagian ini.

Topik

- [Anda Perlu Memulihkan Pita Virtual dari Gateway Tape yang Rusak](#)
- [Anda Perlu Memulihkan Pita Virtual dari Disk Cache yang Rusak](#)

Anda Perlu Memulihkan Pita Virtual dari Gateway Tape yang Rusak

Jika Tape Gateway atau host hypervisor mengalami kegagalan yang tidak dapat dipulihkan, Anda dapat memulihkan data apa pun yang telah diunggah ke Tape Gateway lain. AWS

Perhatikan bahwa data yang ditulis ke kaset mungkin tidak sepenuhnya diunggah sampai rekaman itu berhasil diarsipkan ke dalam VTS. Data pada kaset yang dipulihkan ke gateway lain dengan cara ini mungkin tidak lengkap atau kosong. Kami merekomendasikan melakukan inventaris pada semua kaset yang dipulihkan untuk memastikan mereka berisi konten yang diharapkan.

Untuk memulihkan kaset ke Tape Gateway lain

1. Identifikasi Tape Gateway yang berfungsi sebagai gateway target pemulihan Anda. Jika Anda tidak memiliki Tape Gateway untuk memulihkan kaset Anda, buat Tape Gateway baru. Untuk informasi tentang cara membuat gateway, lihat [Membuat Gateway](#).
2. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
3. Di panel navigasi, pilih Gateway, lalu pilih Tape Gateway tempat Anda ingin memulihkan kaset.
4. Pilih tab Detail. Pesan pemulihan tape ditampilkan di tab.
5. Pilih Buat kaset pemulihan untuk menonaktifkan gateway.
6. Di kotak dialog yang muncul, pilih Nonaktifkan gateway.

Proses ini secara permanen menghentikan fungsi normal Tape Gateway Anda dan memperlihatkan titik pemulihan yang tersedia. Untuk petunjuk, lihat [Menonaktifkan Gateway Tape Anda](#).

7. Dari kaset yang ditampilkan gateway yang dinonaktifkan, pilih pita virtual dan titik pemulihan yang ingin Anda pulihkan. Rekaman virtual dapat memiliki beberapa titik pemulihan.
8. Untuk mulai memulihkan kaset apa pun yang Anda butuhkan ke Tape Gateway target, pilih Buat pita pemulihan.
9. Dalam kotak dialog Buat pita pemulihan, verifikasi kode batang pita virtual yang ingin Anda pulihkan.
10. Untuk Gateway, pilih Tape Gateway yang ingin Anda pulihkan kaset virtual.
11. Pilih Buat pita pemulihan.

12. Hapus Tape Gateway yang gagal sehingga Anda tidak dikenakan biaya. Untuk petunjuk, lihat [Menghapus Gateway Anda dengan Menggunakan AWS Storage Gateway Konsol dan Menghapus Sumber Daya Terkait](#).

Storage Gateway memindahkan tape dari Tape Gateway yang gagal ke Tape Gateway yang Anda tentukan. Tape Gateway menandai status rekaman sebagai RECOVERY.

Anda Perlu Memulihkan Pita Virtual dari Disk Cache yang Rusak

Jika disk cache Anda mengalami kesalahan, gateway mencegah operasi baca dan tulis pada kaset virtual di gateway. Misalnya, kesalahan dapat terjadi ketika disk rusak atau dihapus dari gateway. Konsol Storage Gateway menampilkan pesan tentang kesalahan.

Dalam pesan kesalahan, Storage Gateway meminta Anda untuk mengambil salah satu dari dua tindakan yang dapat memulihkan kaset Anda:

- Shut Down dan Re-Add Disks — Ambil pendekatan ini jika disk memiliki data utuh dan telah dihapus. Misalnya, jika kesalahan terjadi karena disk dihapus dari host Anda secara tidak sengaja tetapi disk dan data utuh, Anda dapat menambahkan kembali disk. Untuk melakukan ini, lihat prosedurnya nanti dalam topik ini.
- Reset Cache Disk — Ambil pendekatan ini jika disk cache rusak atau tidak dapat diakses. Jika kesalahan disk menyebabkan disk cache tidak dapat diakses, tidak dapat digunakan, atau rusak, Anda dapat mengatur ulang disk. Jika Anda mengatur ulang disk cache, kaset yang memiliki data bersih (yaitu, kaset yang datanya di disk cache dan Amazon S3 disinkronkan) akan terus tersedia untuk Anda gunakan. Namun, kaset yang memiliki data yang tidak disinkronkan dengan Amazon S3 secara otomatis dipulihkan. Status kaset ini diatur ke RECOVERY, tetapi kasetnya hanya akan dibaca. Untuk informasi tentang cara menghapus disk dari host Anda, lihat [Menentukan ukuran buffer unggahan yang akan dialokasikan](#).

Important

Jika disk cache yang Anda atur ulang berisi data yang belum diunggah ke Amazon S3, data tersebut dapat hilang. Setelah Anda mengatur ulang disk cache, tidak ada disk cache yang dikonfigurasi yang tersisa di gateway, jadi Anda harus mengonfigurasi setidaknya satu disk cache baru agar gateway Anda berfungsi dengan baik.

Untuk mengatur ulang disk cache, lihat prosedur nanti dalam topik ini.

Untuk mematikan dan menambahkan kembali disk

1. Matikan pintu gerbangnya. Untuk informasi tentang cara mematikan gateway, lihat [Mematikan VM Gateway Anda](#).
2. Tambahkan disk kembali ke host Anda, dan pastikan nomor node disk tidak berubah. Untuk informasi tentang cara menambahkan disk, lihat [Menentukan ukuran buffer unggahan yang akan dialokasikan](#).
3. Mulai ulang gateway. Untuk informasi tentang cara memulai ulang gateway, lihat [Mematikan VM Gateway Anda](#).

Setelah gateway dimulai ulang, Anda dapat memverifikasi status disk cache. Status disk dapat berupa salah satu dari yang berikut:

- Present — Disk tersedia untuk digunakan.
- hilang — Disk tidak lagi terhubung ke gateway.
- ketidakcocokan — Node disk ditempati oleh disk yang memiliki metadata yang salah, atau konten disk rusak.

Untuk mengatur ulang dan mengkonfigurasi ulang disk cache

1. Dalam pesan kesalahan A disk telah terjadi yang diilustrasikan sebelumnya, pilih Reset Cache Disk.
2. Pada halaman Configure gateway, konfigurasi disk untuk penyimpanan cache. Untuk informasi tentang cara melakukannya, lihat [Mengkonfigurasi Gateway Tape Anda](#).
3. Setelah Anda mengkonfigurasi penyimpanan cache, matikan dan restart gateway seperti yang dijelaskan dalam prosedur sebelumnya.

Gateway harus pulih setelah restart. Anda kemudian dapat memverifikasi status disk cache.

Untuk memverifikasi status disk cache

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway Anda.
3. Untuk Tindakan, pilih Konfigurasi Penyimpanan Lokal untuk menampilkan kotak dialog Konfigurasi Penyimpanan Lokal. Kotak dialog ini menampilkan semua disk lokal di gateway.

Status node disk cache ditampilkan di sebelah disk.

Note

Jika Anda tidak menyelesaikan proses pemulihan, gateway akan menampilkan spanduk yang meminta Anda untuk mengonfigurasi penyimpanan lokal.

Memecahkan Masalah Kaset yang Tidak Dapat Dipulihkan

Jika rekaman virtual Anda gagal secara tak terduga, Storage Gateway menetapkan status rekaman virtual yang gagal ke IRRECOVERABLE. Tindakan yang Anda ambil tergantung pada keadaan. Anda dapat menemukan informasi berikut tentang beberapa masalah yang mungkin Anda temukan, dan cara memecahkan masalah tersebut.

Anda Perlu Memulihkan Data Dari Pita yang Tidak Dapat Dipulihkan

Jika Anda memiliki rekaman virtual dengan status IRRECOVERABLE, dan Anda perlu bekerja dengannya, coba salah satu dari yang berikut ini:

- Aktifkan Tape Gateway baru jika Anda belum mengaktifkannya. Untuk informasi selengkapnya, lihat [Membuat Gateway](#).
- Nonaktifkan Tape Gateway yang berisi pita yang tidak dapat dipulihkan, dan pulihkan kaset dari titik pemulihan ke Tape Gateway baru. Untuk informasi selengkapnya, lihat [Anda Perlu Memulihkan Pita Virtual dari Gateway Tape yang Rusak](#).

Note

Anda harus mengonfigurasi ulang inisiator iSCSI dan aplikasi cadangan untuk menggunakan Tape Gateway baru. Untuk informasi selengkapnya, lihat [Menghubungkan Perangkat VTL Anda](#).

Anda Tidak Perlu Pita YANG TIDAK DAPAT DIPULIHKAN Yang Tidak Diarsipkan

Jika Anda memiliki rekaman virtual dengan status IRRECOVERABLE, Anda tidak membutuhkannya, dan rekaman itu tidak pernah diarsipkan, Anda harus menghapus rekaman itu. Untuk informasi selengkapnya, lihat [Menghapus Kaset](#).

Disk Cache di Gateway Anda Menghadapi Kegagalan

Jika satu atau beberapa disk cache di gateway Anda mengalami kegagalan, gateway mencegah operasi baca dan tulis ke kaset dan volume virtual Anda. Untuk melanjutkan fungsionalitas normal, konfigurasi ulang gateway Anda seperti yang dijelaskan berikut:

- Jika disk cache tidak dapat diakses atau tidak dapat digunakan, hapus disk dari konfigurasi gateway Anda.
- Jika disk cache masih dapat diakses dan digunakan, sambungkan kembali ke gateway Anda.

Note

Jika Anda menghapus disk cache, kaset atau volume yang memiliki data bersih (yaitu, untuk mana data dalam disk cache dan Amazon S3 disinkronkan) akan terus tersedia ketika gateway melanjutkan fungsionalitas normal. Misalnya, jika gateway Anda memiliki tiga disk cache dan Anda menghapus dua, kaset atau volume yang bersih akan memiliki status TERSEDIA. Kaset dan volume lain akan memiliki status IRRECOVERABLE.

Jika Anda menggunakan disk sementara sebagai disk cache untuk gateway Anda atau memasang disk cache Anda pada drive sementara, disk cache Anda akan hilang saat Anda mematikan gateway. Mematikan gateway saat disk cache dan Amazon S3 Anda tidak disinkronkan dapat mengakibatkan hilangnya data. Akibatnya, kami tidak menyarankan menggunakan drive atau disk sementara.

Pemberitahuan Kesehatan Ketersediaan Tinggi

Saat menjalankan gateway Anda di platform VMware vSphere High Availability (HA), Anda mungkin menerima pemberitahuan kesehatan. Untuk informasi selengkapnya tentang pemberitahuan kesehatan, lihat [Memecahkan masalah ketersediaan tinggi](#).

Memecahkan masalah ketersediaan tinggi

Anda dapat menemukan informasi berikut tentang tindakan yang harus diambil jika Anda mengalami masalah ketersediaan.

Topik

- [Pemberitahuan Kesehatan](#)

- [Metrik](#)

Pemberitahuan Kesehatan

Saat Anda menjalankan gateway Anda di VMware vSphere HA, semua gateway menghasilkan pemberitahuan kesehatan berikut ke grup log Amazon Anda yang dikonfigurasi. CloudWatch Pemberitahuan ini masuk ke aliran log yang disebut `AvailabilityMonitor`.

Topik

- [Pemberitahuan: Reboot](#)
- [Pemberitahuan: HardReboot](#)
- [Pemberitahuan: HealthCheckFailure](#)
- [Pemberitahuan: AvailabilityMonitorTest](#)

Pemberitahuan: Reboot

Anda bisa mendapatkan notifikasi reboot saat gateway VM dimulai ulang. Anda dapat memulai ulang VM gateway dengan menggunakan konsol VM Hypervisor Management atau konsol Storage Gateway. Anda juga dapat memulai ulang dengan menggunakan perangkat lunak gateway selama siklus pemeliharaan gateway.

Tindakan untuk Mengambil

Jika waktu reboot dalam 10 menit dari [waktu mulai pemeliharaan](#) gateway yang dikonfigurasi, ini mungkin kejadian normal dan bukan pertanda masalah. Jika reboot terjadi secara signifikan di luar jendela pemeliharaan, periksa apakah gateway dimulai ulang secara manual.

Pemberitahuan: HardReboot

Anda bisa mendapatkan `HardReboot` notifikasi saat gateway VM dimulai ulang secara tak terduga. Restart semacam itu dapat disebabkan oleh hilangnya daya, kegagalan perangkat keras, atau peristiwa lain. Untuk gateway VMware, reset oleh vSphere High Availability Application Monitoring dapat meluncurkan acara ini.

Tindakan untuk Mengambil

Saat gateway Anda berjalan di lingkungan seperti itu, periksa keberadaan `HealthCheckFailure` notifikasi dan lihat log peristiwa VMware untuk VM.

Pemberitahuan: HealthCheckFailure

Untuk gateway di VMware vSphere HA, Anda bisa mendapatkan `HealthCheckFailure` pemberitahuan ketika pemeriksaan kesehatan gagal dan restart VM diminta. Peristiwa ini juga terjadi selama pengujian untuk memantau ketersediaan, ditunjukkan oleh `AvailabilityMonitorTest` pemberitahuan. Dalam hal ini, `HealthCheckFailure` pemberitahuan diharapkan.

Note

Pemberitahuan ini hanya untuk gateway VMware.

Tindakan untuk Mengambil

Jika peristiwa ini berulang kali terjadi tanpa `AvailabilityMonitorTest` pemberitahuan, periksa infrastruktur VM Anda untuk masalah (penyimpanan, memori, dan sebagainya). Jika Anda membutuhkan bantuan tambahan, hubungi AWS Support.

Pemberitahuan: AvailabilityMonitorTest

Untuk gateway di VMware vSphere HA, Anda bisa mendapatkan `AvailabilityMonitorTest` pemberitahuan ketika Anda [menjalankan tes Ketersediaan dan sistem pemantauan aplikasi](#) di VMware.

Metrik

`AvailabilityNotifications` metrik tersedia di semua gateway. Metrik ini adalah hitungan jumlah pemberitahuan kesehatan terkait ketersediaan yang dihasilkan oleh gateway. Gunakan Sum statistik untuk mengamati apakah gateway mengalami peristiwa terkait ketersediaan. Konsultasikan dengan grup CloudWatch log Anda yang dikonfigurasi untuk detail tentang peristiwa tersebut.

Praktik terbaik untuk memulihkan data Anda

Meskipun jarang, gateway Anda mungkin mengalami kegagalan yang tidak dapat dipulihkan. Kegagalan seperti itu dapat terjadi di mesin virtual Anda (VM), gateway itu sendiri, penyimpanan lokal, atau di tempat lain. Jika terjadi kegagalan, kami sarankan Anda mengikuti petunjuk di bagian yang sesuai berikut untuk memulihkan data Anda.

⚠ Important

Storage Gateway tidak mendukung pemulihan VM gateway dari snapshot yang dibuat oleh hypervisor Anda atau dari Amazon EC2 Amazon Machine Image (AMI). Jika VM gateway Anda tidak berfungsi, aktifkan gateway baru dan pulihkan data Anda ke gateway itu menggunakan instruksi berikut.

Topik

- [Memulihkan dari shutdown mesin virtual yang tidak terduga](#)
- [Memulihkan data Anda dari gateway atau VM yang tidak berfungsi](#)
- [Memulihkan data Anda dari rekaman yang tidak dapat dipulihkan](#)
- [Memulihkan data Anda dari disk cache yang tidak berfungsi](#)
- [Memulihkan data Anda dari pusat data yang tidak dapat diakses](#)

Memulihkan dari shutdown mesin virtual yang tidak terduga

Jika VM Anda mati secara tak terduga, misalnya selama pemadaman listrik, gateway Anda menjadi tidak terjangkau. Ketika daya dan konektivitas jaringan dipulihkan, gateway Anda dapat dijangkau dan mulai berfungsi secara normal. Berikut adalah beberapa langkah yang dapat Anda ambil pada saat itu untuk membantu memulihkan data Anda:

- Jika pemadaman menyebabkan masalah konektivitas jaringan, Anda dapat memecahkan masalah tersebut. Untuk informasi tentang cara menguji konektivitas jaringan, lihat [Menguji Koneksi Gateway Anda ke Internet](#).
- Untuk pengaturan kaset, ketika gateway Anda dapat dijangkau, kaset Anda masuk ke status BOOTSTRAPPING. Fungsionalitas ini memastikan bahwa data yang disimpan secara lokal Anda terus disinkronkan. AWS Untuk informasi lebih lanjut tentang status ini, lihat [Memahami Status Pita](#).
- Jika kegagalan fungsi dan masalah gateway Anda terjadi dengan volume atau kaset Anda sebagai akibat dari shutdown yang tidak terduga, Anda dapat memulihkan data Anda. Untuk informasi tentang cara memulihkan data Anda, lihat bagian berikut yang berlaku untuk skenario Anda.

Memulihkan data Anda dari gateway atau VM yang tidak berfungsi

Jika Tape Gateway atau host hypervisor mengalami kegagalan yang tidak dapat dipulihkan, Anda dapat menggunakan langkah-langkah berikut untuk memulihkan kaset dari Gateway Tape yang tidak berfungsi ke Tape Gateway lain:

1. Identifikasi Tape Gateway yang ingin Anda gunakan sebagai target pemulihan, atau buat yang baru.
2. Nonaktifkan gateway yang tidak berfungsi.
3. Buat kaset pemulihan untuk setiap kaset yang ingin Anda pulihkan dan tentukan target Tape Gateway.
4. Hapus Tape Gateway yang tidak berfungsi.

Untuk informasi rinci tentang cara memulihkan kaset dari Tape Gateway yang tidak berfungsi ke Tape Gateway lain, lihat [Anda Perlu Memulihkan Pita Virtual dari Gateway Tape yang Rusak](#)

Memulihkan data Anda dari rekaman yang tidak dapat dipulihkan

Jika rekaman Anda mengalami kegagalan dan status rekaman tidak dapat dipulihkan, kami sarankan Anda menggunakan salah satu opsi berikut untuk memulihkan data Anda atau menyelesaikan kegagalan tergantung pada situasi Anda:

- Jika Anda memerlukan data pada rekaman yang tidak dapat dipulihkan, Anda dapat memulihkan rekaman itu ke gateway baru.
- Jika Anda tidak memerlukan data pada rekaman itu, dan rekaman itu tidak pernah diarsipkan, Anda cukup menghapus kaset dari Tape Gateway Anda.

Untuk informasi rinci tentang cara memulihkan data Anda atau menyelesaikan kegagalan jika rekaman Anda tidak dapat dipulihkan, lihat [Memecahkan Masalah Kaset yang Tidak Dapat Dipulihkan](#)

Memulihkan data Anda dari disk cache yang tidak berfungsi

Jika disk cache Anda mengalami kegagalan, kami sarankan Anda menggunakan langkah-langkah berikut untuk memulihkan data Anda tergantung pada situasi Anda:

- Jika kerusakan terjadi karena disk cache telah dihapus dari host Anda, matikan gateway, tambahkan kembali disk, dan restart gateway.
- Jika disk cache rusak atau tidak dapat diakses, matikan gateway, atur ulang disk cache, konfigurasi ulang disk untuk penyimpanan cache, dan restart gateway.

Untuk detail informasi, lihat [Anda Perlu Memulihkan Pita Virtual dari Disk Cache yang Rusak](#).

Memulihkan data Anda dari pusat data yang tidak dapat diakses

Jika gateway atau pusat data Anda menjadi tidak dapat diakses karena alasan tertentu, Anda dapat memulihkan data Anda ke gateway lain di pusat data yang berbeda atau memulihkan ke gateway yang dihosting pada instans Amazon EC2. Jika Anda tidak memiliki akses ke pusat data lain, sebaiknya buat gateway pada instans Amazon EC2. Langkah-langkah yang Anda ikuti tergantung pada jenis gateway tempat Anda meliput datanya.

Untuk memulihkan data dari Tape Gateway di pusat data yang tidak dapat diakses

1. Buat dan aktifkan Tape Gateway baru di host Amazon EC2. Untuk informasi selengkapnya, lihat [Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway](#).
2. Memulihkan kaset dari gateway sumber di pusat data ke gateway baru yang Anda buat di Amazon EC2 Untuk informasi selengkapnya, lihat. [Memulihkan Pita Virtual Dari Gateway yang Tidak Dapat Dipulihkan](#)

Kaset Anda harus ditutup ke gateway Amazon EC2 yang baru.

Sumber Daya Storage Gateway Tambahan

Bagian ini menjelaskan AWS dan perangkat lunak, alat, dan sumber daya pihak ketiga yang dapat membantu Anda mengatur atau mengelola gateway Anda, dan juga kuota Storage Gateway.

Topik

- [Pengaturan Host](#)
- [Gerbang Pita](#)
- [Mendapatkan kunci aktivasi untuk gateway Anda](#)
- [Menghubungkan Inisiator iSCSI](#)
- [Menggunakan AWS Direct Connect dengan Storage Gateway](#)
- [Persyaratan Pelabuhan](#)
- [Menghubungkan ke Gateway Anda](#)
- [Memahami Sumber Daya Storage Gateway dan ID Sumber Daya](#)
- [Menandai Sumber Daya Storage Gateway](#)
- [Bekerja dengan Komponen Sumber Terbuka untuk AWS Storage Gateway](#)
- [AWS Storage Gateway kuota](#)

Pengaturan Host

Topik

- [Mengkonfigurasi VMware untuk Storage Gateway](#)
- [Menyinkronkan Waktu VM Gateway Anda](#)
- [Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway](#)
- [Menerapkan Amazon EC2 dengan Pengaturan Default](#)
- [Ubah opsi metadata instans Amazon EC2](#)

Mengkonfigurasi VMware untuk Storage Gateway

Saat mengonfigurasi VMware untuk Storage Gateway, pastikan untuk menyinkronkan waktu VM Anda dengan waktu host Anda, konfigurasi VM untuk menggunakan pengontrol disk

paravirtualisasi saat menyediakan penyimpanan dan memberikan perlindungan dari kegagalan pada lapisan infrastruktur yang mendukung VM gateway.

Topik

- [Sinkronisasi Waktu VM dengan Waktu Host](#)
- [Mengkonfigurasi AWS Storage Gateway VM untuk Menggunakan Pengontrol Disk Paravirtualisasi](#)
- [Menggunakan Storage Gateway dengan VMware Ketersediaan Tinggi](#)

Sinkronisasi Waktu VM dengan Waktu Host

Agar berhasil mengaktifkan gateway Anda, Anda harus memastikan bahwa waktu VM Anda disinkronkan dengan waktu host, dan waktu host diatur dengan benar. Di bagian ini, Anda terlebih dahulu menyinkronkan waktu pada VM ke waktu host. Kemudian Anda memeriksa waktu host dan, jika perlu, mengatur waktu host dan mengkonfigurasi host untuk menyinkronkan waktunya secara otomatis ke server Network Time Protocol (NTP).

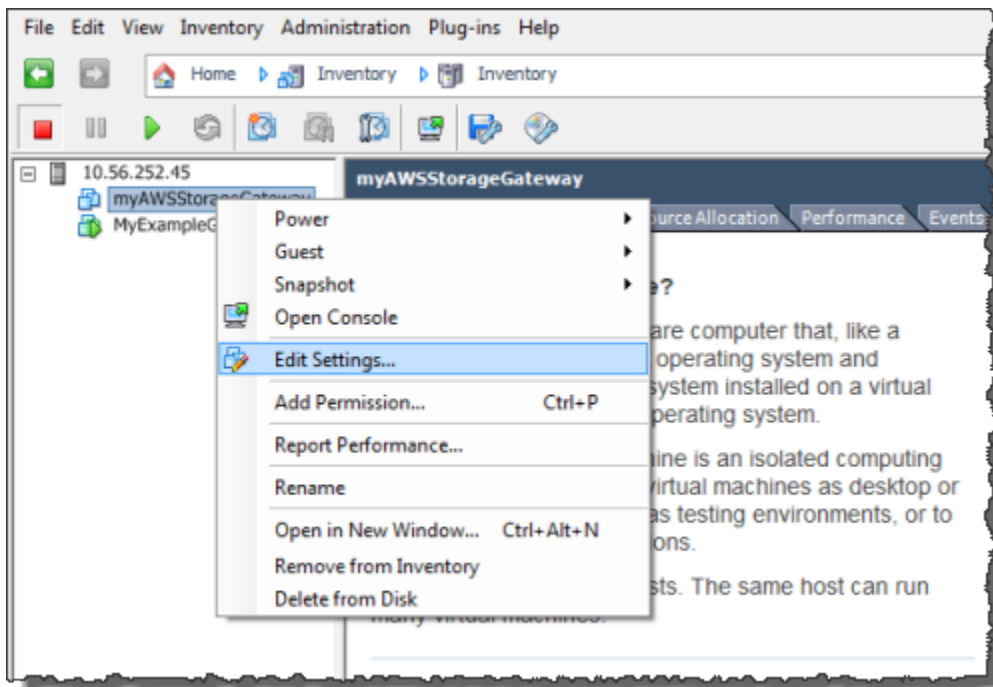
Important

Sinkronisasi waktu VM dengan waktu host diperlukan untuk aktivasi gateway yang berhasil.

Untuk menyinkronkan waktu VM dengan waktu host

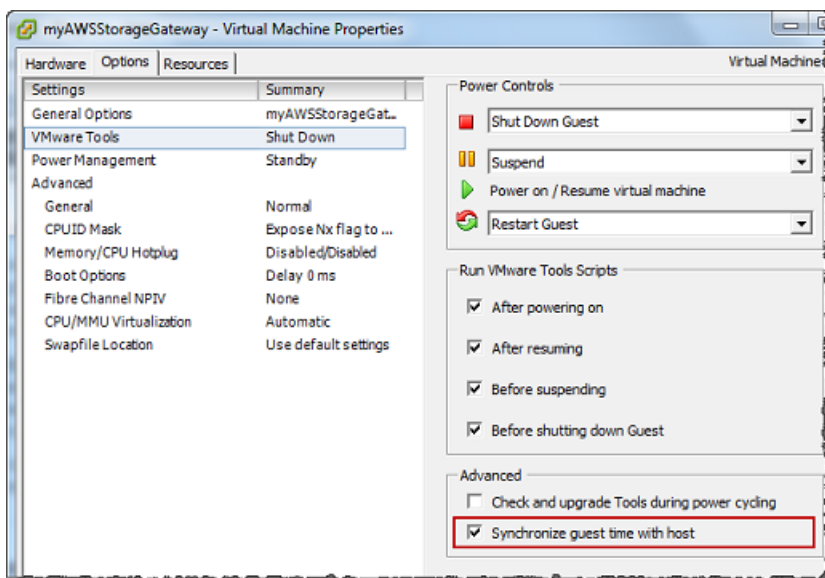
1. Konfigurasi waktu VM Anda.
 - a. Di klien vSphere, buka menu konteks (klik kanan) untuk VM gateway Anda, dan pilih Edit Pengaturan.

Kotak dialog Virtual Machine Properties terbuka.



- b. Pilih tab Opsi, dan pilih Alat VMware di daftar opsi.
- c. Periksa opsi Sinkronisasi waktu tamu dengan host, lalu pilih OK.

VM menyinkronkan waktunya dengan host.

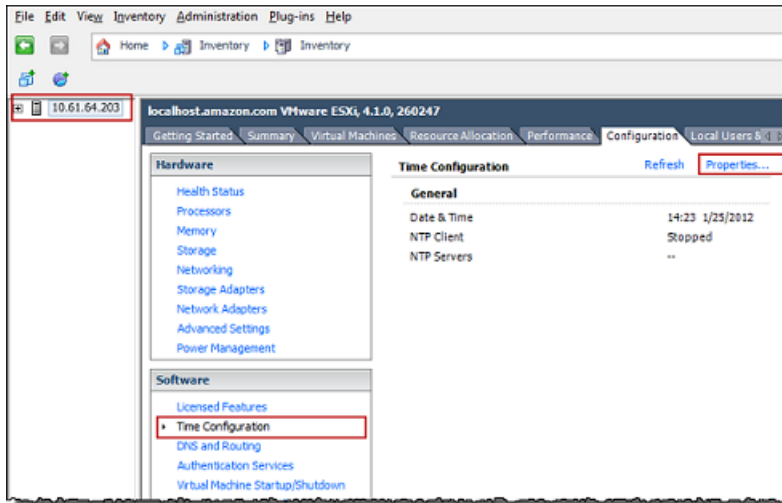


2. Konfigurasi waktu host.

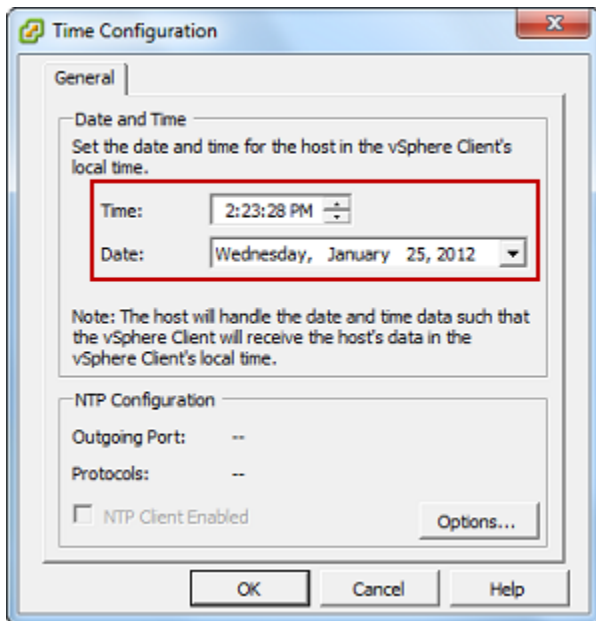
Penting untuk memastikan bahwa jam host Anda diatur ke waktu yang tepat. Jika Anda belum mengonfigurasi jam host Anda, lakukan langkah-langkah berikut untuk mengatur dan menyinkronkannya dengan server NTP.

- a. Di klien VMware vSphere, pilih node host vSphere di panel kiri, lalu pilih tab Konfigurasi.
- b. Pilih Konfigurasi Waktu di panel Perangkat Lunak, lalu pilih tautan Properties.

Kotak dialog Konfigurasi Waktu muncul.

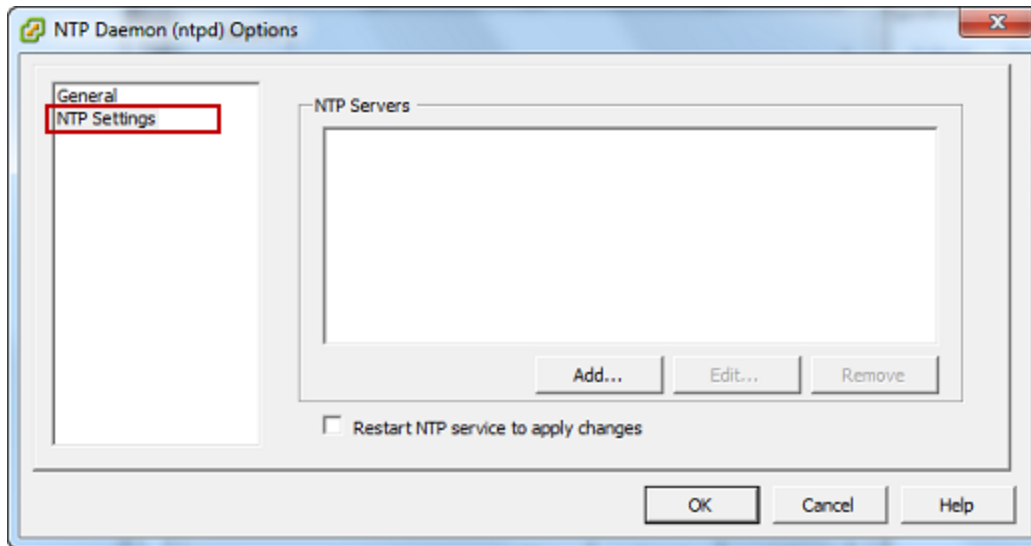


- c. Di panel Tanggal dan Waktu, atur tanggal dan waktu.



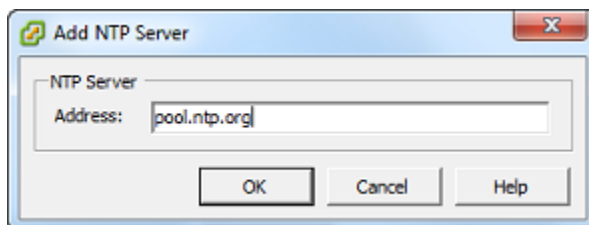
- d. Konfigurasi host untuk menyinkronkan waktunya secara otomatis ke server NTP.

- i. Pilih Opsi di kotak dialog Konfigurasi Waktu, dan kemudian di kotak dialog Opsi Daemon NTP (ntpd), pilih Pengaturan NTP di panel kiri.



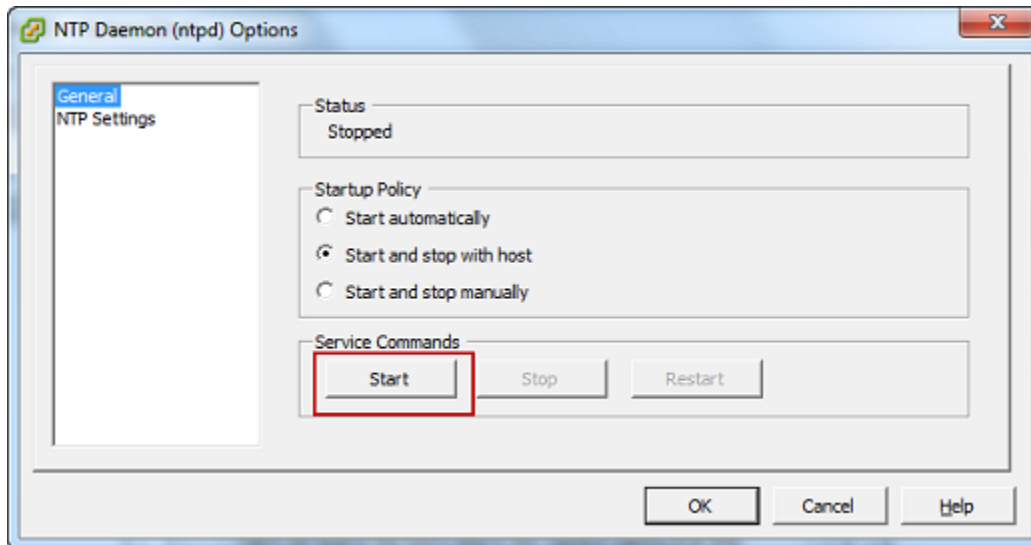
- ii. Pilih Tambah untuk menambahkan server NTP baru.
- iii. Dalam kotak dialog Add NTP Server, ketik alamat IP atau nama domain yang sepenuhnya memenuhi syarat dari server NTP, lalu pilih OK.

Anda dapat menggunakan `pool.ntp.org` seperti yang ditunjukkan pada contoh berikut.



- iv. Dalam kotak dialog Opsi Daemon NTP (ntpd), pilih Umum di panel kiri.
- v. Di panel Perintah Layanan, pilih Mulai untuk memulai layanan.

Perhatikan bahwa jika Anda mengubah referensi server NTP ini atau menambahkan yang lain nanti, Anda harus memulai ulang layanan untuk menggunakan server baru.



- e. Pilih OK untuk menutup kotak dialog Opsi Daemon NTP (ntpd).
- f. Pilih OK untuk menutup kotak dialog Konfigurasi Waktu.

Mengkonfigurasi AWS Storage Gateway VM untuk Menggunakan Pengontrol Disk Paravirtualisasi

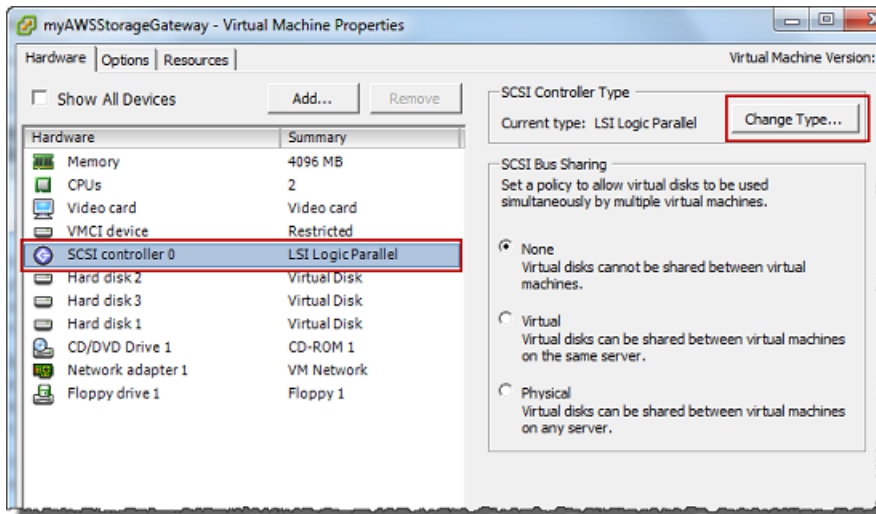
Dalam tugas ini, Anda mengatur pengontrol iSCSI sehingga VM menggunakan paravirtualisasi. Paravirtualisasi adalah mode di mana gateway VM bekerja dengan sistem operasi host sehingga konsol dapat mengidentifikasi disk virtual yang Anda tambahkan ke VM Anda.

Note

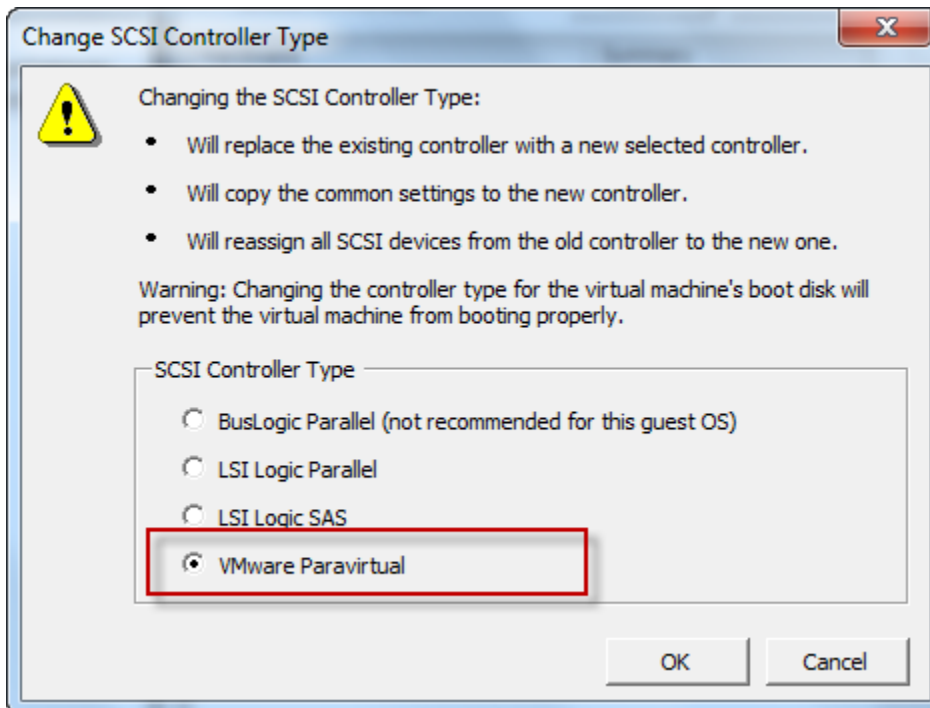
Anda harus menyelesaikan langkah ini untuk menghindari masalah dalam mengidentifikasi disk ini saat Anda mengkonfigurasinya di konsol gateway.

Untuk mengonfigurasi VM Anda untuk menggunakan pengontrol paravirtualisasi

1. Di klien VMware vSphere, buka menu konteks (klik kanan) untuk VM gateway Anda, lalu pilih Edit Pengaturan.
2. Di kotak dialog Virtual Machine Properties, pilih tab Hardware, pilih SCSI controller 0, lalu pilih Change Type.



3. Dalam kotak dialog Ubah Jenis Pengontrol SCSI, pilih jenis pengontrol SCSI Paravirtual VMware, lalu pilih OK.



Menggunakan Storage Gateway dengan VMware Ketersediaan Tinggi

VMware High Availability (HA) adalah komponen dari vSphere yang dapat memberikan perlindungan dari kegagalan pada lapisan infrastruktur yang mendukung gateway VM. VMware HA melakukan ini dengan menggunakan beberapa host yang dikonfigurasi sebagai cluster sehingga jika host yang menjalankan gateway VM gagal, VM gateway dapat dimulai ulang secara otomatis pada host lain di

dalam cluster. Untuk informasi lebih lanjut tentang VMware HA, lihat [VMware HA: Konsep dan Praktik Terbaik](#) di situs web VMware.

Untuk menggunakan Storage Gateway dengan VMware HA, sebaiknya lakukan hal-hal berikut:

- Menyebarkan paket .ova download VMware ESX yang berisi VM Storage Gateway hanya pada satu host dalam sebuah cluster.
- Saat menerapkan .ova paket, pilih penyimpanan data yang tidak lokal ke satu host. Sebagai gantinya, gunakan penyimpanan data yang dapat diakses oleh semua host di cluster. Jika Anda memilih penyimpanan data yang lokal ke host dan host gagal, maka sumber data mungkin tidak dapat diakses oleh host lain di cluster dan failover ke host lain mungkin tidak berhasil.
- Untuk mencegah inisiator Anda terputus dari target volume penyimpanan selama failover, ikuti pengaturan iSCSI yang disarankan untuk sistem operasi Anda. Dalam peristiwa failover, dibutuhkan beberapa detik hingga beberapa menit agar VM gateway dimulai di host baru di cluster failover. Batas waktu iSCSI yang disarankan untuk klien Windows dan Linux lebih besar daripada waktu yang diperlukan untuk failover terjadi. Untuk informasi selengkapnya tentang menyesuaikan pengaturan batas waktu klien Windows, lihat [Menyesuaikan Pengaturan Windows iSCSI Anda](#). Untuk informasi selengkapnya tentang menyesuaikan pengaturan batas waktu klien Linux, lihat [Menyesuaikan Pengaturan iSCSI Linux Anda](#).
- Dengan pengelompokan, jika Anda menerapkan .ova paket ke cluster, pilih host saat Anda diminta untuk melakukannya. Sebagai alternatif, Anda dapat menerapkan langsung ke host di cluster.

Menyinkronkan Waktu VM Gateway Anda

Untuk gateway yang digunakan pada VMware ESXi, mengatur waktu host hypervisor dan menyinkronkan waktu VM ke host sudah cukup untuk menghindari penyimpangan waktu. Untuk informasi selengkapnya, lihat [Sinkronisasi Waktu VM dengan Waktu Host](#). Untuk gateway yang digunakan di Microsoft Hyper-V, Anda harus memeriksa waktu VM Anda secara berkala menggunakan prosedur yang dijelaskan berikut.

Untuk melihat dan menyinkronkan waktu VM gateway hypervisor ke server Network Time Protocol (NTP)

1. Masuk ke konsol lokal gateway Anda:

- Untuk informasi selengkapnya tentang masuk ke konsol lokal VMware ESXi, lihat. [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
 - Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
 - Untuk informasi selengkapnya tentang masuk ke konsol lokal untuk Linux Kernel-based Virtuam Machine (KVM), lihat. [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)
2. Pada menu utama Storage Gateway Configuration, masukkan **4** untuk System Time Management.

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

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

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

3. Pada menu Manajemen Waktu Sistem, masukkan **1** untuk Lihat dan Sinkronisasi Waktu Sistem.

```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: _
```

4. Jika hasilnya menunjukkan bahwa Anda harus menyinkronkan waktu VM Anda ke waktu NTP, masukkan. **y** Jika tidak, masukkan.

Jika Anda masuk **y** untuk menyinkronkan, sinkronisasi mungkin memakan waktu beberapa saat.

Tangkapan layar berikut menunjukkan VM yang tidak memerlukan sinkronisasi waktu.

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

Tangkapan layar berikut menunjukkan VM yang memang membutuhkan sinkronisasi waktu.

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

Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway

Anda dapat menerapkan dan mengaktifkan Tape Gateway Volume Gateway Amazon Elastic Compute Cloud (Amazon EC2). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai komunitas AMI.

Note

AMI komunitas Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.

Untuk menerapkan instans Amazon EC2 untuk meng-host Tape Gateway

1. Mulai menyiapkan gateway baru menggunakan konsol Storage Gateway. Untuk petunjuk, lihat [Mengatur Gateway Tape Mengatur Gerbang](#).
2. Pilih Launch instance untuk membuka template AWS Storage Gateway AMI di konsol Amazon EC2, tempat Anda dapat mengonfigurasi pengaturan tambahan.

Gunakan Quicklaunch untuk meluncurkan instans Amazon EC2 dengan pengaturan default. Untuk informasi selengkapnya tentang spesifikasi default Amazon EC2 Quicklaunch, lihat [Spesifikasi Konfigurasi Quicklaunch](#) untuk Amazon EC2.

3. Untuk Nama, masukkan nama untuk instans Amazon EC2. Setelah instance di-deploy, Anda dapat mencari nama ini untuk menemukan instance Anda di halaman daftar di konsol Amazon EC2.
4. Di bagian Jenis instans, untuk tipe Instance, pilih konfigurasi perangkat keras untuk instans Anda. Konfigurasi perangkat keras harus memenuhi persyaratan minimum tertentu untuk mendukung gateway Anda. Sebaiknya mulai dengan tipe instans m5.xlarge, yang memenuhi persyaratan perangkat keras minimum agar gateway Anda berfungsi dengan baik. Untuk informasi selengkapnya, lihat [Persyaratan untuk jenis instans Amazon EC2](#).


Anda dapat mengubah ukuran instans Anda setelah meluncurkan, jika perlu. Untuk informasi selengkapnya, lihat [Mengubah ukuran instans Anda](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Note

Jenis instans tertentu, terutama i3 EC2, menggunakan disk SSD NVMe. Ini dapat menyebabkan masalah ketika Anda memulai atau menghentikan Tape Gateway; misalnya, Anda dapat kehilangan data dari cache. Pantau CloudWatch metrik CachePercentDirty Amazon, dan hanya mulai atau hentikan sistem Anda saat parameter itu0. Untuk mempelajari selengkapnya tentang memantau metrik untuk

gateway Anda, lihat [Metrik dan dimensi Storage Gateway](#) dalam dokumentasi CloudWatch

5. Di bagian Key pair (login), untuk Key pair name - required, pilih key pair yang ingin Anda gunakan untuk terhubung dengan aman ke instance Anda. Anda dapat membuat key pair baru jika perlu. Untuk informasi selengkapnya, lihat [Membuat key pair](#) di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.
6. Di bagian Pengaturan jaringan, tinjau pengaturan yang telah dikonfigurasi sebelumnya dan pilih Edit untuk membuat perubahan pada bidang berikut:
 - a. Untuk VPC - diperlukan, pilih VPC tempat Anda ingin meluncurkan instans Amazon EC2 Anda. Untuk informasi selengkapnya, lihat [Cara kerja Amazon VPC](#) di Panduan Pengguna Amazon Virtual Private Cloud.
 - b. (Opsional) Untuk Subnet, pilih subnet tempat Anda ingin meluncurkan instans Amazon EC2 Anda.
 - c. Untuk Tetapkan Otomatis IP Publik, pilih Aktifkan.
7. Di subbagian Firewall (grup keamanan), tinjau pengaturan yang telah dikonfigurasi sebelumnya. Anda dapat mengubah nama default dan deskripsi grup keamanan baru yang akan dibuat untuk instans Amazon EC2 Anda jika Anda mau, atau memilih untuk menerapkan aturan firewall dari grup keamanan yang ada.
8. Dalam subbagian aturan grup keamanan masuk, tambahkan aturan firewall untuk membuka port yang akan digunakan klien untuk terhubung ke instans Anda. Untuk informasi selengkapnya tentang port yang diperlukan untuk Tape Gateway, lihat [Persyaratan port](#). Untuk informasi selengkapnya tentang menambahkan aturan firewall, lihat [Aturan grup keamanan](#) di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

 Note

Tape Gateway mengharuskan port TCP 80 terbuka untuk lalu lintas masuk dan untuk akses HTTP satu kali selama aktivasi gateway. Setelah aktivasi, Anda dapat menutup port ini.

Selain itu, Anda harus membuka port TCP 3260 untuk akses iSCSI.

9. Di subbagian Konfigurasi jaringan lanjutan, tinjau pengaturan yang telah dikonfigurasi sebelumnya dan buat perubahan jika perlu.

10. Di bagian Konfigurasi penyimpanan, pilih Tambahkan volume baru untuk menambahkan penyimpanan ke instance gateway Anda.

 Important

Anda harus menambahkan setidaknya satu volume Amazon EBS dengan setidaknya 165 GiB kapasitas untuk penyimpanan cache, dan setidaknya satu volume Amazon EBS dengan setidaknya 150 GiB kapasitas untuk upload buffer, selain volume Root yang telah dikonfigurasi sebelumnya. Untuk meningkatkan kinerja, kami sarankan mengalokasikan beberapa volume EBS untuk penyimpanan cache dengan masing-masing setidaknya 150 GiB.

11. Di bagian Detail lanjutan, tinjau pengaturan yang telah dikonfigurasi sebelumnya dan buat perubahan jika perlu.
12. Pilih Luncurkan instans untuk meluncurkan instans gateway Amazon EC2 baru Anda dengan pengaturan yang dikonfigurasi.
13. Untuk memverifikasi bahwa instans baru berhasil diluncurkan, buka halaman Instans di konsol Amazon EC2 dan cari instans baru berdasarkan nama. Pastikan bahwa status Instance menampilkan Berjalan dengan tanda centang hijau, dan pemeriksaan Status selesai, dan menunjukkan tanda centang hijau.
14. Pilih contoh Anda dari halaman detail. Salin alamat IPv4 Publik dari bagian ringkasan Instans, lalu kembali ke halaman Pengaturan gateway di konsol Storage Gateway untuk melanjutkan pengaturan Gateway Gateway Tape Anda.

Anda dapat menentukan ID AMI yang akan digunakan untuk meluncurkan Gateway Gateway Tape dengan menggunakan konsol Storage Gateway atau dengan menanyakan penyimpanan AWS Systems Manager parameter.

Untuk menentukan ID AMI, lakukan salah satu hal berikut:

- Mulai menyiapkan gateway baru menggunakan konsol Storage Gateway. Untuk petunjuk, lihat [Mengatur Gateway Tape Mengatur Gerbang](#) . Saat Anda mencapai bagian Opsi platform, pilih Amazon EC2 sebagai platform Host, lalu pilih Launch instance untuk membuka template AWS Storage Gateway AMI di konsol Amazon EC2.

Anda diarahkan ke halaman AMI komunitas EC2, di mana Anda dapat melihat ID AMI untuk AWS Wilayah Anda di URL.

- Kueri penyimpanan parameter Systems Manager. Anda dapat menggunakan AWS CLI atau Storage Gateway API untuk menanyakan parameter publik Systems Manager di bawah namespace/`aws/service/storagegateway/ami/VTL/latest`. Misalnya, menggunakan perintah CLI berikut mengembalikan ID AMI saat ini di yang Wilayah AWS Anda tentukan.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/latest
```

Perintah CLI mengembalikan output yang mirip dengan berikut ini.

```
{
  "Parameter": {
    "Type": "String",
    "LastModifiedDate": 1561054105.083,
    "Version": 4,
    "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/VTL/latest",
    "Name": "/aws/service/storagegateway/ami/VTL/latest",
    "Value": "ami-123c45dd67d891000"
  }
}
```

Menerapkan Amazon EC2 dengan Pengaturan Default

Topik ini mencantumkan langkah-langkah untuk menerapkan host Amazon EC2 menggunakan spesifikasi default.

Anda dapat menerapkan dan mengaktifkan Tape Gateway Volume Gateway Amazon Elastic Compute Cloud (Amazon EC2). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai AMI komunitas.

Note

AMI komunitas Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.

1. Untuk menyiapkan Amazon EC2Instance, pilih Amazon EC2 sebagai platform Host di bagian Opsi platform pada alur kerja. Untuk petunjuk cara mengonfigurasi instans Amazon EC2, [lihat](#)

[Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway Menerapkan instans Amazon EC2 untuk meng-host Anda.](#)

2. Pilih Launch instance untuk membuka template AWS Storage Gateway AMI di konsol Amazon EC2 dan sesuaikan pengaturan tambahan seperti tipe Instans, Pengaturan jaringan, dan Konfigurasi penyimpanan.
3. Secara opsional, Anda dapat memilih Gunakan pengaturan default di konsol Storage Gateway untuk menerapkan instans Amazon EC2 dengan konfigurasi default.

Instans Amazon EC2 yang dibuat oleh Use default settings memiliki spesifikasi default berikut:

- Jenis contoh - m5.xlarge
- Pengaturan Jaringan
 - Untuk VPC, pilih VPC yang Anda inginkan untuk menjalankan instans EC2 Anda.
 - Untuk Subnet, tentukan subnet tempat instans EC2 Anda harus diluncurkan.

Note

Subnet VPC akan muncul di drop-down hanya jika mereka mengaktifkan pengaturan alamat IPv4 publik yang ditetapkan secara otomatis dari konsol manajemen VPC.

- Tetapkan IP Publik secara otomatis - Diaktifkan

Grup keamanan EC2 dibuat dan dikaitkan dengan instans EC2. Grup keamanan memiliki aturan port masuk berikut:

Note

Anda akan membutuhkan Port 80 terbuka selama aktivasi gateway. Port ditutup segera setelah aktivasi. Setelah itu, instans EC2 Anda hanya dapat diakses melalui port lain dari VPC yang dipilih.

Target iSCSI di gateway Anda hanya dapat diakses dari host di VPC yang sama dengan gateway. Jika target iSCSI perlu diakses dari host di luar VPC, Anda harus memperbarui aturan grup keamanan yang sesuai.

Anda dapat mengedit grup keamanan kapan saja dengan menavigasi ke halaman detail instans Amazon EC2, memilih Keamanan, menavigasi ke detail grup Keamanan, dan memilih ID grup keamanan.

Port	Protokol	Protokol Sistem File				
80	TCP	Akses HTTP untuk aktivasi				
3260	TCP	iSCSI				

- Konfigurasi penyimpanan

Pengaturan Default	Volume Akar AMI	Volume 2 Cache	Volume 3 Cache			
Nama perangkat		'/dev/sdb'	'/dev/sdc'			
Ukuran	80 Gib	165 GiB	150 GiB			
Jenis Volume	gp3	gp3	gp3			
IOPS	3000	3000	3000			
Hapus saat penghentian	Ya	Ya	Ya			
Dienkripsi	Tidak	Tidak	Tidak			
Throughput	125	125	125			

Ubah opsi metadata instans Amazon EC2

Layanan metadata instance (IMDS) adalah komponen on-instance yang menyediakan akses aman ke metadata instans Amazon EC2. Sebuah instance dapat dikonfigurasi untuk menerima permintaan metadata masuk yang menggunakan IMDS Versi 1 (IMDSv1) atau mengharuskan semua permintaan metadata menggunakan IMDS Versi 2 (IMDSv2). IMDSv2 menggunakan permintaan berorientasi sesi dan mengurangi beberapa jenis kerentanan yang dapat digunakan untuk mencoba mengakses IMDS. Untuk informasi tentang IMDSv2, lihat [Cara Kerja Layanan Metadata Instans Versi 2 di Panduan Pengguna Amazon Elastic Compute Cloud](#).

Sebaiknya Anda memerlukan IMDSv2 untuk semua instans Amazon EC2 yang menghosting Storage Gateway. IMDSv2 diperlukan secara default pada semua instance gateway yang baru diluncurkan. Jika Anda memiliki instans yang masih dikonfigurasi untuk menerima permintaan metadata IMDSv1, lihat [Memerlukan penggunaan IMDSv2 di Panduan Pengguna Amazon Elastic Compute Cloud](#) untuk petunjuk mengubah opsi metadata instans Anda agar memerlukan penggunaan IMDSv2. Menerapkan perubahan ini tidak memerlukan reboot instance.

Gerbang Pita

Topik

- [Menghapus Disk dari Gateway Anda](#)
- [Menambahkan dan Menghapus Volume Amazon EBS untuk Gateway Anda yang Dihosting di Amazon EC2](#)
- [Bekerja dengan Perangkat VTL](#)
- [Bekerja Dengan Kaset](#)

Menghapus Disk dari Gateway Anda

Meskipun kami tidak menyarankan untuk menghapus disk yang mendasarinya dari gateway Anda, Anda mungkin ingin menghapus disk dari gateway Anda, misalnya jika Anda memiliki disk yang gagal.

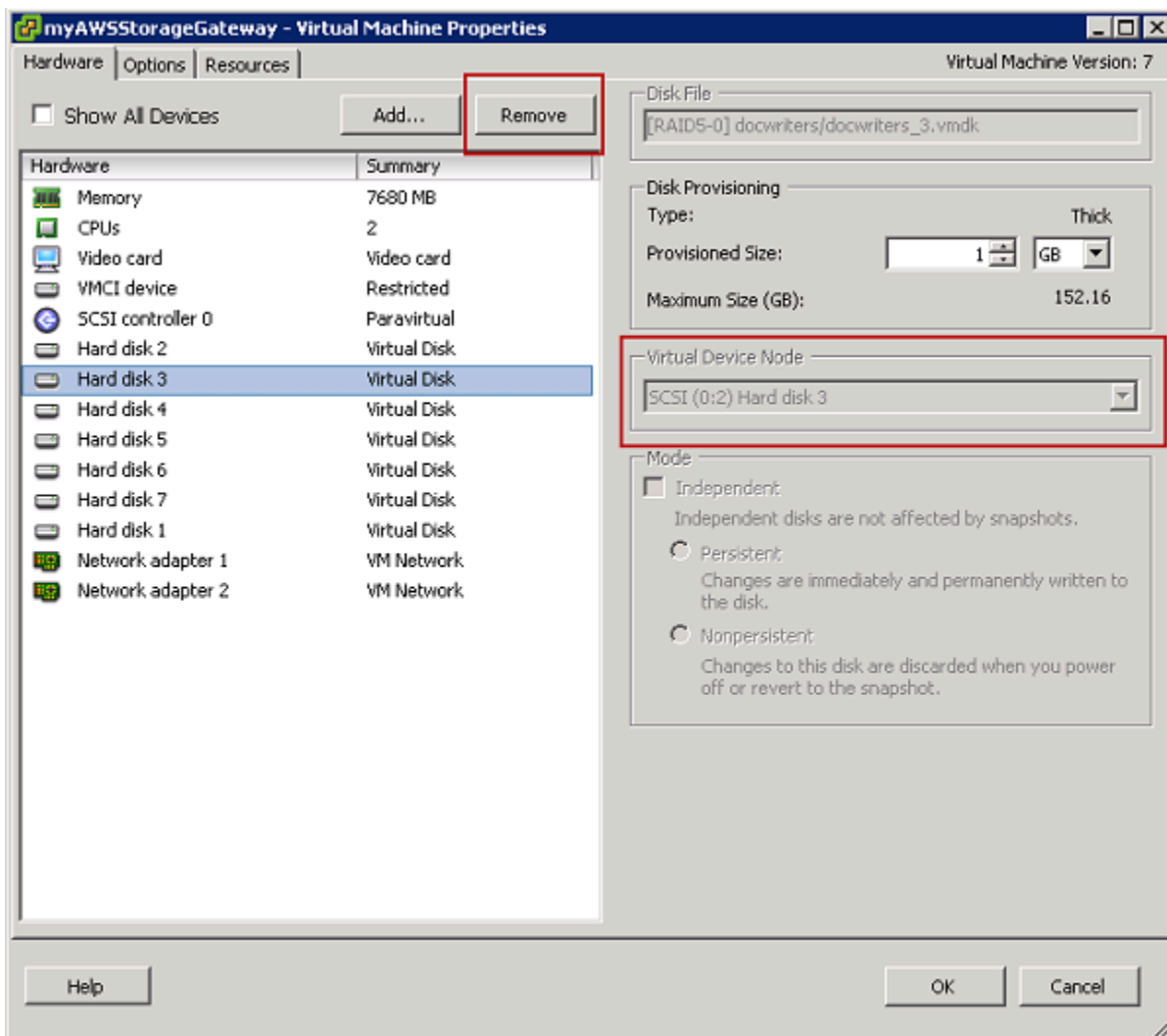
Menghapus Disk dari Gateway yang Dihosting di VMware ESXi

Anda dapat menggunakan prosedur berikut untuk menghapus disk dari gateway Anda yang dihosting di hypervisor VMware.

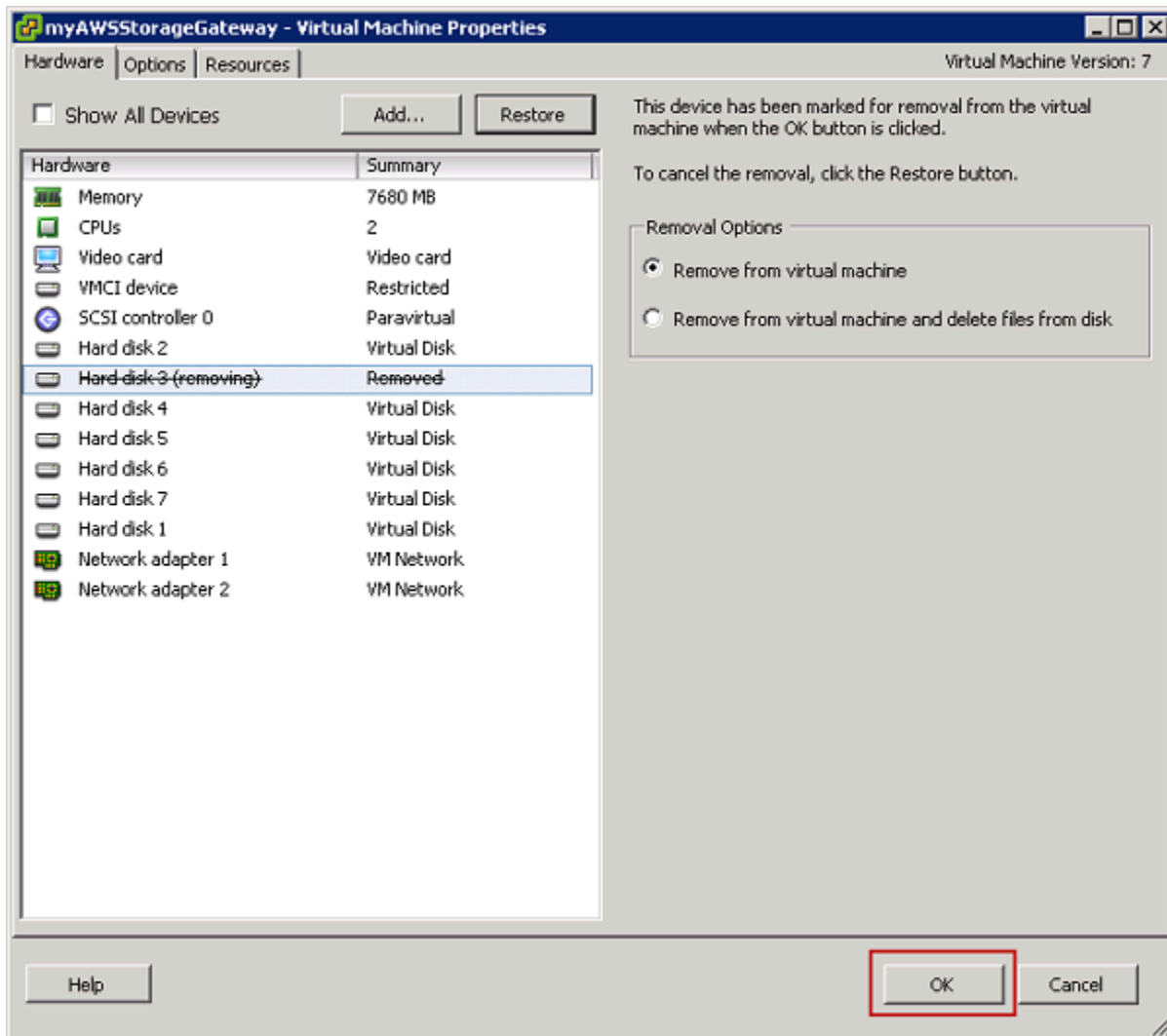
Untuk menghapus disk yang dialokasikan untuk buffer unggah (VMware ESXi)

1. Di klien vSphere, buka menu konteks (klik kanan), pilih nama VM gateway Anda, lalu pilih Edit Pengaturan.
2. Pada tab Hardware pada kotak dialog Properti Mesin Virtual, pilih disk yang dialokasikan sebagai ruang buffer unggah, lalu pilih Hapus.

Verifikasi bahwa nilai Virtual Device Node di kotak dialog Virtual Machine Properties memiliki nilai yang sama dengan yang Anda catat sebelumnya. Melakukan hal ini membantu memastikan bahwa Anda menghapus disk yang benar.



3. Pilih opsi di panel Opsi Penghapusan, lalu pilih OK untuk menyelesaikan proses menghapus disk.



Menghapus Disk dari Gateway yang Dihosting di Microsoft Hyper-V

Dengan menggunakan prosedur berikut, Anda dapat menghapus disk dari gateway yang dihosting di hypervisor Microsoft Hyper-V.

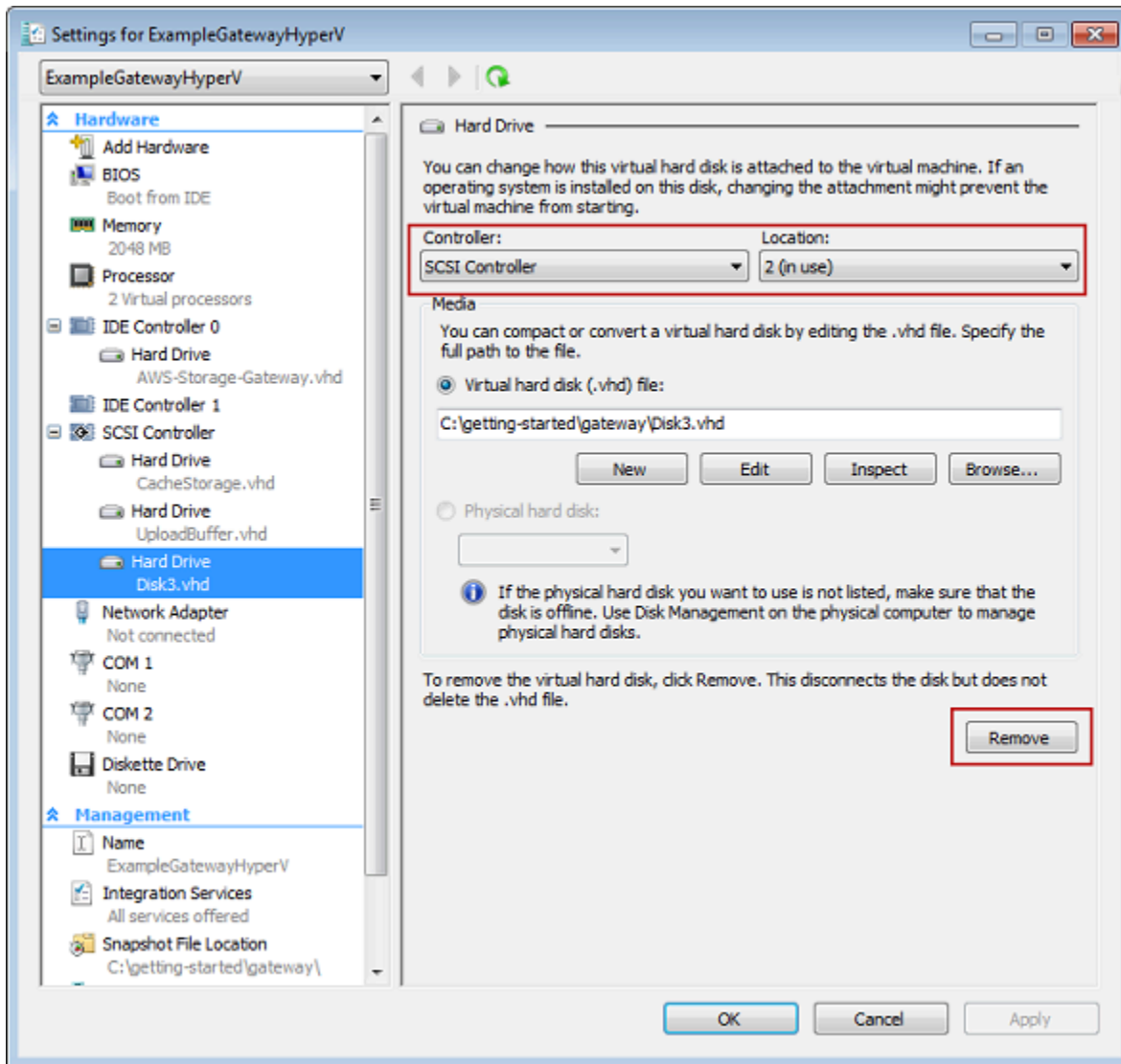
Untuk menghapus disk dasar yang dialokasikan untuk buffer upload (Microsoft Hyper-V)

1. Di Microsoft Hyper-V Manager, buka menu konteks (klik kanan), pilih nama gateway VM Anda, lalu pilih Pengaturan.
2. Dalam daftar perangkat keras kotak dialog Pengaturan, pilih disk yang akan dihapus, lalu pilih Hapus.

Disk yang Anda tambahkan ke gateway muncul di bawah entri SCSI Controller dalam daftar Hardware. Verifikasi bahwa nilai Controller dan Location adalah nilai yang sama dengan yang

Anda catat sebelumnya. Melakukan hal ini membantu memastikan bahwa Anda menghapus disk yang benar.

Pengontrol SCSI pertama yang ditampilkan di Microsoft Hyper-V Manager adalah controller 0.



3. Pilih OK untuk menerapkan perubahan.

Menghapus Disk dari Gateway yang Dihosting di Linux KVM

Untuk melepaskan disk dari gateway Anda yang dihosting di hypervisor Linux Kernel-based Virtual Machine (KVM), Anda dapat menggunakan perintah yang mirip dengan yang `virsh` berikut ini.

```
$ virsh detach-disk domain_name /device/path
```

Untuk detail selengkapnya tentang mengelola disk KVM, lihat dokumentasi distribusi Linux Anda.

Menambahkan dan Menghapus Volume Amazon EBS untuk Gateway Anda yang Dihosting di Amazon EC2

Saat pertama kali mengonfigurasi gateway untuk dijalankan sebagai instans Amazon EC2, Anda mengalokasikan volume Amazon EBS untuk digunakan sebagai buffer unggahan dan penyimpanan cache. Seiring waktu, karena aplikasi Anda perlu berubah, Anda dapat mengalokasikan volume Amazon EBS tambahan untuk penggunaan ini. Anda juga dapat mengurangi penyimpanan yang dialokasikan dengan menghapus volume Amazon EBS yang dialokasikan sebelumnya. Untuk informasi selengkapnya tentang Amazon EBS, lihat [Amazon Elastic Block Store \(Amazon EBS\) di Panduan Pengguna](#) Amazon EC2 untuk Instans Linux.

Sebelum menambahkan lebih banyak penyimpanan ke gateway, Anda harus meninjau cara mengukur buffer unggahan dan penyimpanan cache berdasarkan kebutuhan aplikasi Anda untuk gateway. Untuk melakukannya, lihat [Menentukan ukuran buffer unggahan yang akan dialokasikan](#) dan [Menentukan ukuran penyimpanan cache yang akan dialokasikan](#).

Ada kuota pada penyimpanan maksimum yang dapat Anda alokasikan sebagai buffer unggahan dan penyimpanan cache. Anda dapat melampirkan volume Amazon EBS sebanyak yang Anda inginkan, tetapi Anda hanya dapat mengonfigurasi volume ini sebagai buffer unggah dan ruang penyimpanan cache hingga kuota penyimpanan ini. Untuk informasi selengkapnya, lihat [AWS Storage Gateway kuota](#).

Untuk menambahkan volume Amazon EBS dan mengonfigurasinya untuk gateway Anda

1. Buat volume Amazon EBS. Untuk petunjuk, lihat [Membuat atau Memulihkan Volume Amazon EBS](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.
2. Lampirkan volume Amazon EBS ke instans Amazon EC2 Anda. Untuk petunjuk, lihat [Melampirkan Volume Amazon EBS ke Instans](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.
3. Konfigurasi volume Amazon EBS yang Anda tambahkan sebagai buffer unggahan atau penyimpanan cache. Untuk petunjuk, lihat [Mengelola disk lokal untuk Storage Gateway Anda](#).

Ada kalanya Anda mungkin menemukan bahwa Anda tidak memerlukan jumlah penyimpanan yang Anda alokasikan untuk buffer unggahan.

Untuk menghapus volume Amazon EBS

Warning

Langkah-langkah ini hanya berlaku untuk volume Amazon EBS yang dialokasikan sebagai ruang buffer unggah, bukan untuk volume yang dialokasikan ke cache. Jika Anda menghapus volume Amazon EBS yang dialokasikan sebagai penyimpanan cache dari Tape Gateway, kaset virtual pada gateway akan memiliki status IRRECOVERABLE, dan Anda berisiko kehilangan data. Untuk informasi selengkapnya tentang status IRRECOVERABLE, lihat [Memahami Informasi Status Tape dalam VTL](#)

1. Matikan gateway dengan mengikuti pendekatan yang dijelaskan di [Mematikan VM Gateway Anda](#) bagian.
2. Lepaskan volume Amazon EBS dari instans Amazon EC2 Anda. Untuk petunjuknya, lihat [Melepaskan Volume Amazon EBS dari Instans](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.
3. Hapus volume Amazon EBS. Untuk petunjuk, lihat [Menghapus Volume Amazon EBS](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.
4. Mulai gateway dengan mengikuti pendekatan yang dijelaskan di [Mematikan VM Gateway Anda](#) bagian.

Bekerja dengan Perangkat VTL

Pengaturan Tape Gateway Anda menyediakan perangkat SCSI berikut, yang Anda pilih saat mengaktifkan gateway Anda.

Topik

- [Memilih Medium Changer Setelah Aktivasi Gateway](#)
- [Memperbarui Driver Perangkat untuk Pengubah Medium Anda](#)
- [Menampilkan Barcode untuk Kaset di Microsoft System Center DPM](#)


Untuk medium changer, AWS Storage Gateway bekerja dengan yang berikut:

- AWS-Gateway-VTL — Perangkat ini dilengkapi dengan gateway.
- STK-L700 - Emulasi perangkat ini dilengkapi dengan gateway.

Saat mengaktifkan Tape Gateway, Anda memilih aplikasi cadangan dari daftar dan Storage Gateway menggunakan medium changer yang sesuai. Jika aplikasi backup Anda tidak terdaftar, Anda memilih Other dan kemudian memilih medium changer yang bekerja dengan aplikasi backup.

Jenis medium changer yang Anda pilih tergantung pada aplikasi cadangan yang Anda rencanakan untuk digunakan. Tabel berikut mencantumkan aplikasi cadangan pihak ketiga yang telah diuji dan ditemukan kompatibel dengan Tape Gateways. Tabel ini mencakup tipe medium changer yang direkomendasikan untuk setiap aplikasi backup.

Aplikasi Backup	Jenis Pengubah Sedang
Cadangan Arcserve	AWS-Gateway-VTL
Bacula Perusahaan V10.x	AWS-Gateway-VTL atau STK-L700
Commvault V11	STK-L700
Dell EMC 19,5 NetWorker	AWS-Gateway-VTL
IBM Spectrum Melindungi v8.1.10	IBM-03584L32-0402
Pelindung Data Fokus Mikro (HPE) 9 atau 11.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 atau 2016 Manajer Perlindungan Data	STK-L700
NovaStor DataCenter/Jaringan 6.4 atau 7.1	STK-L700
NetVault Cadangan Quest 12.4 atau 13.x	STK-L700
Cadangan & Replikasi Veeam 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014 atau 15 atau 16 atau 20 atau 22.x	AWS-Gateway-VTL

Aplikasi Backup	Jenis Pengubah Sedang
Eksekutif Cadangan Veritas 2012 <div data-bbox="147 304 808 527" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note Veritas telah mengakhiri dukungan untuk Backup Exec 2012.</p> </div>	STK-L700
Veritas NetBackup Versi 7.x atau 8.x	AWS-Gateway-VTL

Important

Kami sangat menyarankan Anda memilih medium changer yang terdaftar untuk aplikasi backup Anda. Pengubah media lainnya mungkin tidak berfungsi dengan baik. Anda dapat memilih medium changer yang berbeda setelah gateway diaktifkan. Untuk informasi selengkapnya, lihat [Memilih Pengubah Medium Setelah Aktivasi Gateway](#).

Untuk tape drive, Storage Gateway bekerja dengan yang berikut:

- IBM-ULT3580-TD5 — Emulasi perangkat ini dilengkapi dengan gateway.

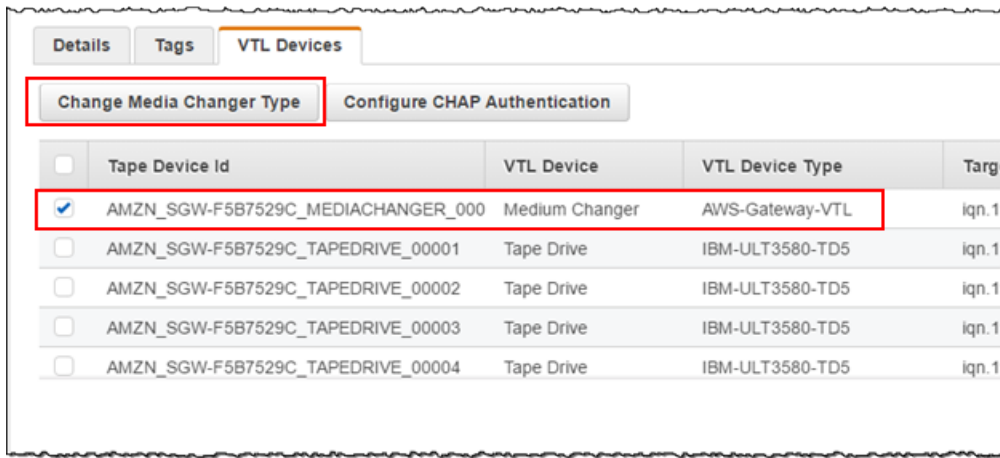
Memilih Medium Changer Setelah Aktivasi Gateway

Setelah gateway Anda diaktifkan, Anda dapat memilih untuk memilih jenis medium changer yang berbeda.

Untuk memilih jenis medium changer yang berbeda setelah aktivasi gateway

1. Hentikan pekerjaan terkait yang berjalan di perangkat lunak cadangan Anda.
2. Di server Windows, buka jendela properti inisiator iSCSI.
3. Pilih tab Target untuk menampilkan target yang ditemukan.
4. Pada panel Target yang ditemukan, pilih medium changer yang ingin diubah, pilih Putuskan sambungan, lalu pilih OK.

5. Pada konsol Storage Gateway, pilih Gateways dari panel navigasi, lalu pilih gateway yang medium changer ingin Anda ubah.
6. Pilih tab Perangkat VTL, pilih pengubah media yang ingin Anda ubah, lalu pilih Ubah Pengubah Media.



7. Dalam kotak dialog Ubah Jenis Pengubah Media yang muncul, pilih pengubah media yang Anda inginkan dari kotak daftar drop-down lalu pilih Simpan.

Memperbarui Driver Perangkat untuk Pengubah Medium Anda

1. Buka Device Manager di server Windows Anda, dan perluas pohon perangkat Medium Changer.
2. Buka menu konteks (klik kanan) untuk Unknown Medium Changer, dan pilih Update Driver Software untuk membuka jendela Update Driver Software-Unknown Medium Changer.
3. Dalam Bagaimana Anda ingin mencari perangkat lunak driver? bagian, pilih Jelajahi komputer saya untuk perangkat lunak driver.
4. Pilih Biarkan saya memilih dari daftar driver perangkat di komputer saya.

Note

Sebaiknya gunakan driver Autoloader Sony TSL-A500C dengan perangkat lunak cadangan Veeam Backup & Replication 11A dan Microsoft System Center Data Protection Manager. Driver Sony ini telah diuji dengan jenis perangkat lunak cadangan ini hingga dan termasuk Windows Server 2019.

5. Di bagian Pilih driver perangkat yang ingin Anda instal untuk perangkat keras ini, kosongkan kotak centang Tampilkan perangkat keras yang kompatibel, pilih Sony di daftar Produsen, pilih Sony - TSL-A500C Autoloader di daftar Model, lalu pilih Berikutnya.

6. Di kotak peringatan yang muncul, pilih Ya. Jika driver berhasil diinstal, tutup jendela Perbarui perangkat lunak drive.

Menampilkan Barcode untuk Kaset di Microsoft System Center DPM

Jika Anda menggunakan driver media changer untuk Sony TSL-A500C Autoloader, Microsoft System Center Data Protection Manager tidak secara otomatis menampilkan barcode untuk kaset virtual yang dibuat di Storage Gateway. Untuk menampilkan barcode dengan benar untuk kaset Anda, ubah driver media changer ke Sun/ Library. StorageTek

Untuk menampilkan barcode

1. Pastikan bahwa semua pekerjaan cadangan telah selesai dan tidak ada tugas yang tertunda atau sedang berlangsung.
2. Keluarkan dan pindahkan kaset ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive) dan keluar dari konsol Administrator DPM. Untuk informasi tentang cara mengeluarkan kaset di DPM, lihat. [Mengarsipkan Tape dengan Menggunakan DPM](#)
3. Di Alat Administratif, pilih Layanan dan buka menu konteks (klik kanan) untuk Layanan DPM di panel Detail, lalu pilih Properti.
4. Pada tab General, pastikan bahwa jenis Startup diatur ke Otomatis dan pilih Stop untuk menghentikan layanan DPM.
5. Dapatkan StorageTek driver dari [Katalog Pembaruan Microsoft](#) di situs web Microsoft.

Note

Perhatikan driver yang berbeda untuk ukuran yang berbeda.

Untuk Ukuran 18K, pilih driver x86.

Untuk Ukuran 19K, pilih driver x64.

6. Di server Windows Anda, buka Device Manager, dan perluas pohon Medium Changer Devices.
7. Buka menu konteks (klik kanan) untuk Unknown Medium Changer, dan pilih Update Driver Software untuk membuka jendela Update Driver Software-Unknown Medium Changer.
8. Jelajahi jalur lokasi driver baru dan instal. Pengemudi muncul sebagai StorageTek Sun/Library. Drive tape tetap sebagai perangkat sekuensial IBM ULT3580-TD5 SCSI.

9. Reboot server DPM.
10. Di konsol Storage Gateway, buat kaset baru.
11. Buka konsol Administrator DPM, pilih Manajemen, lalu pilih Rescan untuk pustaka rekaman baru. Anda harus melihat StorageTek Sun/perpustakaan.
12. Pilih perpustakaan dan pilih Inventaris.
13. Pilih Tambahkan Kaset untuk menambahkan kaset baru ke DPM. Kaset baru sekarang harus menampilkan barcode mereka.

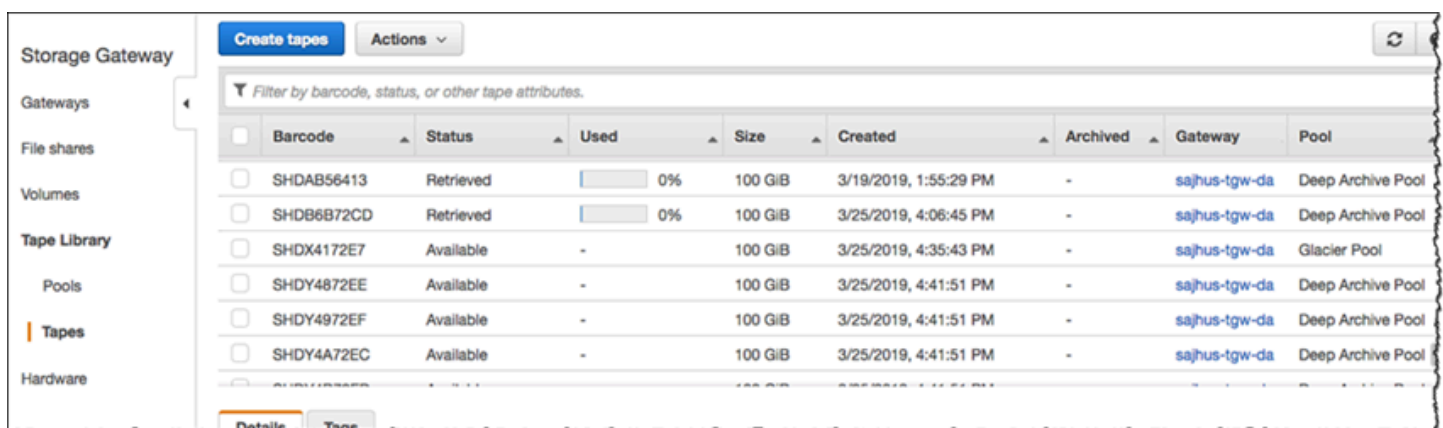
Bekerja Dengan Kaset

Storage Gateway menyediakan satu pustaka pita virtual (VTL) untuk setiap Tape Gateway yang Anda aktifkan. Awalnya, perpustakaan tidak berisi kaset, tetapi Anda dapat membuat kaset kapan pun Anda perlu. Aplikasi Anda dapat membaca dan menulis ke kaset apa pun yang tersedia di Tape Gateway Anda. Status rekaman harus TERSEDIA bagi Anda untuk menulis ke rekaman itu. Kaset ini didukung oleh Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) —yaitu, saat Anda menulis ke kaset ini, Tape Gateway menyimpan data di Amazon S3. Untuk informasi selengkapnya, lihat [Memahami Informasi Status Tape dalam VTL](#).

Topik

- [Kaset Pengarsipan](#)
- [Membatalkan Arsip Pita](#)

Pustaka rekaman menunjukkan kaset di Tape Gateway Anda. Pustaka menunjukkan kode batang pita, status, dan ukuran, jumlah pita yang digunakan, dan gerbang yang terkait dengan rekaman itu.



	Barcode	Status	Used	Size	Created	Archived	Gateway	Pool
<input type="checkbox"/>	SHDAB56413	Retrieved	0%	100 GiB	3/19/2019, 1:55:29 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDB6B72CD	Retrieved	0%	100 GiB	3/25/2019, 4:06:45 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDX4172E7	Available	-	100 GiB	3/25/2019, 4:35:43 PM	-	sajhus-tgw-da	Glacier Pool
<input type="checkbox"/>	SHDY4872EE	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDY4972EF	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDY4A72EC	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive Pool

Ketika Anda memiliki sejumlah besar kaset di perpustakaan, konsol mendukung pencarian kaset berdasarkan kode batang, berdasarkan status, atau keduanya. Saat Anda mencari berdasarkan kode batang, Anda dapat memfilter berdasarkan status dan gateway.

Untuk mencari berdasarkan barcode, status, dan gateway

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih Kaset, lalu ketik nilai di kotak pencarian. Nilainya bisa berupa barcode, status, atau gateway. Secara default, Storage Gateway mencari semua kaset virtual. Namun, Anda juga dapat memfilter pencarian Anda berdasarkan status.

Jika Anda memfilter status, kaset yang cocok dengan kriteria akan muncul di pustaka di konsol Storage Gateway.

Jika Anda memfilter gateway, kaset yang terkait dengan gateway tersebut akan muncul di pustaka di konsol Storage Gateway.

Note

Secara default, Storage Gateway menampilkan semua kaset terlepas dari statusnya.

Kaset Pengarsipan

Anda dapat mengarsipkan kaset virtual yang ada di Tape Gateway Anda. Saat Anda mengarsipkan kaset, Storage Gateway memindahkan rekaman ke arsip.

Untuk mengarsipkan kaset, Anda menggunakan perangkat lunak cadangan Anda. Proses arsip tape terdiri dari tiga tahap, dilihat sebagai status tape IN TRANSIT TO VTS, ARCHIVING, dan ARCHIVED:

- Untuk mengarsipkan kaset, gunakan perintah yang disediakan oleh aplikasi cadangan Anda. Ketika proses pengarsipan dimulai, status rekaman berubah menjadi IN TRANSIT TO VTS dan rekaman itu tidak lagi dapat diakses oleh aplikasi cadangan Anda. Pada tahap ini, Tape Gateway Anda mengunggah data ke AWS. Jika perlu, Anda dapat membatalkan arsip yang sedang berlangsung. Untuk informasi selengkapnya tentang membatalkan arsip, lihat. [Membatalkan Arsip Pita](#)

Note

Langkah-langkah untuk mengarsipkan kaset tergantung pada aplikasi cadangan Anda. Untuk petunjuk terperinci, lihat dokumentasi untuk aplikasi cadangan Anda.

- Setelah data upload AWS selesai, status tape berubah menjadi ARCHIVING dan Storage Gateway mulai memindahkan tape ke arsip. Anda tidak dapat membatalkan proses pengarsipan pada saat ini.
- Setelah rekaman dipindahkan ke arsip, statusnya berubah menjadi ARCHIVED dan Anda dapat mengambil rekaman ke salah satu gateway Anda. Untuk informasi selengkapnya tentang pengambilan rekaman, lihat [Mengambil Kaset yang Diarsipkan](#).

Langkah-langkah yang terlibat dalam pengarsipan kaset tergantung pada perangkat lunak cadangan Anda. Untuk petunjuk tentang cara mengarsipkan rekaman menggunakan NetBackup perangkat lunak Symantec, lihat [Mengarsipkan Tape](#).

Membatalkan Arsip Pita

Setelah Anda mulai mengarsipkan kaset, Anda mungkin memutuskan bahwa Anda membutuhkan kaset Anda kembali. Misalnya, Anda mungkin ingin membatalkan proses pengarsipan, mendapatkan rekaman kembali karena proses pengarsipan terlalu lama, atau membaca data dari rekaman itu. Rekaman yang sedang diarsipkan melewati tiga status, seperti yang ditunjukkan sebagai berikut:


- **DALAM TRANSIT KE VTS:** Tape Gateway Anda mengunggah data ke AWS
- **PENGARSIPAN:** Pengunggahan data selesai dan Tape Gateway memindahkan rekaman ke arsip.
- **DIARSIPKAN:** Rekaman dipindahkan dan arsip dan tersedia untuk pengambilan.

Anda dapat membatalkan arsip hanya ketika status rekaman dalam transit ke vts. Bergantung pada faktor-faktor seperti bandwidth upload dan jumlah data yang diunggah, status ini mungkin atau mungkin tidak terlihat di konsol Storage Gateway. Untuk membatalkan arsip rekaman, gunakan [CancelRetrieval](#) tindakan dalam referensi API.

Mendapatkan kunci aktivasi untuk gateway Anda

Untuk menerima kunci aktivasi untuk gateway Anda, buat permintaan web ke mesin virtual gateway (VM). VM mengembalikan pengalihan yang berisi kunci aktivasi, yang diteruskan sebagai salah satu


parameter untuk tindakan `ActivateGateway` API untuk menentukan konfigurasi gateway Anda. Untuk informasi selengkapnya, lihat [ActivateGateway](#) di Referensi API Storage Gateway.

 Note

Kunci aktivasi gateway kedaluwarsa dalam 30 menit jika tidak digunakan.

Permintaan yang Anda buat ke VM gateway mencakup AWS Wilayah tempat aktivasi terjadi. URL yang dikembalikan oleh pengalihan dalam respons berisi parameter string kueri yang disebut `activationkey`. Parameter string kueri ini adalah kunci aktivasi Anda. Format string kueri terlihat seperti berikut: `http://gateway_ip_address/?activationRegion=activation_region`. Output dari query ini mengembalikan kedua wilayah aktivasi dan kunci.

URL juga menyertakan `vpcEndpoint`, ID Titik Akhir VPC untuk gateway yang terhubung menggunakan tipe titik akhir VPC.

 Note

Storage Gateway Hardware Appliance, template gambar VM, dan Amazon EC2 Amazon Machine Images (AMI) telah dikonfigurasi sebelumnya dengan layanan HTTP yang diperlukan untuk menerima dan menanggapi permintaan web yang dijelaskan di halaman ini. Tidak diperlukan atau disarankan untuk menginstal layanan tambahan apa pun di gateway Anda.

Topik

- [Linux \(ikal\)](#)
- [Linux \(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)
- [Menggunakan konsol lokal Anda](#)

Linux (ikal)

Contoh berikut menunjukkan cara mendapatkan kunci aktivasi menggunakan Linux (curl).

Note

Ganti variabel yang disorot dengan nilai aktual untuk gateway Anda. Nilai yang dapat diterima adalah sebagai berikut:

- *gateway_ip_address* - Alamat IPv4 gateway Anda, misalnya 172.31.29.201
- *gateway_type* - Jenis gateway yang ingin Anda aktifkan, seperti,,, STOREDCACHED, VTL atau. FILE_S3 FILE_FSX_SMB
- *region_code* - Wilayah tempat Anda ingin mengaktifkan gateway Anda. Lihat [titik akhir Regional](#) di Panduan Referensi AWS Umum.
- *vpc_endpoint* - Nama titik akhir VPC untuk gateway Anda, misalnya. vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com

Untuk mendapatkan kunci aktivasi untuk titik akhir publik:

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

Untuk mendapatkan kunci aktivasi untuk titik akhir VPC:

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

Linux (bash/zsh)

Contoh berikut menunjukkan cara menggunakan Linux (bash/zsh) untuk mengambil respons HTTP, mengurai header HTTP, dan mendapatkan kunci aktivasi.

```
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

Contoh berikut menunjukkan cara menggunakan Microsoft Windows PowerShell untuk mengambil respons HTTP, mengurai header HTTP, dan mendapatkan kunci aktivasi.

```
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]
        }
    }
}
```

Menggunakan konsol lokal Anda

Contoh berikut menunjukkan cara menggunakan konsol lokal Anda untuk menghasilkan dan menampilkan kunci aktivasi.

Untuk mendapatkan kunci aktivasi untuk gateway Anda dari konsol lokal Anda

1. Masuk ke konsol lokal Anda. Jika Anda terhubung ke instans Amazon EC2 dari komputer Windows, masuk sebagai admin.

2. Setelah Anda masuk dan melihat menu utama Aktivasi AWS Alat - Konfigurasi, pilih 0 untuk memilih Dapatkan kunci aktivasi.
3. Pilih Storage Gateway untuk opsi keluarga gateway.
4. Saat diminta, masukkan AWS Wilayah tempat Anda ingin mengaktifkan gateway Anda.
5. Masukkan 1 untuk Publik atau 2 untuk titik akhir VPC sebagai jenis jaringan.
6. Masukkan 1 Standard atau Federal 2 Information Processing Standard (FIPS) sebagai tipe endpoint.

Menghubungkan Inisiator iSCSI

Saat mengelola gateway Anda, Anda bekerja dengan volume atau perangkat pustaka pita virtual (VTL) yang diekspos sebagai target Internet Small Computer System Interface (iSCSI). Untuk Volume Gateways, target iSCSI adalah volume. Untuk Tape Gateways, targetnya adalah perangkat VTL. Sebagai bagian dari pekerjaan ini, Anda melakukan tugas-tugas seperti menghubungkan ke target tersebut, menyesuaikan pengaturan iSCSI, menghubungkan dari klien Red Hat Linux, dan mengonfigurasi Challenge-Handshake Authentication Protocol (CHAP).

Topik

- [Menghubungkan Perangkat VTL Anda ke klien Windows](#)
- [Menghubungkan Volume atau Perangkat VTL Anda ke Klien Linux](#)
- [Menyesuaikan Pengaturan iSCSI](#)
- [Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda](#)

Standar iSCSI adalah standar jaringan penyimpanan berbasis Internet Protocol (IP) untuk memulai dan mengelola koneksi antara perangkat penyimpanan berbasis IP dan klien. Daftar berikut mendefinisikan beberapa istilah yang digunakan untuk menggambarkan koneksi iSCSI dan komponen yang terlibat.

Inisiator iSCSI

Komponen klien dari jaringan iSCSI. Inisiator mengirimkan permintaan ke target iSCSI. Inisiator dapat diimplementasikan dalam perangkat lunak atau perangkat keras. Storage Gateway hanya mendukung inisiator perangkat lunak.

Target iSCSI

Komponen server dari jaringan iSCSI yang menerima dan menanggapi permintaan dari inisiator. Setiap volume Anda diekspos sebagai target iSCSI. Hubungkan hanya satu inisiator iSCSI ke setiap target iSCSI.

Pemrakarsa Microsoft iSCSI

Program perangkat lunak pada komputer Microsoft Windows yang memungkinkan Anda untuk menghubungkan komputer klien (yaitu, komputer yang menjalankan aplikasi yang datanya ingin Anda tulis ke gateway) ke array berbasis iSCSI eksternal (yaitu, gateway). Koneksi dibuat menggunakan kartu adaptor jaringan Ethernet komputer host. Inisiator Microsoft iSCSI telah divalidasi dengan Storage Gateway pada Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016, dan Windows Server 2019. Inisiator dibangun ke dalam sistem operasi ini.

Pemrakarsa iSCSI Red Hat

Paket `iscsi-initiator-utils` Resource Package Manager (RPM) memberi Anda inisiator iSCSI yang diimplementasikan dalam perangkat lunak untuk Red Hat Linux. Paket termasuk daemon server untuk protokol iSCSI.

Setiap jenis gateway dapat terhubung ke perangkat iSCSI, dan Anda dapat menyesuaikan koneksi tersebut, seperti yang dijelaskan berikut.

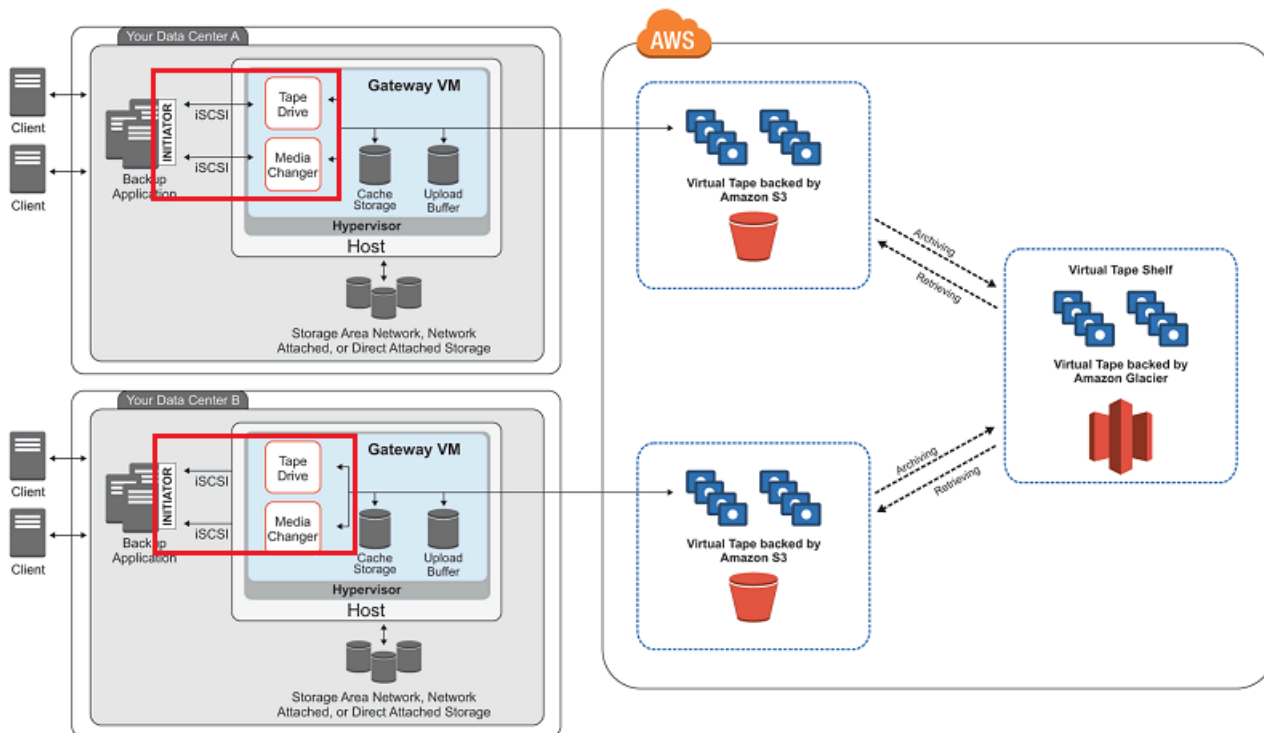
Menghubungkan Perangkat VTL Anda ke klien Windows

Sebuah Tape Gateway mengekspos beberapa tape drive dan media changer, disebut secara kolektif sebagai perangkat VTL, sebagai target iSCSI. Untuk informasi selengkapnya, lihat [Persyaratan](#).

Note

Anda hanya menghubungkan satu aplikasi ke setiap target iSCSI.

Diagram berikut menyoroti target iSCSI dalam gambar yang lebih besar dari arsitektur Storage Gateway. Untuk informasi selengkapnya tentang arsitektur Storage Gateway, lihat [Cara kerja Tape Gateway \(arsitektur\)](#).



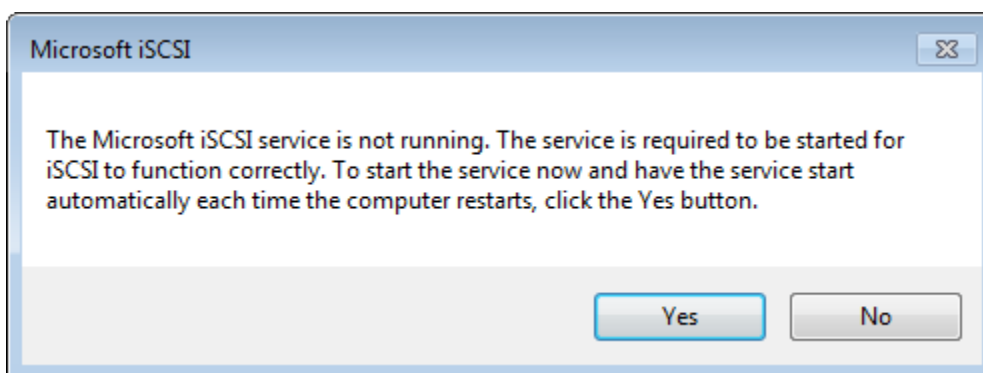
Untuk menghubungkan klien Windows Anda ke perangkat VTL

1. Pada menu Start komputer klien Windows Anda, masukkan **iscsicpl.exe** di kotak Cari Program dan file, cari program inisiator iSCSI, lalu jalankan.

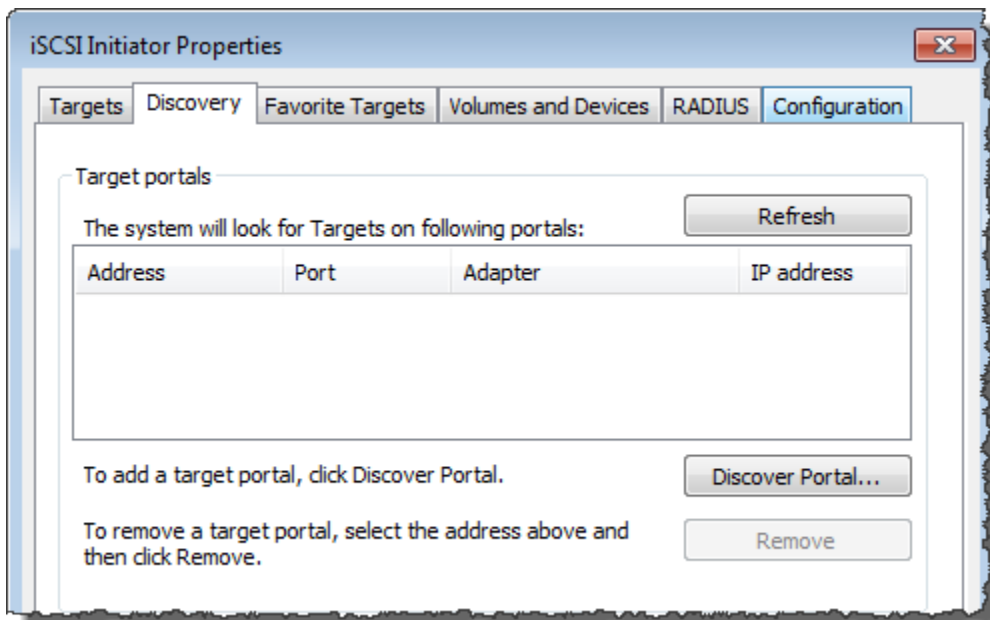
Note

Anda harus memiliki hak administrator pada komputer klien untuk menjalankan inisiator iSCSI.

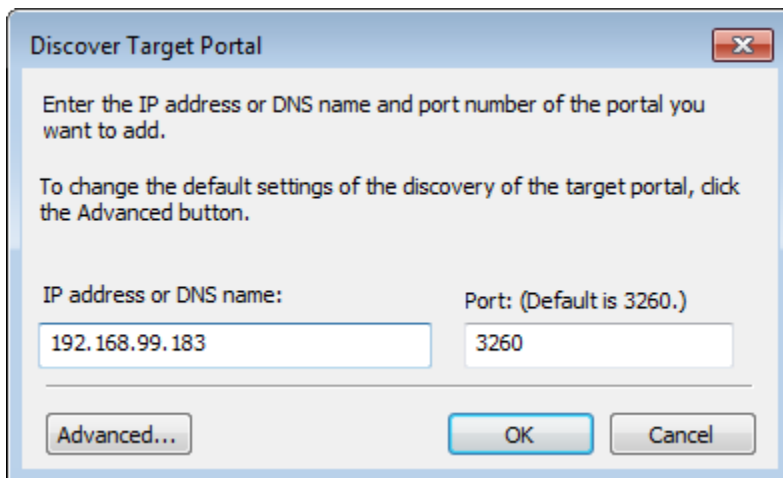
2. Jika diminta, pilih Ya untuk memulai layanan inisiator Microsoft iSCSI.



3. Di kotak dialog iSCSI Initiator Properties, pilih tab Discovery, lalu pilih Discover Portal.



4. Di kotak dialog Discover Target Portal, masukkan alamat IP Tape Gateway Anda untuk alamat IP atau nama DNS, lalu pilih OK. Untuk mendapatkan alamat IP gateway Anda, periksa tab Gateway di konsol Storage Gateway. Jika Anda menerapkan gateway pada instans Amazon EC2, Anda dapat menemukan IP publik atau alamat DNS di tab Deskripsi di konsol Amazon EC2.

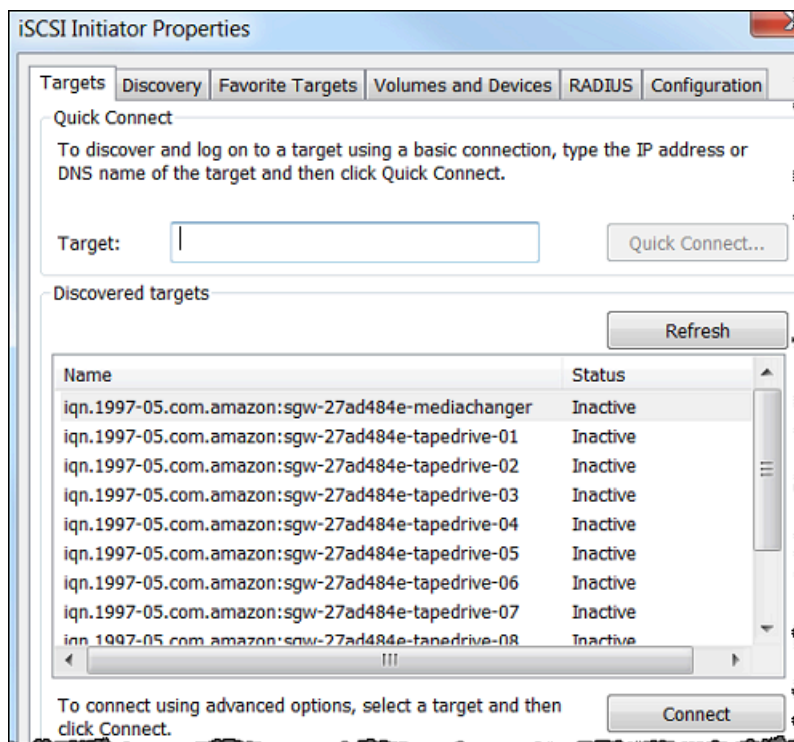


⚠ Warning

Untuk gateway yang digunakan pada instans Amazon EC2, mengakses gateway melalui koneksi internet publik tidak didukung. Alamat IP Elastis instans Amazon EC2 tidak dapat digunakan sebagai alamat target.

5. Pilih tab Target, lalu pilih Refresh. Semua 10 tape drive dan media changer muncul di kotak Target Ditemukan. Status target tidak aktif.

Tangkapan layar berikut menunjukkan target yang ditemukan.

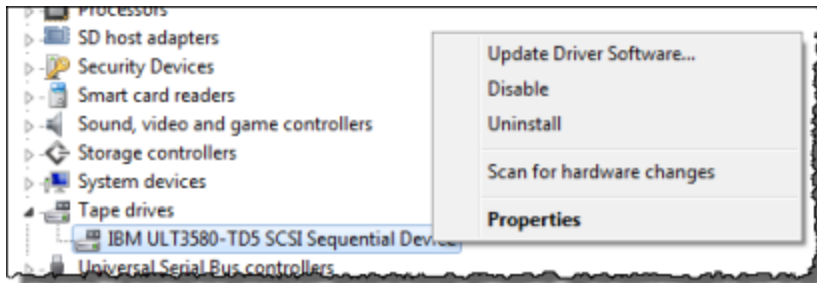


6. Pilih perangkat pertama dan pilih Connect. Anda menghubungkan perangkat satu per satu.
7. Dalam Connect to Target kotak dialog, pilih OK.
8. Ulangi langkah 6 dan 7 untuk masing-masing perangkat untuk menghubungkan semuanya, lalu pilih OK di kotak dialog Properti Inisiator iSCSI.

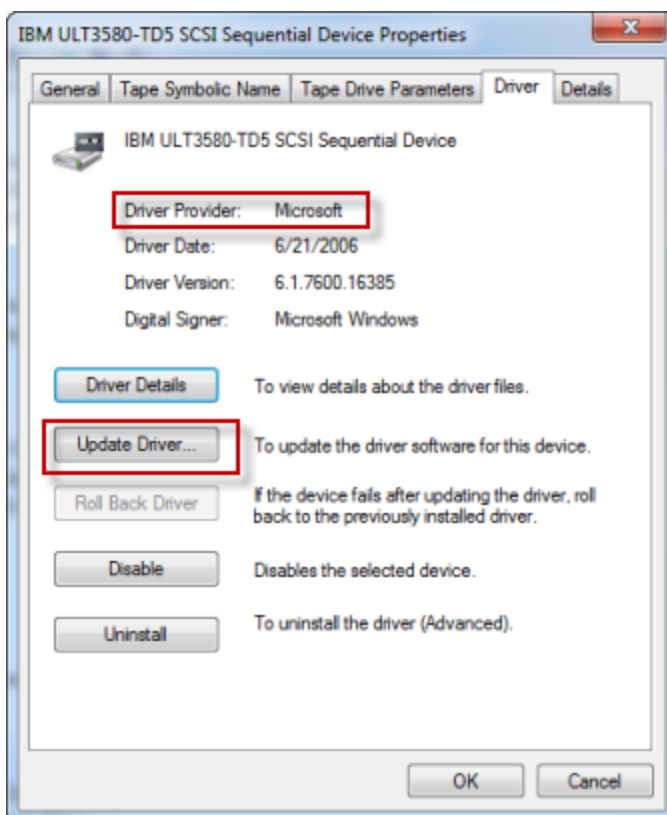
Pada klien Windows, penyedia driver untuk tape drive harus Microsoft. Gunakan prosedur berikut untuk memverifikasi penyedia driver, dan perbarui driver dan penyedia jika perlu.

Untuk memverifikasi penyedia driver dan (jika perlu) memperbarui penyedia dan driver pada klien Windows

1. Pada klien Windows Anda, mulai Device Manager.
2. Perluas drive Tape, pilih menu konteks (klik kanan) untuk tape drive, dan pilih Properties.

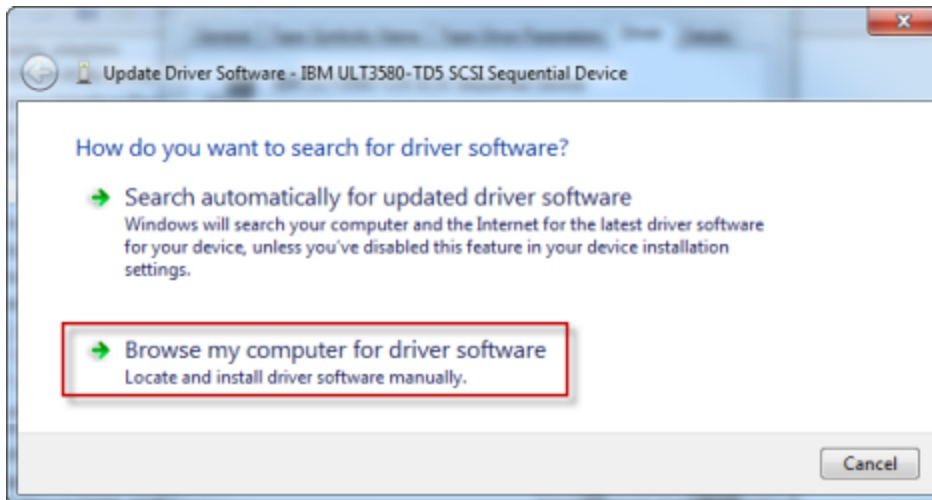


3. Di tab Driver pada kotak dialog Properti Perangkat, verifikasi bahwa Penyedia Driver adalah Microsoft.

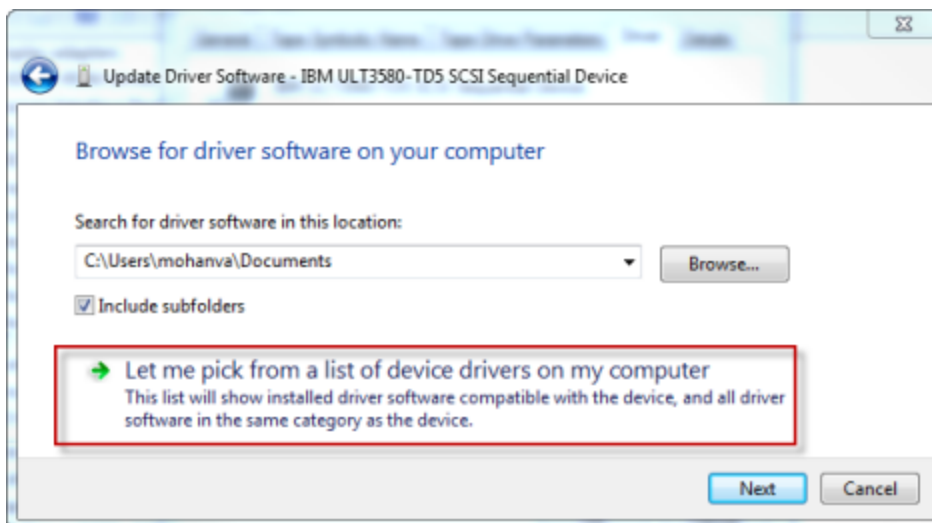


4. Jika Penyedia Driver bukan Microsoft, tetapkan nilainya sebagai berikut:
 - a. Pilih Perbarui Driver.

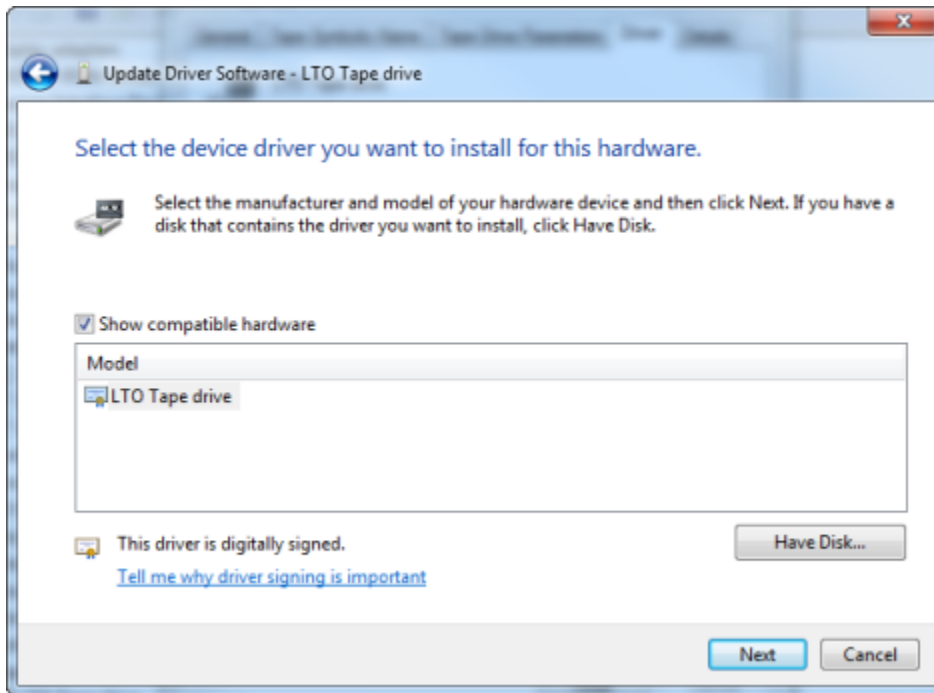
- b. Dalam kotak dialog Perbarui Perangkat Lunak Driver, pilih Jelajahi komputer saya untuk perangkat lunak driver.



- c. Dalam kotak dialog Perbarui Perangkat Lunak Driver, pilih Biarkan saya memilih dari daftar driver perangkat di komputer saya.



- d. Pilih LTO Tape drive dan pilih Berikutnya.



- e. Pilih Tutup untuk menutup jendela Perbarui Perangkat Lunak Driver, dan verifikasi bahwa nilai Penyedia Driver sekarang diatur ke Microsoft.
5. Ulangi langkah 4.1 hingga 4.5 untuk memperbarui semua tape drive.

Menghubungkan Volume atau Perangkat VTL Anda ke Klien Linux

Saat menggunakan Red Hat Enterprise Linux (RHEL), Anda menggunakan paket `iscsi-initiator-utils` RPM untuk terhubung ke target iSCSI gateway Anda (volume atau perangkat VTL).

Untuk menghubungkan klien Linux ke target iSCSI

1. Instal paket `iscsi-initiator-utils` RPM, jika belum diinstal pada klien Anda.

Anda dapat menggunakan perintah berikut untuk menginstal paket.

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

2. Pastikan daemon iSCSI sedang berjalan.
 - a. Verifikasi bahwa daemon iSCSI sedang berjalan menggunakan salah satu perintah berikut.

Untuk RHEL 5 atau 6, gunakan perintah berikut.

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

Untuk RHEL 7, gunakan perintah berikut.

```
sudo service iscsid status
```

- b. Jika perintah status tidak mengembalikan status berjalan, mulai daemon menggunakan salah satu perintah berikut.

Untuk RHEL 5 atau 6, gunakan perintah berikut.

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

Untuk RHEL 7, gunakan perintah berikut. Untuk RHEL 7, Anda biasanya tidak perlu secara eksplisit memulai layanan. `iscsid`

```
sudo service iscsid start
```

3. Untuk menemukan volume atau target perangkat VTL yang ditentukan untuk gateway, gunakan perintah penemuan berikut.

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

Gantikan alamat IP gateway Anda untuk variabel `[GATEWAY_IP]` pada perintah sebelumnya. Anda dapat menemukan IP gateway di properti Info Target iSCSI dari volume pada konsol Storage Gateway.

Output dari perintah penemuan akan terlihat seperti contoh output berikut.


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

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

Nama kualifikasi iSCSI Anda (IQN) akan berbeda dari yang ditunjukkan sebelumnya, karena nilai IQN unik untuk suatu organisasi. Nama target adalah nama yang Anda tentukan saat Anda membuat volume. Anda juga dapat menemukan nama target ini di panel properti Info Target iSCSI saat memilih volume di konsol Storage Gateway.

4. Untuk terhubung ke target, gunakan perintah berikut.

Perhatikan bahwa Anda perlu menentukan `[GATEWAY_IP]` dan IQN yang benar dalam perintah `connect`.

 Warning

Untuk gateway yang digunakan pada instans Amazon EC2, mengakses gateway melalui koneksi internet publik tidak didukung. Alamat IP Elastis instans Amazon EC2 tidak dapat digunakan sebagai alamat target.

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

5. Untuk memverifikasi bahwa volume terpasang ke mesin klien (inisiator), gunakan perintah berikut.

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

Output dari perintah akan terlihat seperti contoh output berikut.

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

Kami sangat menyarankan bahwa setelah Anda mengatur inisiator Anda, Anda menyesuaikan pengaturan iSCSI Anda seperti yang dibahas di [Menyesuaikan Pengaturan iSCSI Linux Anda](#)

Menyesuaikan Pengaturan iSCSI

Setelah menyiapkan inisiator, kami sangat menyarankan agar Anda menyesuaikan pengaturan iSCSI agar inisiator tidak terputus dari target.

Dengan meningkatkan nilai batas waktu iSCSI seperti yang ditunjukkan pada langkah-langkah berikut, Anda membuat aplikasi Anda lebih baik dalam menangani operasi tulis yang memakan waktu lama dan masalah sementara lainnya seperti gangguan jaringan.

Note

Sebelum membuat perubahan pada registri, Anda harus membuat salinan cadangan registri. Untuk informasi tentang membuat salinan cadangan dan praktik terbaik lainnya yang harus diikuti saat bekerja dengan registri, lihat [Praktik terbaik registri](#) di TechNet Perpustakaan Microsoft.

Topik

- [Menyesuaikan Pengaturan Windows iSCSI Anda](#)
- [Menyesuaikan Pengaturan iSCSI Linux Anda](#)
- [Menyesuaikan Pengaturan Batas Waktu Disk Linux Anda untuk Volume Gateways](#)

Menyesuaikan Pengaturan Windows iSCSI Anda

Untuk penyiapan Tape Gateway, menghubungkan ke perangkat VTL Anda dengan menggunakan inisiator Microsoft iSCSI adalah proses dua langkah:

1. Hubungkan perangkat Tape Gateway Anda ke klien Windows Anda.
2. Jika Anda menggunakan aplikasi cadangan, konfigurasi aplikasi untuk menggunakan perangkat.

Pengaturan contoh Memulai memberikan instruksi untuk kedua langkah ini. Ini menggunakan aplikasi NetBackup cadangan Symantec. Lihat informasi yang lebih lengkap di [Menghubungkan Perangkat VTL Anda](#) dan [Mengkonfigurasi Perangkat NetBackup Penyimpanan](#).

Untuk menyesuaikan pengaturan Windows iSCSI Anda

1. Tingkatkan waktu maksimum untuk permintaan yang diantrian.
 - a. Mulai Editor Registri (`Regedit.exe`).
 - b. Arahkan ke kunci pengenalan unik global (GUID) untuk kelas perangkat yang berisi setelan pengontrol iSCSI, yang ditampilkan sebagai berikut.

⚠ Warning

Pastikan Anda bekerja di CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318} dan bukan set kontrol lain, seperti ControlSet001 atau ControlSet002.

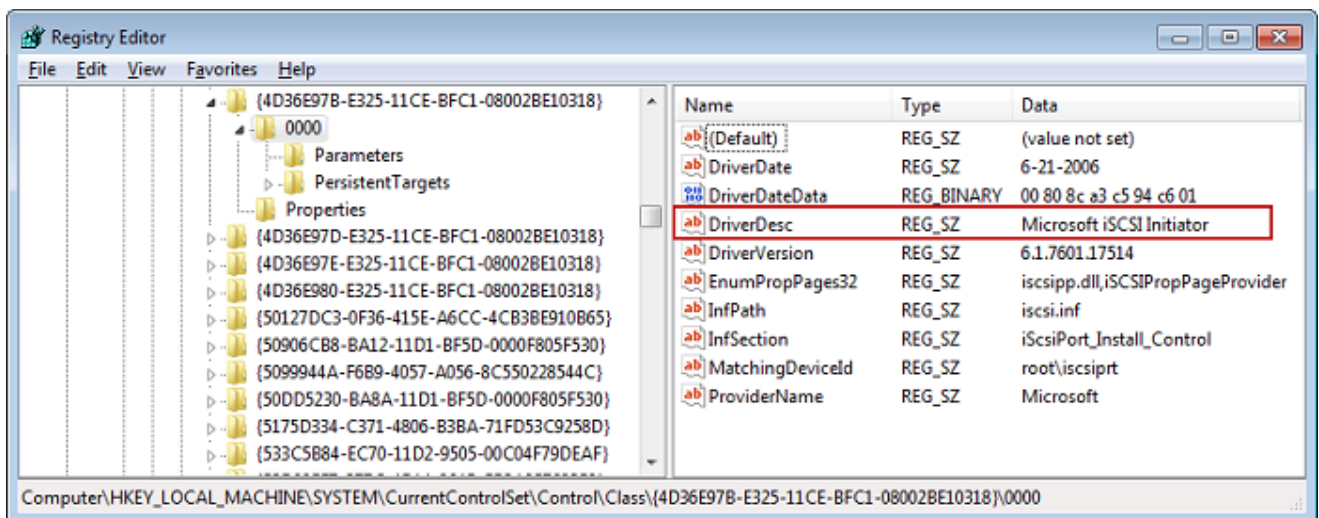
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

- c. *Temukan subkunci untuk inisiator Microsoft iSCSI, yang ditampilkan berikut sebagai [*<Nomor Instance*].*

Kunci diwakili oleh angka empat digit, seperti 0000.

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

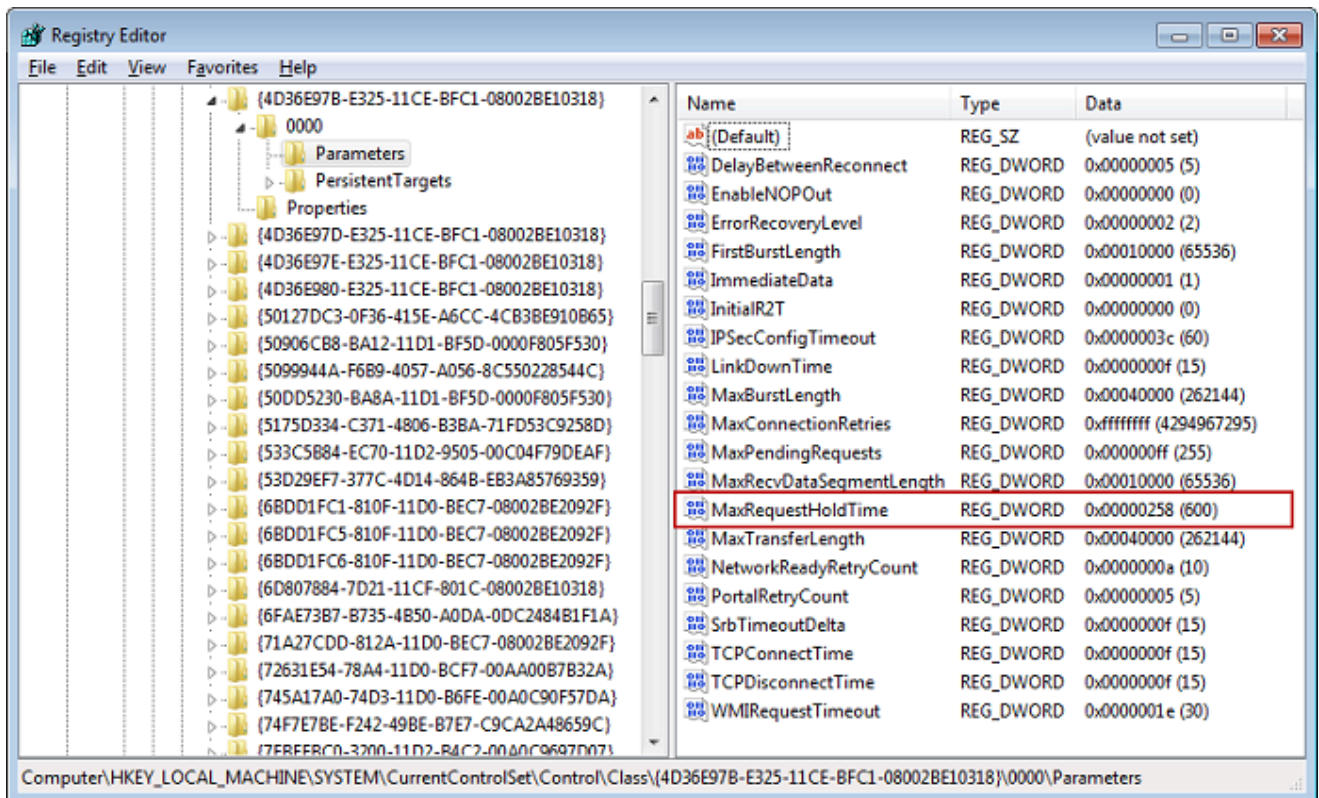
Bergantung pada apa yang diinstal pada komputer Anda, inisiator Microsoft iSCSI mungkin bukan subkuncinya. 0000 Anda dapat memastikan bahwa Anda telah memilih subkunci yang benar dengan memverifikasi bahwa string DriverDesc memiliki nilai Microsoft iSCSI Initiator, seperti yang ditunjukkan pada contoh berikut.



- d. Untuk menampilkan pengaturan iSCSI, pilih subkunci Parameter.

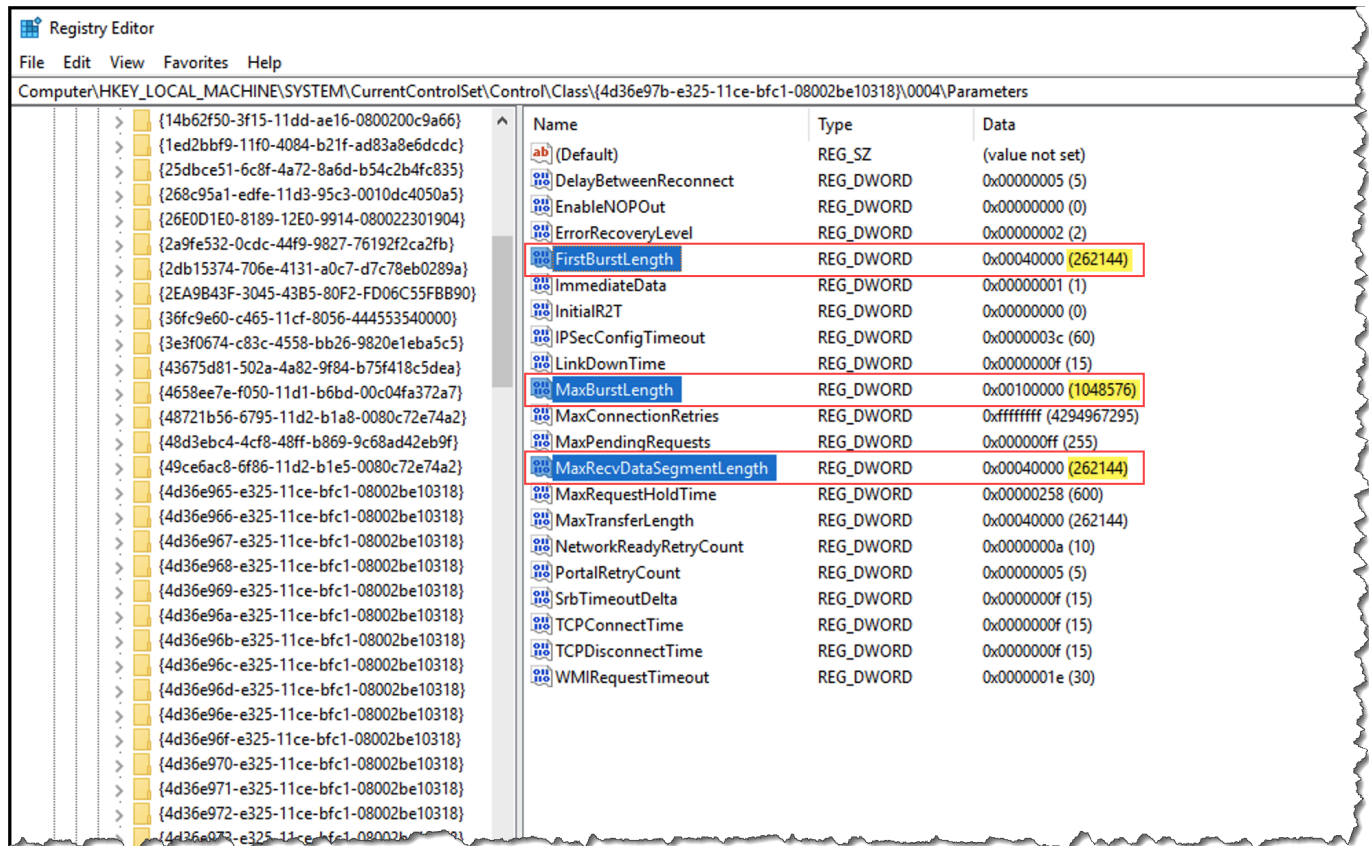
- e. Buka menu konteks (klik kanan) untuk nilai MaxRequestHoldTimeDWORD (32-bit), pilih Ubah, lalu ubah nilainya menjadi. **600**

MaxRequestHoldTime menentukan berapa detik inisiator Microsoft iSCSI harus menahan dan mencoba lagi perintah yang luar biasa untuk, sebelum memberi tahu lapisan atas suatu peristiwa. Device Removal Nilai ini mewakili waktu penahanan 600 detik, seperti yang ditunjukkan pada contoh berikut.



2. Anda dapat meningkatkan jumlah maksimum data yang dapat dikirim dalam paket iSCSI dengan memodifikasi parameter berikut:

- FirstBurstLength mengontrol jumlah maksimum data yang dapat dikirimkan dalam permintaan tulis yang tidak diminta. Tetapkan nilai ini ke **262144** atau default OS Windows, mana yang lebih tinggi.
- MaxBurstLength mirip dengan FirstBurstLength, tetapi menetapkan jumlah maksimum data yang dapat ditransmisikan dalam urutan tulis yang diminta. Tetapkan nilai ini ke **1048576** atau default OS Windows, mana yang lebih tinggi.
- MaxRecvDataSegmentLength mengontrol ukuran segmen data maksimum yang dikaitkan dengan unit data protokol tunggal (PDU). Tetapkan nilai ini ke **262144** atau default OS Windows, mana yang lebih tinggi.



Note

Perangkat lunak cadangan yang berbeda dapat dioptimalkan untuk bekerja paling baik menggunakan pengaturan iSCSI yang berbeda. Untuk memverifikasi nilai mana untuk parameter ini yang akan memberikan kinerja terbaik, lihat dokumentasi untuk perangkat lunak cadangan Anda.

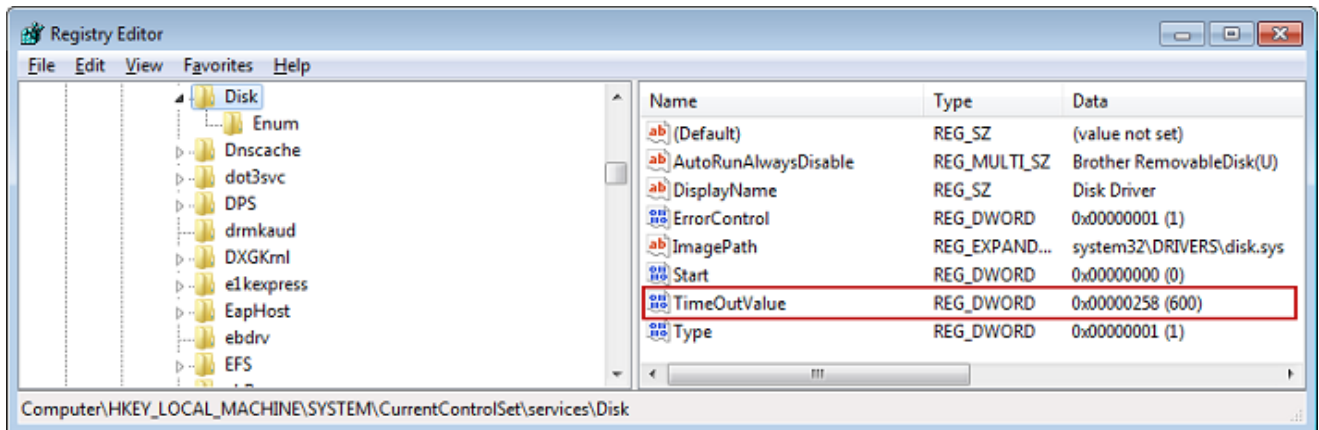
3. Tingkatkan nilai batas waktu disk, seperti yang ditunjukkan berikut:

- Mulai Registry Editor (Regedit . exe), jika Anda belum melakukannya.
- Arahkan ke subkunci Disk di subkunci Layanan dari CurrentControlSet, yang ditunjukkan berikut.

HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk

- Buka menu konteks (klik kanan) untuk nilai TimeoutValueDWORD (32-bit), pilih Ubah, lalu ubah nilainya menjadi. **600**

TimeoutValue menentukan berapa detik iSCSI inisiator akan menunggu respons dari target sebelum mencoba pemulihan sesi dengan menjatuhkan dan membangun kembali koneksi. Nilai ini mewakili periode batas waktu 600 detik, seperti yang ditunjukkan pada contoh berikut.



4. Untuk memastikan bahwa nilai konfigurasi baru berlaku, restart sistem Anda.

Sebelum memulai ulang, Anda harus memastikan bahwa hasil dari semua operasi penulisan ke volume dibilas. Untuk melakukan ini, ambil disk volume penyimpanan yang dipetakan secara offline sebelum memulai ulang.

Menyesuaikan Pengaturan iSCSI Linux Anda

Setelah menyiapkan inisiator untuk gateway Anda, kami sangat menyarankan Anda menyesuaikan pengaturan iSCSI Anda untuk mencegah inisiator terputus dari target. Dengan meningkatkan nilai batas waktu iSCSI seperti yang ditunjukkan berikut, Anda membuat aplikasi Anda lebih baik dalam menangani operasi tulis yang memakan waktu lama dan masalah sementara lainnya seperti gangguan jaringan.

Note

Perintah mungkin sedikit berbeda untuk jenis Linux lainnya. Contoh berikut didasarkan pada Red Hat Linux.

Untuk menyesuaikan pengaturan iSCSI Linux Anda

1. Tingkatkan waktu maksimum untuk permintaan yang diantrian.

- a. Buka `/etc/iscsi/iscsid.conf` file dan temukan baris berikut.


```
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. Setel nilai `[replacement_timeout_value]` ke. **600**

Setel nilai `[noop_out_interval_value]` ke. **60**

Setel nilai `[noop_out_timeout_value]` ke. **600**

Ketiga nilai dalam hitungan detik.

 Note

`iscsid.conf` Pengaturan harus dilakukan sebelum menemukan gateway. Jika Anda telah menemukan gateway atau masuk ke target, atau keduanya, Anda dapat menghapus entri dari database penemuan menggunakan perintah berikut. Kemudian Anda dapat menemukan kembali atau masuk lagi untuk mengambil konfigurasi baru.

```
iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
```

2. Tingkatkan nilai maksimum untuk jumlah data yang dapat ditransmisikan di setiap respons.
 - a. Buka `/etc/iscsi/iscsid.conf` file dan temukan baris berikut.


```
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. Kami merekomendasikan nilai-nilai berikut untuk mencapai kinerja yang lebih baik. Perangkat lunak cadangan Anda mungkin dioptimalkan untuk menggunakan nilai yang berbeda, jadi lihat dokumentasi perangkat lunak cadangan Anda untuk hasil terbaik.

Setel nilai `[replacement_first_burst_length_value]` ke *atau default* OS Linux, mana yang lebih tinggi. **262144**

Setel nilai `[replacement_max_burst_length_value]` ke atau default OS Linux, mana yang lebih tinggi. **1048576**

Setel nilai `[replacement_segment_length_value]` ke **262144** atau default OS Linux, mana yang lebih tinggi.

 Note

Perangkat lunak cadangan yang berbeda dapat dioptimalkan untuk bekerja paling baik menggunakan pengaturan iSCSI yang berbeda. Untuk memverifikasi nilai mana untuk parameter ini yang akan memberikan kinerja terbaik, lihat dokumentasi untuk perangkat lunak cadangan Anda.

3. Mulai ulang sistem Anda untuk memastikan bahwa nilai konfigurasi baru berlaku.

Sebelum memulai ulang, pastikan bahwa hasil dari semua operasi penulisan ke kaset Anda dibilas. Untuk melakukan ini, lepaskan kaset sebelum memulai ulang.

Menyesuaikan Pengaturan Batas Waktu Disk Linux Anda untuk Volume Gateways

Jika Anda menggunakan Volume Gateway, Anda dapat menyesuaikan pengaturan batas waktu disk Linux berikut selain pengaturan iSCSI yang dijelaskan di bagian sebelumnya.

Untuk menyesuaikan pengaturan batas waktu disk Linux Anda

1. Tingkatkan nilai batas waktu disk dalam file aturan.
 - a. Jika Anda menggunakan inisiator RHEL 5, buka `/etc/udev/rules.d/50-udev.rules` file, dan temukan baris berikut.

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \  
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

File aturan ini tidak ada di inisiator RHEL 6 atau 7, jadi Anda harus membuatnya menggunakan aturan berikut.

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway", \  
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Untuk mengubah nilai batas waktu di RHEL 6, gunakan perintah berikut, lalu tambahkan baris kode yang ditunjukkan sebelumnya.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

Untuk mengubah nilai batas waktu di RHEL 7, gunakan perintah berikut, lalu tambahkan baris kode yang ditunjukkan sebelumnya.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

- b. Tetapkan nilai [*timeout*] ke**600**.

Nilai ini mewakili batas waktu 600 detik.

2. Mulai ulang sistem Anda untuk memastikan bahwa nilai konfigurasi baru berlaku.

Sebelum memulai ulang, pastikan bahwa hasil dari semua operasi penulisan ke volume Anda dibilas. Untuk melakukan ini, lepaskan volume penyimpanan sebelum memulai ulang.

3. Anda dapat menguji konfigurasi dengan menggunakan perintah berikut.

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

Perintah ini menunjukkan aturan udev yang diterapkan ke perangkat iSCSI.

Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda

Storage Gateway mendukung otentikasi antara gateway Anda dan inisiator iSCSI dengan menggunakan Challenge-Handshake Authentication Protocol (CHAP). CHAP memberikan perlindungan terhadap serangan pemutaran dengan memverifikasi identitas inisiator iSCSI secara berkala sebagai otentikasi untuk mengakses volume dan target perangkat VTL.

Note

Konfigurasi CHAP bersifat opsional tetapi sangat disarankan.

Untuk mengatur CHAP, Anda harus mengonfigurasinya di konsol Storage Gateway dan di perangkat lunak inisiator iSCSI yang Anda gunakan untuk terhubung ke target. Storage Gateway menggunakan CHAP bersama, yaitu ketika inisiator mengotentikasi target dan target mengotentikasi inisiator.

Untuk mengatur CHAP bersama untuk target Anda

1. Konfigurasi CHAP di konsol Storage Gateway, seperti yang dibahas di [Untuk mengonfigurasi CHAP untuk target perangkat VTL di konsol Storage Gateway](#).
2. Dalam perangkat lunak inisiator klien Anda, selesaikan konfigurasi CHAP:
 - Untuk mengkonfigurasi CHAP bersama pada klien Windows, lihat [Untuk mengkonfigurasi CHAP bersama pada klien Windows](#).
 - Untuk mengkonfigurasi CHAP bersama pada klien Red Hat Linux, lihat [Untuk mengkonfigurasi CHAP bersama pada klien Red Hat Linux](#).


Untuk mengonfigurasi CHAP untuk target perangkat VTL di konsol Storage Gateway

Dalam prosedur ini, Anda menentukan dua kunci rahasia yang digunakan untuk membaca dan menulis ke rekaman virtual. Kunci yang sama ini digunakan dalam prosedur untuk mengkonfigurasi inisiator klien.

1. Di panel navigasi, pilih Gateway.
2. Pilih gateway Anda, lalu pilih tab Perangkat VTL untuk menampilkan semua perangkat VTL Anda.
3. Pilih perangkat yang ingin Anda konfigurasi CHAP.
4. Berikan informasi yang diminta di kotak dialog Configure CHAP Authentication.
 - a. Untuk Nama Inisiator, masukkan nama inisiator iSCSI Anda. Nama ini adalah nama yang memenuhi syarat Amazon iSCSI (IQN) yang ditambahkan dengan diikuti oleh nama target `iqn.1997-05.com.amazon:`. Berikut sebuah contoh.

`iqn.1997-05.com.amazon:your-tape-device-name`

Anda dapat menemukan nama inisiator dengan menggunakan perangkat lunak inisiator iSCSI Anda. Misalnya, untuk klien Windows, namanya adalah nilai pada tab Konfigurasi inisiator iSCSI. Untuk informasi selengkapnya, lihat [Untuk mengkonfigurasi CHAP bersama pada klien Windows](#).

 Note


Untuk mengubah nama inisiator, Anda harus terlebih dahulu menonaktifkan CHAP, mengubah nama inisiator di perangkat lunak inisiator iSCSI Anda, dan kemudian mengaktifkan CHAP dengan nama baru.

- b. Untuk Rahasia yang digunakan untuk Mengautentikasi Inisiator, masukkan rahasia yang diminta.

Rahasia ini harus minimal 12 karakter dan panjang maksimal 16 karakter. Nilai ini adalah kunci rahasia yang harus diketahui oleh inisiator (yaitu, klien Windows) untuk berpartisipasi dalam CHAP dengan target.

- c. Untuk Rahasia yang digunakan untuk Mengautentikasi Target (Mutual CHAP), masukkan rahasia yang diminta.

Rahasia ini harus minimal 12 karakter dan panjang maksimal 16 karakter. Nilai ini adalah kunci rahasia yang harus diketahui target untuk berpartisipasi dalam CHAP dengan inisiator.

 Note

Rahasia yang digunakan untuk mengotentikasi target harus berbeda dari rahasia untuk mengotentikasi inisiator.

- d. Pilih Simpan.
5. Pada tab Perangkat VTL, konfirmasi bahwa bidang otentikasi iSCSI CHAP disetel ke true.

Untuk mengkonfigurasi CHAP bersama pada klien Windows

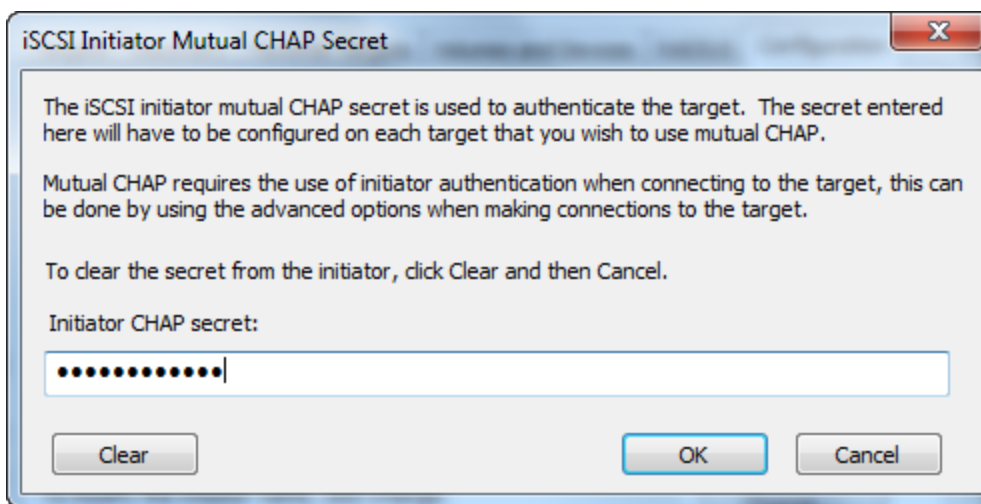
Dalam prosedur ini, Anda mengonfigurasi CHAP di inisiator Microsoft iSCSI menggunakan tombol yang sama yang Anda gunakan untuk mengonfigurasi CHAP untuk volume di konsol.

1. Jika inisiator iSCSI belum dimulai, pada menu Start komputer klien Windows Anda, pilih Run, **iscsicpl.exe** enter, lalu pilih OK untuk menjalankan program.
2. Konfigurasi konfigurasi CHAP timbal balik untuk inisiator (yaitu, klien Windows):
 - a. Pilih tab Konfigurasi.

Note

Nilai Nama Inisiator unik untuk inisiator dan perusahaan Anda. Nama yang ditampilkan sebelumnya adalah nilai yang Anda gunakan di kotak dialog Configure CHAP Authentication dari konsol Storage Gateway.
Nama yang ditunjukkan pada gambar contoh adalah untuk tujuan demonstrasi saja.

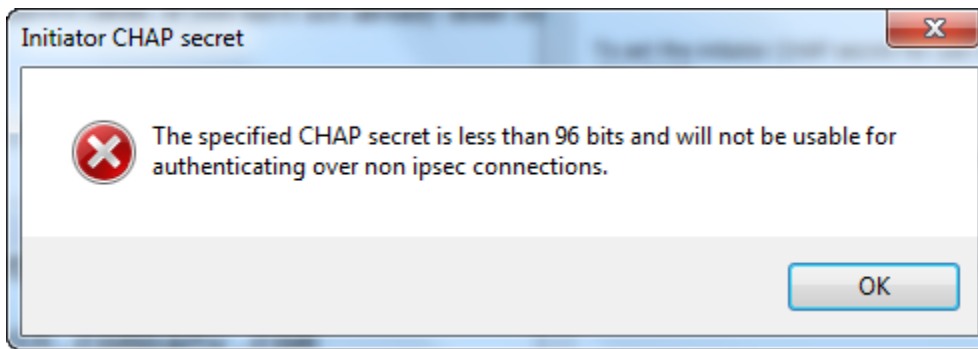
- b. Pilih CHAP.
- c. Dalam kotak dialog iSCSI Initiator Mutual Chap Secret, masukkan nilai rahasia CHAP bersama.



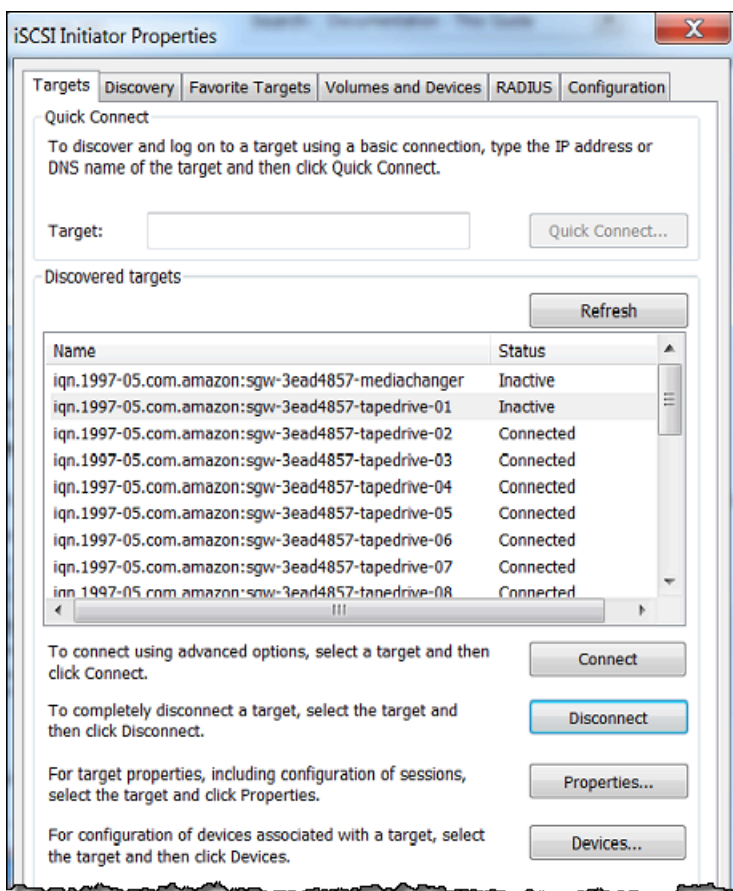
Di kotak dialog ini, Anda memasukkan rahasia yang digunakan inisiator (klien Windows) untuk mengotentikasi target (volume penyimpanan). Rahasia ini memungkinkan target untuk membaca dan menulis ke inisiator. Rahasia ini sama dengan rahasia yang dimasukkan ke dalam kotak Secret used to Authenticate Target (Mutual CHAP) di kotak dialog Configure CHAP Authentication. Untuk informasi selengkapnya, lihat [Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda](#).

- d. Jika kunci yang Anda masukkan kurang dari 12 karakter atau lebih dari 16 karakter, kotak dialog kesalahan rahasia Initiator CHAP akan muncul.

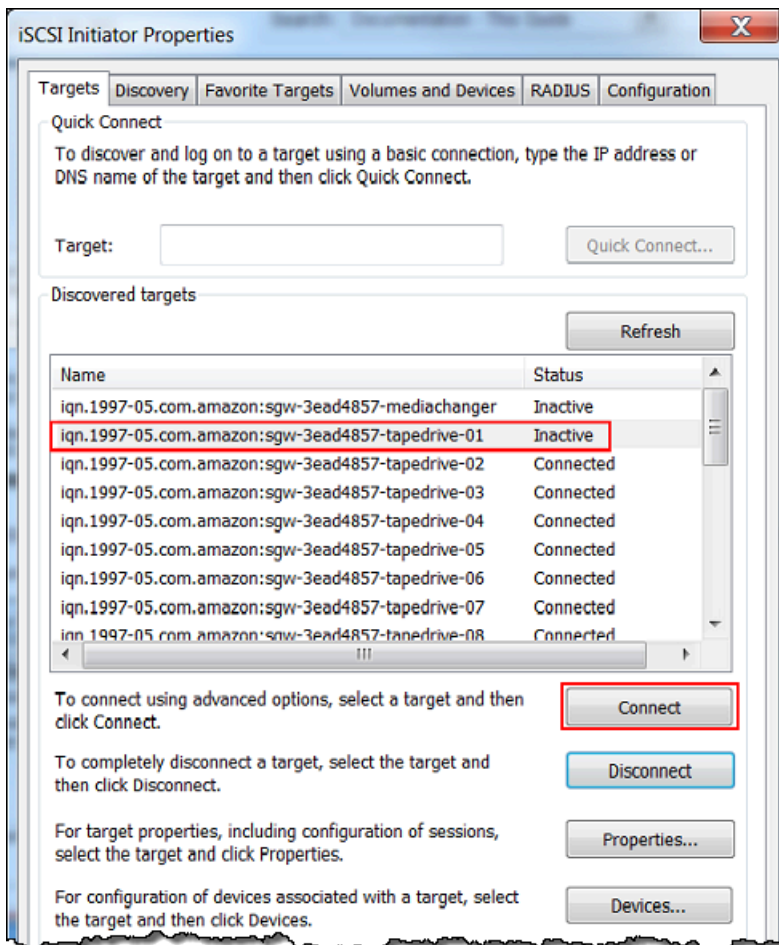
Pilih OK, lalu masukkan kunci lagi.



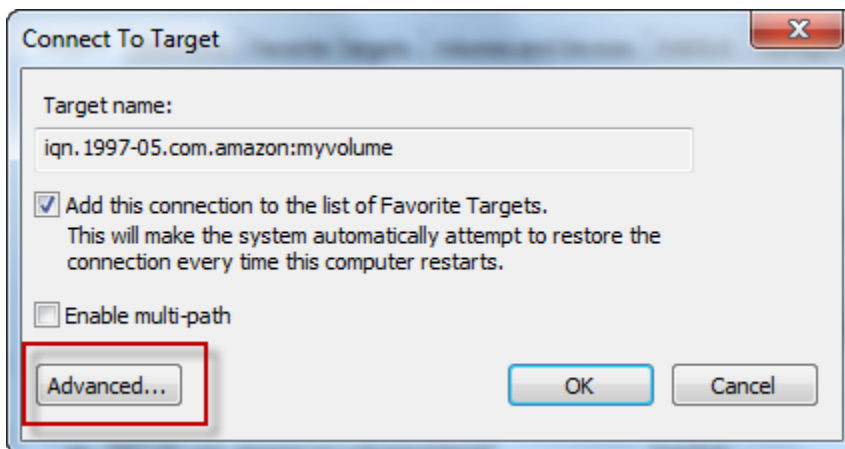
3. Konfigurasi target dengan rahasia inisiator untuk menyelesaikan konfigurasi CHAP bersama.
 - a. Pilih tab Target.



- b. Jika target yang ingin Anda konfigurasi untuk CHAP saat ini terhubung, putuskan sambungan target dengan memilihnya dan memilih Putuskan sambungan.
 - c. Pilih target yang ingin Anda konfigurasi untuk CHAP, lalu pilih Connect.

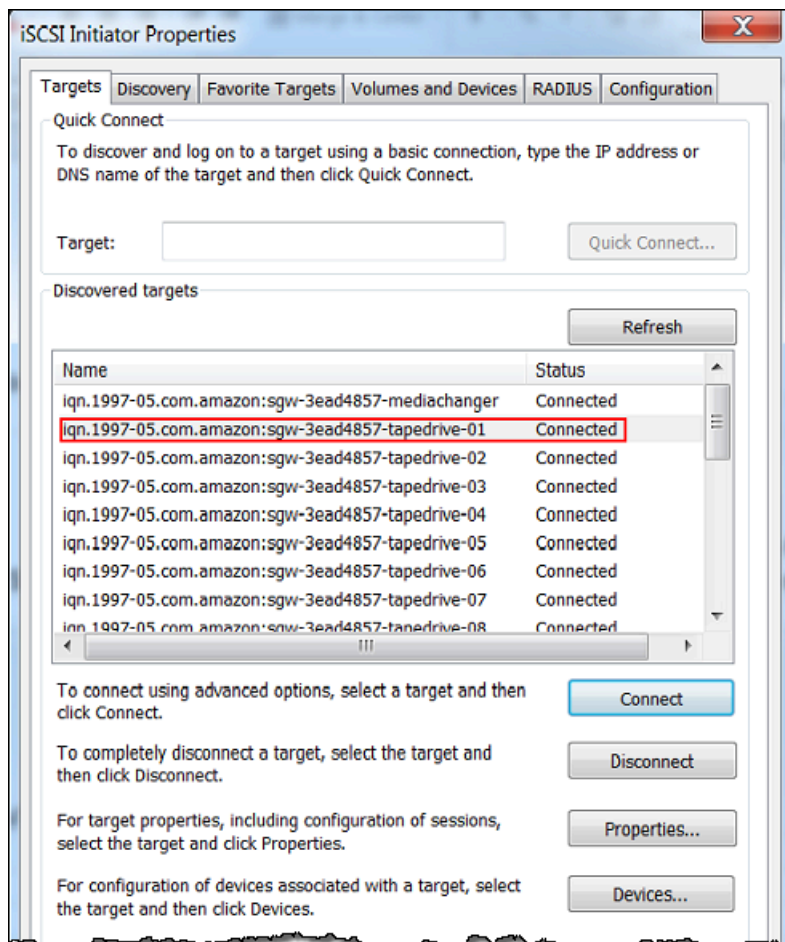


- d. Di kotak dialog Connect to Target, pilih Advanced.



- e. Di kotak dialog Pengaturan Lanjut, konfigurasi CHAP.
- i. Pilih Aktifkan CHAP log on.

- ii. Masukkan rahasia yang diperlukan untuk mengautentikasi inisiator. Rahasia ini sama dengan rahasia yang dimasukkan ke dalam kotak Secret used to Authenticate Initiator di kotak dialog Configure CHAP Authentication. Untuk informasi selengkapnya, lihat [Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda](#).
 - iii. Pilih Lakukan otentikasi timbal balik.
 - iv. Untuk menerapkan perubahan, pilih OK.
- f. Dalam Connect to Target kotak dialog, pilih OK.
4. Jika Anda memberikan kunci rahasia yang benar, target menunjukkan status Terhubung.



Untuk mengkonfigurasi CHAP bersama pada klien Red Hat Linux

Dalam prosedur ini, Anda mengkonfigurasi CHAP di inisiator iSCSI Linux menggunakan tombol yang sama yang Anda gunakan untuk mengkonfigurasi CHAP untuk volume pada konsol Storage Gateway.

1. Pastikan daemon iSCSI sedang berjalan dan Anda telah terhubung ke target. Jika Anda belum menyelesaikan dua tugas ini, lihat [yang Menghubungkan ke Klien Linux](#).
2. Putuskan sambungan dan hapus konfigurasi yang ada untuk target yang akan Anda konfigurasi CHAP.
 - a. Untuk menemukan nama target dan memastikannya adalah konfigurasi yang ditentukan, daftarkan konfigurasi yang disimpan menggunakan perintah berikut.

```
sudo /sbin/iscsiadm --mode node
```

- b. Putuskan sambungan dari target.

Perintah berikut terputus dari target bernama **myvolume** yang didefinisikan dalam nama yang memenuhi syarat Amazon iSCSI (IQN). Ubah nama target dan IQN sesuai kebutuhan untuk situasi Anda.

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1  
iqn.1997-05.com.amazon:myvolume
```

- c. Hapus konfigurasi untuk target.

Perintah berikut menghapus konfigurasi untuk **myvolume** target.

```
sudo /sbin/iscsiadm --mode node --op delete --targetname  
iqn.1997-05.com.amazon:myvolume
```

3. Edit file konfigurasi iSCSI untuk mengaktifkan CHAP.
 - a. Dapatkan nama inisiator (yaitu, klien yang Anda gunakan).

Perintah berikut mendapatkan nama inisiator dari `/etc/iscsi/initiatorname.iscsi` file.

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

Output dari perintah ini terlihat seperti ini:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

- b. Buka file `/etc/iscsi/iscsid.conf`.

- c. *Hapus komentar baris berikut dalam file dan tentukan nilai yang benar untuk nama pengguna, kata sandi, `username_in`, dan `password_in`.*

```
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
```

Untuk panduan tentang nilai apa yang akan ditentukan, lihat tabel berikut.

Pengaturan Konfigurasi	Nilai
<i>username</i>	Nama inisiator yang Anda temukan di langkah sebelumnya dalam prosedur ini. Nilai dimulai dengan iqn. Misalnya, iqn.1994-05.com.redhat:8e89b27b5b8 adalah nilai <i>nama pengguna</i> yang valid.
<i>password</i>	Kunci rahasia yang digunakan untuk mengotentikasi inisiator (klien yang Anda gunakan) ketika berkomunikasi dengan volume.
<i>username_in</i>	IQN dari volume target. Nilai dimulai dengan iqn dan diakhiri dengan nama target. Misalnya, iqn.1997-05.com.amazon:myvolume adalah nilai <i>username_in</i> yang valid.
<i>password_in</i>	Kunci rahasia yang digunakan untuk mengotentikasi target (volume) ketika berkomunikasi dengan inisiator.

- d. Simpan perubahan dalam file konfigurasi, lalu tutup file.
4. Temukan dan masuk ke target. Untuk melakukannya, ikuti langkah-langkah dalam yang [Menghubungkan ke Klien Linux](#).

Menggunakan AWS Direct Connect dengan Storage Gateway

AWS Direct Connect menghubungkan jaringan internal Anda ke Amazon Web Services Cloud. AWS Direct Connect Dengan menggunakan Storage Gateway, Anda dapat membuat koneksi untuk kebutuhan beban kerja throughput tinggi, menyediakan koneksi jaringan khusus antara gateway lokal dan. AWS

Storage Gateway menggunakan endpoint publik. Dengan AWS Direct Connect koneksi di tempat, Anda dapat membuat antarmuka virtual publik untuk memungkinkan lalu lintas dirutekan ke titik akhir Storage Gateway. Antarmuka virtual publik melewati penyedia layanan internet di jalur jaringan Anda. Endpoint publik layanan Storage Gateway dapat berada di AWS Wilayah yang sama dengan AWS Direct Connect lokasi, atau dapat berada di AWS Wilayah yang berbeda.

Ilustrasi berikut menunjukkan contoh cara AWS Direct Connect kerja dengan Storage Gateway. arsitektur jaringan yang menunjukkan Storage Gateway terhubung ke cloud menggunakan koneksi AWS langsung.

Prosedur berikut mengasumsikan bahwa Anda telah membuat gateway yang berfungsi.

Untuk digunakan AWS Direct Connect dengan Storage Gateway

1. Membuat dan membuat AWS Direct Connect koneksi antara pusat data lokal dan titik akhir Storage Gateway Anda. Untuk informasi selengkapnya tentang cara membuat sambungan, lihat [Memulai AWS Direct Connect](#) di Panduan AWS Direct Connect Pengguna.
2. Hubungkan alat Storage Gateway lokal Anda ke AWS Direct Connect router.
3. Buat antarmuka virtual publik, dan konfigurasi router lokal Anda sesuai dengan itu. Bahkan dengan Direct Connect, titik akhir VPC harus dibuat dengan HAProxy. Untuk informasi selengkapnya, lihat [Membuat Antarmuka Virtual](#) di Panduan AWS Direct Connect Pengguna.

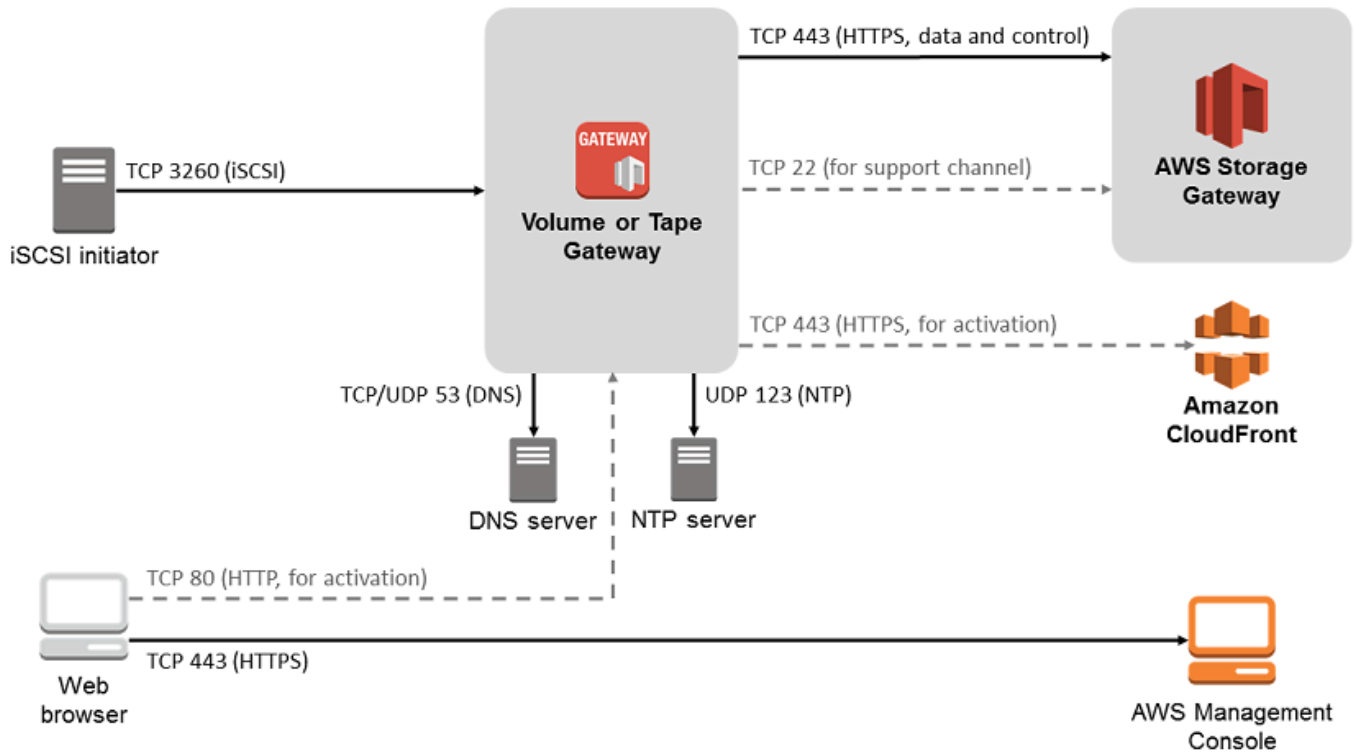
Untuk detailnya AWS Direct Connect, lihat [Apa itu AWS Direct Connect?](#) dalam AWS Direct Connect User Guide.

Persyaratan Pelabuhan

Storage Gateway membutuhkan port berikut untuk operasinya. Beberapa port umum dan dibutuhkan oleh semua jenis gateway. Port lain diperlukan oleh jenis gateway tertentu. Di bagian ini, Anda dapat menemukan ilustrasi dan daftar port yang diperlukan untuk Tape Gateway .

Gerbang Gerbang Pita

Ilustrasi berikut menunjukkan semua port yang perlu Anda buka untuk operasi gateway Tape Gateway .



Port berikut adalah umum untuk dan diperlukan oleh semua jenis gateway.

Dari	Ke	Protokol	Port	Bagaimana Digunakan
Storage Gateway VM	AWS	Protokol Kontrol Transmisi (TCP)	443 (HTTPS)	Untuk komunikasi dari VM keluar Storage Gateway ke titik akhir AWS layanan. Untuk

Dari	Ke	Protokol	Port	Bagaimana Digunakan	
				informasi tentang titik akhir layanan, lihat Mengizinkan AWS Storage Gateway akses melalui firewall dan router.	

Dari	Ke	Protokol	Port	Bagaimana Digunakan
Peramban web Anda	Storage Gateway VM	TCP	80 (HTTP)	<p>Dengan sistem lokal untuk mendapatkan kunci aktivasi Storage Gateway. Port 80 hanya digunakan selama aktivasi alat Storage Gateway.</p> <p>VM Storage Gateway tidak memerlukan port 80 agar dapat diakses publik. Tingkat akses yang diperlukan ke port 80 tergantung pada konfigurasi jaringan Anda. Jika Anda mengaktifkan gateway</p>

Dari	Ke	Protokol	Port	Bagaimana Digunakan	
				dari Storage Gateway Management Console, host tempat Anda terhubung ke konsol harus memiliki akses ke port gateway 80 Anda.	
Storage Gateway VM	Server Domain Name Service (DNS)	Protokol Datagram Pengguna (UDP) /UDP	53 (DNS)	Untuk komunikasi antara Storage Gateway VM dan server DNS.	

Dari	Ke	Protokol	Port	Bagaimana Digunakan	
Storage Gateway VM	AWS	TCP	22 (Saluran dukungan)	Memungkinkan AWS Support untuk mengakses gateway Anda untuk membantu Anda mengatasi masalah gateway. Anda tidak perlu port ini terbuka untuk operasi normal gateway Anda, tetapi diperlukan untuk pemecahan masalah.	

Dari	Ke	Protokol	Port	Bagaimana Digunakan
Storage Gateway VM	Server Protokol Waktu Jaringan (NTP)	UDP	123 (NTP)	<p>Digunakan oleh sistem lokal untuk menyinkronkan waktu VM ke waktu host. VM Storage Gateway dikonfigurasi untuk menggunakan server NTP berikut:</p> <ul style="list-style-type: none"> • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org
Peralatan Perangkat Keras Storage Gateway	Proksi Protokol Transfer Hypertext (HTTP)	TCP	8080 (HTTP)	Diperlukan sebentar untuk aktivasi.

Selain port umum, Tape Gateway juga membutuhkan port berikut.

Dari	Ke	Protokol	Port	Bagaimana Digunakan
Pemrakarsa iSCSI	Storage Gateway VM	TCP	3260 (iSCSI)	Dengan sistem lokal untuk terhubung ke target iSCSI yang diekspos oleh gateway.

Menghubungkan ke Gateway Anda

Setelah Anda memilih host dan menyebarkan VM gateway Anda, Anda menghubungkan dan mengaktifkan gateway Anda. Untuk melakukan ini, Anda memerlukan alamat IP VM gateway Anda. Anda mendapatkan alamat IP dari konsol lokal gateway Anda. Anda masuk ke konsol lokal dan mendapatkan alamat IP dari bagian atas halaman konsol.

Untuk gateway yang digunakan di lokasi, Anda juga bisa mendapatkan alamat IP dari hypervisor Anda. Untuk gateway Amazon EC2, Anda juga bisa mendapatkan alamat IP instans Amazon EC2 dari Amazon EC2 Management Console. Untuk mengetahui cara mendapatkan alamat IP gateway Anda, lihat salah satu dari berikut ini:

- Host VMware: [Mengakses Konsol Lokal Gateway dengan VMware ESXi](#)
- Host HyperV: [Akses Konsol Lokal Gateway dengan Microsoft Hyper-V](#)
- Host Mesin Virtual (KVM) berbasis Kernel Linux: [Mengakses Konsol Lokal Gateway dengan Linux KVM](#)
- Tuan rumah EC2: [Mendapatkan Alamat IP dari Host Amazon EC2](#)

Ketika Anda menemukan alamat IP, perhatikan itu. Kemudian kembali ke konsol Storage Gateway dan ketik alamat IP ke konsol.

Mendapatkan Alamat IP dari Host Amazon EC2

Untuk mendapatkan alamat IP instans Amazon EC2 gateway Anda digunakan, masuk ke konsol lokal instans EC2. Kemudian dapatkan alamat IP dari bagian atas halaman konsol. Untuk petunjuk, lihat [Masuk ke Konsol Lokal Amazon EC2 Gateway](#).

Anda juga bisa mendapatkan alamat IP dari Amazon EC2 Management Console. Kami merekomendasikan menggunakan alamat IP publik untuk aktivasi. Untuk mendapatkan alamat IP publik, gunakan prosedur 1. Jika Anda memilih untuk menggunakan alamat IP elastis sebagai gantinya, lihat prosedur 2.

Prosedur 1: Untuk terhubung ke gateway Anda menggunakan alamat IP publik

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi, pilih Instans, lalu pilih instans EC2 tempat gateway Anda digunakan.
3. Pilih tab Deskripsi di bagian bawah, lalu catat IP publik. Anda menggunakan alamat IP ini untuk terhubung ke gateway. Kembali ke konsol Storage Gateway dan ketik alamat IP.

Jika Anda ingin menggunakan alamat IP elastis untuk aktivasi, gunakan prosedur berikut.

Prosedur 2: Untuk terhubung ke gateway Anda menggunakan alamat IP elastis

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi, pilih Instans, lalu pilih instans EC2 tempat gateway Anda digunakan.
3. Pilih tab Deskripsi di bagian bawah, dan kemudian perhatikan nilai IP Elastis. Anda menggunakan alamat IP elastis ini untuk terhubung ke gateway. Kembali ke konsol Storage Gateway dan ketik alamat IP elastis.
4. Setelah gateway Anda diaktifkan, pilih gateway yang baru saja Anda aktifkan, lalu pilih tab perangkat VTL di panel bawah.
5. Dapatkan nama semua perangkat VTL Anda.
6. Untuk setiap target, jalankan perintah berikut untuk mengkonfigurasi target.

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. Untuk setiap target, jalankan perintah berikut untuk masuk.

```
iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
```

Gateway Anda sekarang terhubung menggunakan alamat IP elastis dari instans EC2.

Memahami Sumber Daya Storage Gateway dan ID Sumber Daya

Di Storage Gateway, sumber daya utama adalah gateway tetapi jenis sumber daya lainnya meliputi: volume, pita virtual, target iSCSI, dan perangkat vtl. Ini disebut sebagai subresource dan mereka tidak ada kecuali mereka terkait dengan gateway.

Sumber daya dan sub-sumber daya ini memiliki nama Amazon Resource Name (ARN) yang unik seperti yang ditunjukkan pada tabel berikut.

Jenis Sumber Daya	Format ARN
Gerbang ARN	<code>arn:aws:storagegateway: <i>region</i>:<i>account-id</i> :gateway/ <i>gateway-id</i></code>
Pita ARN	<code>arn:aws:storagegateway: <i>region</i>:<i>account-id</i> :tape/<i>tapebarcode</i></code>
Target ARN (target iSCSI)	<code>arn:aws:storagegateway: <i>region</i>:<i>account-id</i> :gateway/ <i>gateway-id</i> /target/<i>iSCSITarget</i></code>
Perangkat VTL ARN	<code>arn:aws:storagegateway: <i>region</i>:<i>account-id</i> :gateway/ <i>gateway-id</i> /device/<i>vtldevice</i></code>

Storage Gateway juga mendukung penggunaan instans EC2 serta volume dan snapshot EBS. Sumber daya ini adalah sumber daya Amazon EC2 yang digunakan di Storage Gateway.

Bekerja dengan ID Sumber Daya

Saat Anda membuat sumber daya, Storage Gateway menetapkan sumber daya ID sumber daya unik. ID sumber daya ini adalah bagian dari sumber daya ARN. ID sumber daya mengambil bentuk pengenal sumber daya, diikuti oleh tanda hubung, dan kombinasi unik dari delapan huruf dan angka. Misalnya, ID gateway adalah bentuk `sgw-12A3456B` di mana `sgw` adalah pengenal sumber daya

untuk gateway. ID volume mengambil bentuk di `vol-3344CCDD` mana `vol` adalah pengidentifikasi sumber daya untuk volume.

Untuk kaset virtual, Anda dapat menambahkan awalan hingga empat karakter ke ID barcode untuk membantu Anda mengatur kaset Anda.

ID sumber daya Storage Gateway dalam huruf besar. Namun, saat Anda menggunakan ID sumber daya ini dengan Amazon EC2 API, Amazon EC2 mengharapkan ID sumber daya dalam huruf kecil. Anda harus mengubah ID sumber daya Anda menjadi huruf kecil untuk menggunakannya dengan EC2 API. Misalnya, di Storage Gateway ID untuk volume mungkin `vol-1122AABB`. Saat Anda menggunakan ID ini dengan EC2 API, Anda harus mengubahnya menjadi `vol-1122aabb`. Jika tidak, API EC2 mungkin tidak berperilaku seperti yang diharapkan.

Menandai Sumber Daya Storage Gateway

Di Storage Gateway, Anda dapat menggunakan tag untuk mengelola sumber daya Anda. Tag memungkinkan Anda menambahkan metadata ke sumber daya Anda dan mengkategorikan sumber daya Anda agar lebih mudah dikelola. Setiap tag terdiri dari pasangan kunci-nilai, yang Anda tentukan. Anda dapat menambahkan tag ke gateway, volume, dan kaset virtual. Anda dapat mencari dan memfilter sumber daya ini berdasarkan tag yang Anda tambahkan.

Sebagai contoh, Anda dapat menggunakan tag untuk mengidentifikasi sumber daya Storage Gateway yang digunakan oleh setiap departemen di organisasi Anda. Anda dapat menandai gateway dan volume yang digunakan oleh departemen akuntansi Anda seperti ini: (`key=departmentdanvalue=accounting`). Anda kemudian dapat memfilter dengan tag ini untuk mengidentifikasi semua gateway dan volume yang digunakan oleh departemen akuntansi Anda dan menggunakan informasi untuk menentukan biaya. Untuk informasi selengkapnya, lihat [Menggunakan Tag Alokasi Biaya](#) dan [Bekerja dengan Editor Tag](#).

Jika Anda mengarsipkan rekaman virtual yang ditandai, rekaman itu mempertahankan tagnya di arsip. Demikian pula, jika Anda mengambil rekaman dari arsip ke gateway lain, tag dipertahankan di gateway baru.

Tag tidak memiliki arti semantik melainkan ditafsirkan sebagai string karakter.

Pembatasan berikut berlaku untuk tag:

- Kunci dan nilai tanda peka huruf besar dan kecil.
- Jumlah maksimum tag untuk setiap sumber daya adalah 50.

- Kunci tag tidak dapat dimulai dengan `aws` : . Awalan ini dicadangkan untuk AWS digunakan.
- Karakter yang valid untuk properti kunci adalah huruf dan angka UTF-8, spasi, dan karakter khusus `+ - = . _ /` dan `@`.

Bekerja dengan Tag

Anda dapat bekerja dengan tag dengan menggunakan konsol Storage Gateway, Storage Gateway API, atau [Storage Gateway Command Line Interface \(CLI\)](#). Prosedur berikut menunjukkan cara menambahkan, mengedit, dan menghapus tag di konsol.

Untuk menambahkan tag

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Di panel navigasi, pilih sumber daya yang ingin Anda tag.

Misalnya, untuk menandai gateway, pilih Gateway, lalu pilih gateway yang ingin Anda tag dari daftar gateway.

3. Pilih Tag, lalu pilih Tambah/edit tag.
4. Dalam kotak dialog Tambah/edit tag, pilih Buat tag.
5. Ketik kunci untuk Kunci dan nilai untuk Nilai. Misalnya, Anda dapat mengetik **Department** kunci dan **Accounting** nilainya.

Note

Anda dapat membiarkan kotak Nilai kosong.

6. Pilih Buat Tag untuk menambahkan lebih banyak tag. Anda dapat menambahkan beberapa tag ke sumber daya.
7. Setelah selesai menambahkan tag, pilih Simpan.

Untuk mengedit tag

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Pilih sumber daya yang tagnya ingin Anda edit.
3. Pilih Tag untuk membuka kotak dialog Tambah/edit tag.
4. Pilih ikon pensil di sebelah tag yang ingin Anda edit, lalu edit tag.

5. Setelah selesai mengedit tag, pilih Simpan.

Untuk menghapus tanda

1. Buka konsol Storage Gateway di <https://console.aws.amazon.com/storagegateway/home>.
2. Pilih sumber daya yang tagnya ingin Anda hapus.
3. Pilih Tag, lalu pilih Tambah/edit tag untuk membuka kotak dialog Tambah/edit tag.
4. Pilih ikon X di sebelah tag yang ingin Anda hapus, lalu pilih Simpan.

Bekerja dengan Komponen Sumber Terbuka untuk AWS Storage Gateway

Bagian ini menjelaskan alat dan lisensi pihak ketiga yang kami andalkan untuk memberikan fungsionalitas Storage Gateway.

Kode sumber untuk komponen perangkat lunak sumber terbuka tertentu yang disertakan dengan AWS Storage Gateway perangkat lunak tersedia untuk diunduh di lokasi berikut:

- [Untuk gateway yang digunakan di VMware ESXi, unduh sources.tar](#)
- [Untuk gateway yang digunakan di Microsoft Hyper-V, unduh sources_hyperv.tar](#)
- [Untuk gateway yang digunakan pada Mesin Virtual berbasis Kernel Linux \(KVM\), unduh sources_KVM.tar](#)

[Produk ini mencakup perangkat lunak yang dikembangkan oleh Proyek OpenSSL untuk digunakan dalam OpenSSL Toolkit \(<http://www.openssl.org/>\)](#). Untuk lisensi yang relevan untuk semua alat pihak ketiga yang bergantung, lihat [Lisensi Pihak Ketiga](#).

AWS Storage Gateway kuota

Dalam topik ini, Anda dapat menemukan informasi tentang kuota volume dan pita, konfigurasi, dan batas kinerja untuk Storage Gateway.

Topik

- [Kuota untuk kaset](#)

- [Ukuran disk lokal yang direkomendasikan untuk gateway Anda](#)

Kuota untuk kaset

Tabel berikut mencantumkan kuota untuk kaset.

Deskripsi	Gerbang Pita
Ukuran minimum pita virtual	100 GiB
Ukuran maksimum pita virtual	15 TiB
Jumlah maksimum kaset virtual yang ditetapkan ke gateway	1.500
Ukuran total semua kaset yang ditetapkan ke gateway	1 PiB
Jumlah maksimum kaset virtual dalam arsip	Tidak ada batas
Ukuran total semua kaset dalam arsip	Tidak ada batas

Ukuran disk lokal yang direkomendasikan untuk gateway Anda

Tabel berikut merekomendasikan ukuran untuk penyimpanan disk lokal untuk gateway yang Anda gunakan.

Jenis Gateway	Cache (Minimum)	Cache (Maksimum)	Unggah Buffer (Minimum)	Unggah Buffer (Maksimum)	Disk Lokal Lain yang Diperlukan
Gerbang pita	150 GiB	64 TiB	150 GiB	2 TiB	—

Note

Anda dapat mengonfigurasi satu atau lebih drive lokal untuk cache Anda dan mengunggah buffer, hingga kapasitas maksimum.

Saat menambahkan cache atau mengunggah buffer ke gateway yang ada, penting untuk membuat disk baru di host Anda (hypervisor atau instans Amazon EC2). Jangan mengubah ukuran disk yang ada jika disk sebelumnya telah dialokasikan sebagai cache atau buffer unggahan.

Referensi API untuk Storage Gateway

Selain menggunakan konsol, Anda dapat menggunakan AWS Storage Gateway API untuk mengonfigurasi dan mengelola gateway secara terprogram. Bagian ini menjelaskan AWS Storage Gateway operasi, penandatanganan permintaan untuk otentikasi, dan penanganan kesalahan. Untuk informasi tentang wilayah dan titik akhir yang tersedia untuk Storage Gateway, lihat [AWS Storage Gateway Endpoints dan Quotas](#) di Referensi Umum AWS

Note

Anda juga dapat menggunakan AWS SDK saat mengembangkan aplikasi dengan AWS Storage Gateway. AWS SDK untuk Java, .NET, dan PHP membungkus AWS Storage Gateway API yang mendasarinya, menyederhanakan tugas pemrograman Anda. Untuk informasi tentang mengunduh pustaka SDK, lihat [Pustaka Kode Contoh](#).

Topik

- [Header Permintaan yang Diperlukan Storage Gateway](#)
- [Menandatangani Permintaan](#)
- [Respons Kesalahan](#)
- [Tindakan](#)

Header Permintaan yang Diperlukan Storage Gateway

Bagian ini menjelaskan header yang diperlukan yang harus Anda kirim dengan setiap permintaan POST ke Storage Gateway. Anda menyertakan header HTTP untuk mengidentifikasi informasi kunci tentang permintaan termasuk operasi yang ingin Anda panggil, tanggal permintaan, dan informasi yang menunjukkan otorisasi Anda sebagai pengirim permintaan. Header tidak peka huruf besar/kecil dan urutan header tidak penting.

Contoh berikut menunjukkan header yang digunakan dalam [ActivateGateway](#) operasi.

```
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
```

Berikut ini adalah header yang harus disertakan dengan permintaan POST Anda ke Storage Gateway. Header yang ditampilkan di bawah ini yang dimulai dengan “x-amz” adalah AWS header -specific. Semua header lain yang terdaftar adalah header umum yang digunakan dalam transaksi HTTP.

Header	Deskripsi
Authorization	<p>Header otorisasi berisi beberapa informasi tentang permintaan yang memungkinkan Storage Gateway untuk menentukan apakah permintaan tersebut merupakan tindakan yang valid untuk pemohon. Format header ini adalah sebagai berikut (jeda baris ditambahkan untuk keterbacaan):</p> <pre>Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd/region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i></pre> <p>Dalam sintaks sebelumnya, Anda menentukan, tahun, bulan <i>YourAccessKey</i>, dan hari (<i>yyyymmdd</i>), wilayah, dan <i>CalculatedSignature</i> Format header otorisasi ditentukan oleh persyaratan proses Penandatanganan AWS V4. Rincian penandatanganan dibahas dalam topik Menandatangani Permintaan.</p>
Content-Type	<p>Gunakan <code>application/x-amz-json-1.1</code> sebagai tipe konten untuk semua permintaan ke Storage Gateway.</p> <pre>Content-Type: application/x-amz-json-1.1</pre>

Header	Deskripsi
Host	<p>Gunakan header host untuk menentukan titik akhir Storage Gateway tempat Anda mengirim permintaan. Misalnya, <code>storagegateway.us-east-2.amazonaws.com</code> adalah titik akhir untuk wilayah AS Timur (Ohio). Untuk informasi selengkapnya tentang titik akhir yang tersedia untuk Storage Gateway, lihat AWS Storage Gateway Endpoints dan Quota di Referensi Umum AWS</p> <pre data-bbox="472 569 1507 646">Host: storagegateway. <i>region</i>.amazonaws.com</pre>
x-amz-date	<p>Anda harus memberikan cap waktu baik di Date header HTTP atau AWS <code>x-amz-date</code> header. (Beberapa pustaka klien HTTP tidak mengizinkan Anda mengatur Date header.) Saat <code>x-amz-date</code> header hadir, Storage Gateway mengabaikan Date header apa pun selama otentikasi permintaan. Formatnya harus ISO8601 Basic <code>x-amz-date</code> dalam format <code>YYYYMMDD'T'HHMMSS'Z'</code>. Jika kedua Date dan <code>x-amz-date</code> header digunakan, format header Tanggal tidak harus ISO8601.</p> <pre data-bbox="472 1079 1507 1157">x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>
x-amz-target	<p>Header ini menentukan versi API dan operasi yang Anda minta. Nilai header target dibentuk dengan menggabungkan versi API dengan nama API dan dalam format berikut.</p> <pre data-bbox="472 1398 1507 1476">x-amz-target: StorageGateway_ <i>APIversion</i> .<i>operationName</i></pre> <p>Nilai <code>operationName</code> (misalnya <code>ActivateGateway</code> "") dapat ditemukan dari daftar API, Referensi API untuk Storage Gateway</p>

Menandatangani Permintaan

Storage Gateway mengharuskan Anda mengautentikasi setiap permintaan yang Anda kirim dengan menandatangani permintaan. Untuk menandatangani permintaan, Anda menghitung tanda tangan

digital menggunakan fungsi hash kriptografi. Hash kriptografi adalah fungsi yang mengembalikan nilai hash unik berdasarkan input. Input ke fungsi hash termasuk teks permintaan Anda dan secret access key Anda. Fungsi hash mengembalikan nilai hash yang Anda sertakan dalam permintaan sebagai tanda tangan Anda. Tanda tangan adalah bagian header `Authorization` dari permintaan Anda.

Setelah menerima permintaan Anda, Storage Gateway menghitung ulang tanda tangan menggunakan fungsi hash yang sama dan input yang Anda gunakan untuk menandatangani permintaan. Jika tanda tangan yang dihasilkan cocok dengan tanda tangan dalam permintaan, Storage Gateway akan memproses permintaan tersebut. Jika tidak, permintaan ditolak.

Storage Gateway mendukung otentikasi menggunakan [AWS Signature Version 4](#). Proses untuk menghitung tanda tangan dapat dibagi menjadi tiga tugas:

- [Tugas 1: Buat Permintaan Canonical](#)

Atur ulang permintaan HTTP Anda ke dalam format kanonik. Menggunakan formulir kanonik diperlukan karena Storage Gateway menggunakan bentuk kanonik yang sama ketika menghitung ulang tanda tangan untuk dibandingkan dengan yang Anda kirim.

- [Tugas 2: Buat String untuk Ditandatangani](#)

Buat string yang akan Anda gunakan sebagai salah satu nilai input untuk fungsi hash kriptografi Anda. String, yang disebut string to sign, adalah rangkaian dari nama algoritme hash, tanggal permintaan, string cakupan kredensial, dan permintaan kanonikalisasi dari tugas sebelumnya. String lingkup kredensial itu sendiri adalah rangkaian informasi tanggal, wilayah, dan layanan.

- [Tugas 3: Buat Tanda Tangan](#)

Buat tanda tangan untuk permintaan Anda menggunakan fungsi hash kriptografi yang menerima dua string input: string to sign dan kunci turunan. Kunci turunan dihitung dengan memulai dengan kunci akses rahasia Anda dan menggunakan string cakupan kredensial untuk membuat serangkaian Kode Otentikasi Pesan Berbasis Hash (HMAC).

Contoh Perhitungan Tanda Tangan

Contoh berikut memandu Anda melalui detail pembuatan tanda tangan untuk [ListGateways](#). Contoh dapat digunakan sebagai referensi untuk memeriksa metode perhitungan tanda tangan Anda.

Perhitungan referensi lainnya disertakan dalam [Rangkaian Pengujian Signature Versi 4](#) dari Daftar Istilah Amazon Web Services.

Contoh tersebut mengasumsikan sebagai berikut:

- Cap waktu permintaan adalah "Senin, 10 Sep 2012 00:00:00" GMT.
- Titik akhirnya adalah wilayah AS Timur (Ohio).

Sintaks permintaan umum (termasuk isi JSON) adalah:

```
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
{}
```

Bentuk kanonik dari permintaan yang dihitung adalah: [Tugas 1: Buat Permintaan Canonical](#)

```
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
```

Baris terakhir dari permintaan kanonik adalah hash dari isi permintaan. Selain itu, perhatikan baris ketiga kosong dalam permintaan kanonik. Ini karena tidak ada parameter kueri untuk API ini (atau Storage Gateway API).

String yang akan ditandatangani [Tugas 2: Buat String untuk Ditandatangani](#) adalah:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```


Baris pertama dari string yang akan ditandatangani adalah algoritme, baris kedua adalah cap waktu, baris ketiga adalah ruang lingkup kredensi, dan baris terakhir adalah hash dari permintaan kanonik dari Tugas 1.

Untuk [Tugas 3: Buat Tanda Tangan](#), kunci turunan dapat direpresentasikan sebagai:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20120910"), "us-east-2"), "storagegateway"), "aws4_request")
```

Jika kunci akses rahasia, bPxRfi wjalrxutnfemi/k7mdeng/ CYEXAMPLEKEY, digunakan, maka tanda tangan yang dihitung adalah:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Langkah terakhir adalah membangun header `Authorization`. Untuk kunci akses demonstrasi AKIAIOSFODNN7EXAMPLE, header (dengan jeda baris ditambahkan untuk keterbacaan) adalah:

```
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
```

Respons Kesalahan

Topik

- [Pengecualian](#)
- [Kode Kesalahan Operasi](#)
- [Respons Kesalahan](#)

Bagian ini memberikan informasi referensi tentang AWS Storage Gateway kesalahan. Kesalahan ini diwakili oleh pengecualian kesalahan dan kode kesalahan operasi. Misalnya, pengecualian kesalahan dikembalikan `InvalidSignatureException` oleh respons API apa pun jika ada masalah dengan tanda tangan permintaan. Namun, kode kesalahan operasi `ActivationKeyInvalid` dikembalikan hanya untuk [ActivateGatewayAPI](#).

Bergantung pada jenis kesalahannya, Storage Gateway hanya dapat mengembalikan pengecualian, atau mungkin mengembalikan pengecualian dan kode kesalahan operasi. Contoh respons kesalahan ditampilkan di [Respons Kesalahan](#).

Pengecualian

Tabel berikut mencantumkan pengecualian AWS Storage Gateway API. Ketika sebuah AWS Storage Gateway operasi mengembalikan respons kesalahan, badan respons berisi salah satu pengecualian ini. `InternalServerError` dan `InvalidGatewayRequestException` mengembalikan salah satu kode [Kode Kesalahan Operasi](#) pesan kode kesalahan operasi yang memberikan kode kesalahan operasi tertentu.

Pengecualian	Pesan	Kode Status HTTP
<code>IncompleteSignatureException</code>	Tanda tangan yang ditentukan tidak lengkap.	400 Permintaan Buruk
<code>InternalFailure</code>	Pemrosesan permintaan gagal karena beberapa kesalahan, pengecualian, atau kegagalan yang tidak diketahui.	500 Kesalahan Server Internal
<code>InternalServerError</code>	Salah satu pesan kode kesalahan operasi Kode Kesalahan Operasi .	500 Kesalahan Server Internal
<code>InvalidAction</code>	Tindakan atau operasi yang diminta tidak valid.	400 Permintaan Buruk
<code>InvalidClientTokenId</code>	Sertifikat X.509 atau ID Kunci AWS Akses yang disediakan tidak ada dalam catatan kami.	403 Dilarang
<code>InvalidGatewayRequestException</code>	Salah satu pesan kode kesalahan operasi di Kode Kesalahan Operasi .	400 Permintaan Buruk
<code>InvalidSignatureException</code>	Tanda tangan permintaan yang kami hitung tidak sesuai dengan tanda tangan yang Anda berikan. Periksa Kunci AWS Akses dan metode penandatanganan.	400 Permintaan Buruk

Pengecualian	Pesan	Kode Status HTTP
MissingAction	Permintaan tidak memiliki parameter tindakan atau operasi.	400 Permintaan Buruk
MissingAuthenticationToken	Permintaan harus berisi ID Kunci AWS Akses yang valid (terdaftar) atau sertifikat X.509.	403 Dilarang
RequestExpired	Permintaan telah melewati tanggal kedaluwarsa atau tanggal permintaan (baik dengan padding 15 menit), atau tanggal permintaan terjadi lebih dari 15 menit di masa mendatang.	400 Permintaan Buruk
SerializationException	Terjadi kesalahan selama serialisasi. Periksa apakah muatan JSON Anda terbentuk dengan baik.	400 Permintaan Buruk
ServiceUnavailable	Permintaan telah gagal karena kegagalan sementara server.	503 Layanan Tidak Tersedia
SubscriptionRequiredException	AWS Access Key Id memerlukan langganan untuk layanan ini.	400 Permintaan Buruk
ThrottlingException	Tarif terlampaui.	400 Permintaan Buruk
UnknownOperationException	Operasi yang tidak diketahui ditentukan. Operasi yang valid tercantum dalam Operasi di Storage Gateway .	400 Permintaan Buruk
UnrecognizedClientException	Token keamanan yang termasuk dalam permintaan tidak valid.	400 Permintaan Buruk
ValidationException	Nilai parameter input buruk atau di luar jangkauan.	400 Permintaan Buruk

Kode Kesalahan Operasi

Tabel berikut menunjukkan pemetaan antara kode kesalahan AWS Storage Gateway operasi dan API yang dapat mengembalikan kode. Semua kode kesalahan operasi dikembalikan dengan salah satu dari dua pengecualian umum— `InternalServerError` dan `InvalidGatewayRequestException` —dijelaskan dalam [Pengecualian](#)

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
<code>ActivationKeyExpired</code>	Kunci aktivasi yang ditentukan telah kedaluwarsa.	ActivateGateway
<code>ActivationKeyInvalid</code>	Kunci aktivasi yang ditentukan tidak valid.	ActivateGateway
<code>ActivationKeyNotFound</code>	Kunci aktivasi yang ditentukan tidak ditemukan.	ActivateGateway
<code>BandwidthThrottleScheduleNotFound</code>	Throttle bandwidth yang ditentukan tidak ditemukan.	DeleteBandwidthRateLimit
<code>CannotExportSnapshot</code>	Snapshot yang ditentukan tidak dapat diekspor.	CreateCachediSCSIVolume CreateStorediSCSIVolume
<code>InitiatorNotFound</code>	Inisiator yang ditentukan tidak ditemukan.	DeleteChapCredentials
<code>DiskAlreadyAllocated</code>	Disk yang ditentukan sudah dialokasikan.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
DiskDoesNotExist	Disk yang ditentukan tidak ada.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	Disk yang ditentukan tidak selaras dengan gigabyte.	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	Ukuran disk yang ditentukan lebih besar dari ukuran volume maksimum.	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	Ukuran disk yang ditentukan kurang dari ukuran volume.	CreateStorediSCSIVolume
DuplicateCertificateInfo	Informasi sertifikat yang ditentukan adalah duplikat.	ActivateGateway

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
GatewayInternalError	Terjadi kesalahan internal gateway.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolume DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolume DescribeWorkingStorage ListLocalDisks

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
GatewayNotConnected	Gateway yang ditentukan tidak terhubung.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolume DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolume DescribeWorkingStorage ListLocalDisks

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
GatewayNotFound	Gateway yang ditentukan tidak ditemukan.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolume DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolume DescribeWorkingStorage

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
GatewayProxyNetworkConnectionBusy	Koneksi jaringan proxy gateway yang ditentukan sibuk.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolume DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolume DescribeWorkingStorage ListLocalDisks

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
InternalError	Terjadi kesalahan internal.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolume DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
InvalidParameters	Permintaan yang ditentukan berisi parameter yang salah.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolume DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	Batas penyimpanan lokal terlampaui.	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	LUN yang ditentukan tidak benar.	CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
MaximumVolumeCount Exceeded	Jumlah volume maksimum terlampaui.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolume DescribeStorediSCSIVolume
NetworkConfigurationChanged	Konfigurasi jaringan gateway telah berubah.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
NotSupported	Operasi yang ditentukan tidak didukung.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolume DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	Gateway yang ditentukan sudah kedaluwarsa.	ActivateGateway
SnapshotInProgressException	Snapshot yang ditentukan sedang berlangsung.	DeleteVolume
SnapshotIdInvalid	Snapshot yang ditentukan tidak valid.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
StagingAreaFull	Area pementasan penuh.	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetAlreadyExists	Target yang ditentukan sudah ada.	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	Target yang ditentukan tidak valid.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	Target yang ditentukan tidak ditemukan.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
UnsupportedOperationForGatewayType	Operasi yang ditentukan tidak valid untuk jenis gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolume DescribeStorediSCSIVolume DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	Volume yang ditentukan sudah ada.	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	Volume yang ditentukan tidak valid.	DeleteVolume
VolumeInUse	Volume yang ditentukan sudah digunakan.	DeleteVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
VolumeNotFound	Volume yang ditentukan tidak ditemukan.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolume DescribeSnapshotSchedule DescribeStorediSCSIVolume UpdateSnapshotSchedule
VolumeNotReady	Volume yang ditentukan belum siap.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Respons Kesalahan

Ketika ada kesalahan, informasi header respons berisi:

- Tipe Konten: aplikasi/ -1.1 x-amz-json
- Kode status yang sesuai 4xx atau 5xx HTTP

Tubuh respons kesalahan berisi informasi tentang kesalahan yang terjadi. Contoh respon kesalahan berikut menunjukkan sintaks output elemen respon umum untuk semua respon kesalahan.

```
{
  "__type": "String",
  "message": "String",
  "error":
    { "errorCode": "String",
      "errorDetails": "String"
    }
}
```

```
}
```

Tabel berikut menjelaskan bidang respons kesalahan JSON yang ditunjukkan dalam sintaks sebelumnya.

__jenis

Salah satu pengecualian dari [Pengecualian](#).

Tipe: String

kesalahan

Berisi detail kesalahan khusus API. Dalam kesalahan umum (yaitu, tidak spesifik untuk API apa pun), informasi kesalahan ini tidak ditampilkan.

Jenis: Koleksi

ErrorCode

Salah satu kode kesalahan operasi.

Tipe: String

Rincian Kesalahan

Bidang ini tidak digunakan dalam versi API saat ini.

Tipe: String

message

Salah satu pesan kode kesalahan operasi.

Tipe: String

Contoh Respon Kesalahan

Badan JSON berikut dikembalikan jika Anda menggunakan DescribeStoredi SCSI Volumes API dan menentukan input permintaan ARN gateway yang tidak ada.

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
}
```



```
"error": {
  "errorCode": "VolumeNotFound"
}
```

Badan JSON berikut dikembalikan jika Storage Gateway menghitung tanda tangan yang tidak cocok dengan tanda tangan yang dikirim dengan permintaan.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
provided."
}
```

Operasi di Storage Gateway

Untuk daftar operasi Storage Gateway, lihat [Tindakan](#) di Referensi AWS Storage Gateway API.

Riwayat dokumen untuk Panduan Pengguna Tape Gateway

- Versi API: 2013-06-30
- Pembaruan dokumentasi terbaru: November 24, 2020

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS Storage Gateway Pengguna setelah April 2018. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Dukungan usang untuk Tape Gateway di Snowball Edge	Tidak mungkin lagi meng-host Tape Gateway di perangkat Snowball Edge.	Maret 14, 2024
Instruksi yang diperbarui untuk menguji pengaturan gateway Anda menggunakan aplikasi pihak ke-3	Petunjuk untuk menguji penyiapan gateway Anda menggunakan aplikasi pihak ketiga sekarang menjelaskan perilaku yang diharapkan jika gateway Anda dimulai ulang selama pekerjaan pencadangan yang sedang berlangsung. Untuk informasi selengkapnya, lihat Menggunakan Perangkat Lunak Cadangan untuk Menguji Pengaturan Gateway Anda .	24 Oktober 2023
CloudWatch Alarm yang direkomendasikan diperbarui	CloudWatch HealthNotifications Alarm sekarang berlaku untuk dan direkomendasikan untuk semua jenis gateway dan platform host. Pengaturan konfigurasi yang disaranka	2 Oktober 2023

	<p>n juga telah diperbarui untuk HealthNotifications danAvailabilityNotifi cations . Untuk informasi selengkapnya lihat Memahami CloudWatch alarm .</p>	
<p>Peningkatan ukuran pita maksimum menjadi 15 TiB untuk Tape Gateways</p>	<p>Untuk Tape Gateways, ukuran maksimum pita virtual sekarang ditingkatkan dari 5 TiB menjadi 15 TiB. Untuk informasi selengkapnya, lihat Kuota untuk Kaset di Panduan Pengguna Storage Gateway. .</p>	<p>4 Oktober 2022</p>
<p>Panduan Pengguna Pita dan Volume Gateway Terpisah</p>	<p>Panduan Pengguna Storage Gateway, yang sebelumnya berisi informasi tentang jenis tape dan Volume Gateway, telah dibagi menjadi Panduan Pengguna Tape Gateway dan Panduan Pengguna Volume Gateway, masing-masing berisi informasi hanya pada satu jenis gateway. Untuk informasi selengkapnya, lihat Panduan Pengguna Tape Gateway dan Panduan Pengguna Volume Gateway.</p>	<p>Maret 23, 2022</p>
<p>Prosedur pembuatan gateway yang diperbarui</p>	<p>Prosedur untuk membuat semua jenis gateway menggunakan konsol Storage Gateway telah diperbarui. Untuk informasi selengkapnya, lihat Membuat Gateway Anda .</p>	<p>18 Januari 2022</p>

[Antarmuka Tapes baru](#)

Halaman ikhtisar Tape di AWS Storage Gateway konsol telah diperbarui dengan fitur pencarian dan pemfilteran baru. Semua prosedur yang relevan dalam panduan ini telah diperbarui untuk menggambarkan fungsionalitas baru. Untuk informasi selengkapnya, lihat [Mengelola Gateway Tape Anda](#).

September 23, 2021

[Support untuk Quest NetVault Backup 13 untuk Tape Gateway](#)

Tape Gateways sekarang mendukung Quest NetVault Backup 13 yang berjalan di Microsoft Windows Server 2012 R2 atau Microsoft Windows Server 2016. Untuk informasi selengkapnya, lihat [Menguji Pengaturan Anda dengan Menggunakan NetVault Cadangan Quest](#).

Agustus 22, 2021

[Topik Gateway File S3 dihapus dari panduan Tape dan Volume Gateway](#)

Untuk membantu membuat panduan pengguna untuk Tape Gateway dan Volume Gateway lebih mudah diikuti bagi pelanggan yang menyiapkan jenis gateway masing-masing, beberapa topik yang tidak perlu telah dihapus.

21 Juli 2021

[Support untuk IBM Spectrum Protect 8.1.10 pada Windows dan Linux untuk Tape Gateway](#)

Tape Gateways sekarang mendukung IBM Spectrum Protect versi 8.1.10 yang berjalan di Microsoft Windows Server dan Linux. Untuk informasi selengkapnya, lihat [Menguji Pengaturan Anda dengan Menggunakan IBM Spectrum Protect](#).

24 November 2020

[Kepatuhan FedRAMP](#)

Storage Gateway sekarang sesuai dengan FedRAMP. Untuk informasi selengkapnya, lihat Validasi [kepatuhan untuk validasi Kepatuhan Storage Gateway](#) Gateway.

24 November 2020

[Pelambatan bandwidth berbasis jadwal](#)

Storage Gateway sekarang mendukung pembatasan bandwidth berbasis jadwal untuk tape dan Volume Gateways. Untuk informasi selengkapnya, lihat [Penjadwalan pembatasan bandwidth menggunakan konsol Storage Gateway](#) konsol Storage Gateway.

9 November 2020

[Volume cache dan penyimpanan cache lokal Tape Gateways meningkat 4x](#)

Storage Gateway sekarang mendukung cache lokal hingga 64 TB untuk volume cache dan Tape Gateways, meningkatkan kinerja untuk aplikasi lokal dengan menyediakan akses latensi rendah ke kumpulan data kerja yang lebih besar. Untuk informasi selengkapnya, lihat [Ukuran disk lokal yang direkomendasikan untuk gateway Anda](#) .

9 November 2020

[Migrasi gerbang](#)

Storage Gateway sekarang mendukung migrasi Volume Gateways yang di-cache ke mesin virtual baru. Untuk informasi selengkapnya, lihat [Memindahkan Volume Cached ke Mesin Virtual Gateway Volume Cached Baru](#) .

10 September 2020

[Support untuk tape retention lock dan write-once-read-many \(WORM\) tape protection](#)

Storage Gateway mendukung kunci retensi pita pada kaset virtual dan menulis setelah membaca banyak (WORM). Kunci retensi pita memungkinkan Anda menentukan mode dan periode retensi pada kaset virtual yang diarsipkan, mencegahnya dihapus untuk jangka waktu tetap hingga 100 tahun. Ini termasuk kontrol izin tentang siapa yang dapat menghapus kaset atau mengubah pengaturan retensi. Untuk informasi selengkapnya, lihat [Menggunakan Kunci Retensi Tape](#). Kaset virtual yang diaktifkan cacing membantu memastikan bahwa data pada kaset aktif di pustaka rekaman virtual Anda tidak dapat ditimpa atau dihapus. Untuk informasi selengkapnya, lihat [Write Once, Read Many \(WORM\) Tape Protection](#).

19 Agustus 2020

[Pesan alat perangkat keras melalui konsol](#)

Anda sekarang dapat memesan alat perangkat keras melalui AWS Storage Gateway konsol. Untuk informasi selengkapnya, lihat [Menggunakan Storage Gateway Hardware Appliance](#).

12 Agustus 2020

Dukungan untuk titik akhir Federal Information Processing Standard (FIPS) di Wilayah baru AWS	Anda sekarang dapat mengaktifkan gateway dengan titik akhir FIPS di Wilayah AS Timur (Ohio), AS Timur (Virginia N.), AS Barat (California), AS Barat (Oregon), dan Kanada (Tengah) Wilayah. Untuk informasi selengkapnya, lihat AWS Storage Gateway titik akhir dan kuota di. Referensi Umum AWS	31 Juli 2020
Migrasi gerbang	Storage Gateway sekarang mendukung migrasi tape dan menyimpan Volume Gateways ke mesin virtual baru. Untuk informasi selengkapnya, lihat Memindahkan Data Anda ke Gateway Baru .	31 Juli 2020
Lihat CloudWatch alarm Amazon di konsol Storage Gateway	Anda sekarang dapat melihat CloudWatch alarm di konsol Storage Gateway. Untuk informasi selengkapnya, lihat Memahami CloudWatch alarm	29 Mei 2020

[Dukungan untuk titik akhir
Federal Information Processin
g Standard \(FIPS\)](#)

Anda sekarang dapat mengaktifkan gateway dengan titik akhir FIPS di Wilayah. AWS GovCloud (US) Untuk memilih titik akhir FIPS untuk Volume Gateway, lihat [Memilih titik akhir layanan](#). Untuk memilih titik akhir FIPS untuk Tape Gateway, lihat [Connect Tape Gateway Anda ke](#). AWS

Mei 22, 2020

[AWS Daerah Baru](#)

Storage Gateway sekarang tersedia di Wilayah Afrika (Cape Town) dan Eropa (Milan). Untuk informasi selengkapnya, lihat [AWS Storage Gateway titik akhir dan kuota](#) di. Referensi Umum AWS

7 Mei 2020

[Support untuk kelas penyimpanan S3 Intelligent-Tiering](#)

Storage Gateway sekarang mendukung kelas penyimpanan S3 Intelligent-Tiering. Kelas penyimpanan S3 Intelligent-Tiering mengoptimalkan biaya penyimpanan dengan memindahkan data secara otomatis ke tingkat akses penyimpanan yang paling hemat biaya, tanpa dampak kinerja atau overhead operasional. Untuk informasi selengkapnya, lihat [Kelas penyimpanan untuk mengoptimalkan objek yang sering dan jarang diakses secara otomatis](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

30 April 2020

[Kinerja tulis dan baca Tape Gateway meningkat 2x](#)

Storage Gateway meningkatkan kinerja untuk membaca dari dan menulis ke kaset virtual di Tape Gateway sebesar 2x, memungkinkan Anda melakukan pencadangan dan pemulihan lebih cepat daripada sebelumnya. Untuk informasi selengkapnya, lihat [Panduan Kinerja untuk Tape Gateways](#) di Panduan Pengguna Storage Gateway.

23 April 2020

[Support untuk pembuatan tape otomatis](#)

Storage Gateway sekarang menyediakan kemampuan untuk secara otomatis membuat kaset virtual baru. Tape Gateway secara otomatis membuat kaset virtual baru untuk mempertahankan jumlah minimum kaset yang tersedia yang Anda konfigurasi dan kemudian membuat kaset baru ini tersedia untuk diimpor oleh aplikasi cadangan, memungkinkan pekerjaan pencadangan Anda berjalan tanpa gangguan. Untuk informasi selengkapnya, lihat [Membuat Kaset Secara Otomatis](#) di Panduan Pengguna Storage Gateway.

23 April 2020

[AWS Wilayah Baru](#)

Storage Gateway sekarang tersedia di Wilayah AWS GovCloud (AS-Timur). Untuk informasi selengkapnya, lihat [AWS Storage Gateway Titik Akhir dan Kuota](#) di Referensi Umum AWS

12 Maret 2020

[Support untuk hypervisor Virtual Machine \(KVM\) berbasis Kernel Linux](#)

Storage Gateway sekarang menyediakan kemampuan untuk menyebarkan gateway lokal pada platform virtualisasi KVM. Gateway yang digunakan di KVM memiliki semua fungsi dan fitur yang sama dengan gateway lokal yang ada. Untuk informasi selengkapnya, lihat [Hypervisor yang Didukung dan Persyaratan Host](#) di Panduan Pengguna Storage Gateway.

4 Februari 2020

[Support untuk VMware vSphere Ketersediaan Tinggi](#)

Storage Gateway sekarang menyediakan dukungan untuk ketersediaan tinggi di VMware untuk membantu melindungi beban kerja penyimpanan terhadap perangkat keras, hypervisor, atau kegagalan jaringan. Untuk informasi selengkapnya, lihat [Menggunakan VMware vSphere High Availability with Storage Gateway di Panduan Pengguna Storage Gateway](#). Rilis ini juga mencakup peningkatan kinerja. Untuk informasi selengkapnya, lihat [Performa](#) di Panduan Pengguna Storage Gateway.

20 November 2019

[AWS Wilayah Baru untuk Tape Gateway](#)

Tape Gateway sekarang tersedia di Wilayah Amerika Selatan (Sao Paulo). Untuk informasi selengkapnya, lihat [AWS Storage Gateway Titik Akhir dan Kuota](#) di. Referensi Umum AWS

24 September 2019

[Support untuk IBM Spectrum Protect versi 7.1.9 di Linux, dan untuk Tape Gateways peningkatan ukuran pita maksimum menjadi 5 TiB](#)

Tape Gateways sekarang mendukung IBM Spectrum Protect (Tivoli Storage Manager) versi 7.1.9 yang berjalan di Linux, selain berjalan di Microsoft Windows. Untuk informasi selengkapnya, lihat [Menguji Pengaturan Anda dengan Menggunakan IBM Spectrum Protect](#) di Panduan Pengguna Storage Gateway. . Juga, untuk Tape Gateways, ukuran maksimum pita virtual sekarang ditingkatkan dari 2,5 TiB menjadi 5 TiB. Untuk informasi selengkapnya, lihat [Kuota untuk Kaset](#) di Panduan Pengguna Storage Gateway. .

10 September 2019

[Support untuk Amazon CloudWatch Log](#)

Anda sekarang dapat mengonfigurasi File Gateways dengan Amazon CloudWatch Log Groups untuk mendapatkan pemberitahuan tentang kesalahan dan kesehatan gateway Anda dan sumber dayanya. Untuk informasi selengkapnya, lihat [Mendapatkan Pemberitahuan Tentang Kesehatan Gateway dan Kesalahan Dengan Grup CloudWatch Log Amazon](#) di Panduan Pengguna Storage Gateway.

4 September 2019

[AWS Wilayah Baru](#)

Storage Gateway sekarang tersedia di Wilayah Asia Pasifik (Hong Kong). Untuk informasi selengkapnya, lihat [AWS Storage Gateway Titik Akhir dan Kuota](#) di. Referensi Umum AWS

14 Agustus 2019

[AWS Wilayah Baru](#)

Storage Gateway sekarang tersedia di Wilayah Timur Tengah (Bahrain). Untuk informasi selengkapnya, lihat [AWS Storage Gateway Titik Akhir dan Kuota](#) di. Referensi Umum AWS

29 Juli 2019

[Support untuk mengaktifkan gateway di virtual private cloud \(VPC\)](#)

Anda sekarang dapat mengaktifkan gateway di VPC. Anda dapat membuat sambungan pribadi antara perangkat lunak lokal dan infrastruktur penyimpanan berbasis cloud. Untuk informasi selengkapnya, lihat [Mengaktifkan Gateway di Virtual Private Cloud](#).

20 Juni 2019

[Support untuk memindahkan kaset virtual dari S3 Glacier Flexible Retrieval ke S3 Glacier Deep Archive](#)

Anda sekarang dapat memindahkan kaset virtual Anda yang diarsipkan di kelas penyimpanan S3 Glacier Flexible Retrieval ke kelas penyimpanan S3 Glacier Deep Archive untuk penyimpanan data yang hemat biaya dan jangka panjang. Untuk informasi lebih lanjut, lihat [Memindahkan Tape dari S3 Glacier Flexible Retrieval ke S3 Glacier Deep Archive](#).

28 Mei 2019

[Dukungan berbagi file SMB untuk Microsoft Windows ACL](#)

Untuk File Gateways, Anda sekarang dapat menggunakan daftar kontrol akses Microsoft Windows (ACL) untuk mengontrol akses ke berbagi file Server Message Block (SMB). Untuk informasi selengkapnya, lihat [Menggunakan Microsoft Windows ACL untuk Mengontrol Akses ke Berbagi File SMB](#).

8 Mei 2019

[Integrasi dengan S3 Glacier Deep Archive](#)

Tape Gateway terintegrasi dengan S3 Glacier Deep Archive. Anda sekarang dapat mengarsipkan kaset virtual di S3 Glacier Deep Archive untuk retensi data jangka panjang. Untuk informasi selengkapnya, lihat [Mengarsipkan Kaset Virtual](#).

27 Maret 2019

[Ketersediaan Storage Gateway Hardware Appliance di Eropa](#)

Storage Gateway Hardware Appliance sekarang tersedia di Eropa. Untuk informasi selengkapnya, lihat [Wilayah Peralatan AWS Storage Gateway Perangkat Keras](#) di Referensi Umum AWS. Selain itu, Anda sekarang dapat meningkatkan penyimpanan yang dapat digunakan pada Storage Gateway Hardware Appliance dari 5 TB menjadi 12 TB dan mengganti kartu jaringan tembaga yang terpasang dengan kartu jaringan serat optik 10 Gigabit. Untuk informasi selengkapnya, lihat [Menyiapkan Peralatan Perangkat Keras Anda](#).

25 Februari 2019

[Integrasi dengan AWS Backup](#)

Storage Gateway terintegrasi dengan AWS Backup. Sekarang Anda dapat menggunakan AWS Backup untuk mencadangkan aplikasi bisnis lokal yang menggunakan volume Storage Gateway untuk penyimpanan yang didukung cloud. Untuk informasi selengkapnya, lihat [Mencadangkan Volume Anda](#).

16 Januari 2019

[Support untuk Bacula Enterprise dan IBM Spectrum Protect](#)

Tape Gateways sekarang mendukung Bacula Enterprise dan IBM Spectrum Protect. Storage Gateway juga sekarang mendukung versi yang lebih baru dari Veritas NetBackup, Veritas Backup Exec dan Quest backup. NetVault Anda sekarang dapat menggunakan aplikasi cadangan ini untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat [Menggunakan Perangkat Lunak Cadangan untuk Menguji Pengaturan Gateway Anda](#).

13 November 2018

[Support untuk Storage Gateway Hardware Appliance](#)

Storage Gateway Hardware Appliance mencakup perangkat lunak Storage Gateway yang sudah diinstal sebelumnya di server pihak ketiga. Anda dapat mengelola alat dari AWS Management Console. Alat ini dapat meng-host file, tape, dan Volume Gateways. Untuk informasi selengkapnya, lihat [Menggunakan Storage Gateway Hardware Appliance](#).

18 September 2018

[Kompatibilitas dengan Microsoft System Center 2016 Data Protection Manager \(DPM\)](#)

Tape Gateways sekarang kompatibel dengan Microsoft System Center 2016 Data Protection Manager (DPM). Anda sekarang dapat menggunakan Microsoft DPM untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat [Menguji Pengaturan Anda dengan Menggunakan Microsoft System Center Data Protection Manager](#).

18 Juli 2018

[Dukungan untuk protokol Server Message Block \(SMB\)](#)

File Gateways menambahkan dukungan untuk protokol Server Message Block (SMB) untuk berbagi file. Untuk informasi selengkapnya, lihat [Membuat Berbagi File](#).

20 Juni 2018

[Support untuk berbagi file, volume cache, dan enkripsi pita virtual](#)

Anda sekarang dapat menggunakan AWS Key Management Service (AWS KMS) untuk mengenkripsi data yang ditulis ke file share, cache volume, atau virtual tape. Saat ini, Anda dapat melakukan ini dengan menggunakan AWS Storage Gateway API. Untuk informasi selengkapnya, lihat [Enkripsi data menggunakan AWS KMS](#).

Juni 12, 2018

[Support NovaStor DataCenter untuk/Jaringan](#)

Tape Gateways sekarang mendukung /Network. NovaStor DataCenter Anda sekarang dapat menggunakan NovaStor DataCenter / Network versi 6.4 atau 7.1 untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat [Menguji Pengaturan Anda dengan Menggunakan NovaStor DataCenter / Jaringan](#).

24 Mei 2018

Pembaruan sebelumnya

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS Storage Gateway Pengguna sebelum Mei 2018.

Perubahan	Deskripsi	Tanggal Diubah
Support untuk kelas penyimpanan S3 One Zone_IA	Untuk File Gateways, Anda sekarang dapat memilih S3 One Zone_IA sebagai kelas penyimpanan default untuk berbagi file Anda. Dengan menggunakan kelas penyimpanan ini, Anda dapat menyimpan data objek Anda dalam satu Availability Zone di Amazon S3. Untuk informasi selengkapnya, lihat Membuat berbagi file .	4 April 2018
Wilayah Baru	Tape Gateway sekarang tersedia di Wilayah Asia Pasifik (Singapura). Untuk detail informasi, lihat AWS Daerah .	3 April 2018
Support untuk pemberitahuan cache refresh, pembayaran pemohon, dan ACL kalengan untuk bucket Amazon S3.	<p>Dengan File Gateways, Anda sekarang dapat diberi tahu saat gateway selesai menyegarkan cache untuk bucket Amazon S3 Anda. Untuk informasi selengkapnya, lihat RefreshCache.html di Referensi API Storage Gateway.</p> <p>File Gateways sekarang memungkinkan pemohon atau pembaca alih-alih pemilik bucket untuk membayar biaya akses.</p> <p>File Gateways sekarang memungkinkan Anda untuk memberikan kontrol penuh kepada pemilik bucket S3 yang memetakan ke berbagi file NFS.</p> <p>Untuk informasi selengkapnya, lihat Membuat berbagi file.</p>	1 Maret 2018
Support untuk Dell NetWorker EMC V9.x	Tape Gateways sekarang mendukung Dell EMC V9.x. NetWorker Anda sekarang dapat menggunakan Dell EMC NetWorker V9.x untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi	27 Februari 2018

Perubahan	Deskripsi	Tanggal Diubah
	selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Dell NetWorker EMC .	
Wilayah Baru	Storage Gateway sekarang tersedia di Wilayah Eropa (Paris). Untuk detail informasi, lihat AWS Daerah .	18 Desember 2017
Support untuk notifikasi unggahan file dan tebakan tipe MIME	<p>File Gateways sekarang dapat memberi tahu Anda ketika semua file yang ditulis ke berbagi file NFS Anda telah diunggah ke Amazon S3. Untuk informasi selengkapnya, lihat NotifyWhenUploaded di Referensi API Storage Gateway.</p> <p>File Gateways sekarang memungkinkan menebak jenis MIME untuk objek yang diunggah berdasarkan ekstensi file. Untuk informasi selengkapnya, lihat Membuat berbagi file.</p>	21 November 2017
Support untuk VMware ESXi Hypervisor versi 6.5	AWS Storage Gateway sekarang mendukung VMware ESXi Hypervisor versi 6.5. Ini adalah tambahan untuk versi 4.1, 5.0, 5.1, 5.5, dan 6.0. Untuk informasi selengkapnya, lihat Hypervisor dan persyaratan host yang didukung .	13 September 2017
Kompatibilitas dengan Commvault 11	Tape Gateways sekarang kompatibel dengan Commvault 11. Anda sekarang dapat menggunakan Commvault untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Commvault .	12 September 2017
Dukungan File Gateway untuk Microsoft Hyper-V hypervisor	Anda sekarang dapat menerapkan File Gateway pada hypervisor Microsoft Hyper-V. Untuk informasi, lihat Hypervisor dan persyaratan host yang didukung .	22 Juni 2017

Perubahan	Deskripsi	Tanggal Diubah
Support untuk pengambilan tape tiga hingga lima jam dari arsip	Untuk Tape Gateway, Anda sekarang dapat mengambil kaset Anda dari arsip dalam tiga hingga lima jam. Anda juga dapat menentukan jumlah data yang ditulis ke rekaman Anda dari aplikasi cadangan atau pustaka pita virtual (VTL) Anda. Untuk informasi selengkapnya, lihat Melihat Penggunaan Tape .	23 Mei 2017
Wilayah Baru	Storage Gateway sekarang tersedia di Wilayah Asia Pasifik (Mumbai). Untuk detail informasi, lihat AWS Daerah .	02 Mei 2017
Pembaruan untuk pengaturan berbagi file Support untuk penyegaran cache untuk berbagi file	File Gateways sekarang menambahkan opsi mount ke pengaturan berbagi file. Sekarang Anda dapat mengatur opsi squash dan read-only untuk berbagi file Anda. Untuk informasi selengkapnya, lihat Membuat berbagi file . File Gateways sekarang dapat menemukan objek di bucket Amazon S3 yang ditambahkan atau dihapus sejak gateway terakhir mencantumkan konten bucket dan menyimpan hasilnya dalam cache. Untuk informasi selengkapnya, lihat RefreshCached di Referensi API.	28 Maret 2017
Support untuk mengkloning volume	Untuk Volume Gateways yang di-cache, AWS Storage Gateway sekarang mendukung kemampuan untuk mengkloning volume dari volume yang ada. Untuk informasi selengkapnya, lihat Mengkloning Volume .	16 Maret 2017

Perubahan	Deskripsi	Tanggal Diubah
Dukungan untuk File Gateways di Amazon EC2	AWS Storage Gateway sekarang menyediakan kemampuan untuk menyebarkan File Gateway di Amazon EC2. Anda dapat meluncurkan File Gateway di Amazon EC2 menggunakan Storage Gateway Amazon Machine Image (AMI) yang sekarang tersedia sebagai AMI komunitas. Untuk informasi tentang cara membuat Gateway File dan menerapkannya pada instans EC2, lihat Membuat dan mengaktifkan Gateway File Amazon S3 atau Membuat dan mengaktifkan Amazon FSx File Gateway . Untuk informasi tentang cara meluncurkan AMI Gateway File, lihat Menerapkan Gateway File S3 di host Amazon EC2 atau Menerapkan Gateway File FSx di host Amazon EC2 .	Februari 08, 2017
Kompatibilitas dengan Arcserve 17	Tape Gateway sekarang kompatibel dengan Arcserve 17. Anda sekarang dapat menggunakan Arcserve untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke S3 Glacier Flexible Retrieval. Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Arcserve Backup r17.0 .	17 Januari 2017
Wilayah Baru	Storage Gateway sekarang tersedia di Wilayah UE (London). Untuk detail informasi, lihat AWS Daerah .	13 Desember 2016
Wilayah Baru	Storage Gateway sekarang tersedia di Wilayah Kanada (Tengah). Untuk detail informasi, lihat AWS Daerah .	Desember 08, 2016

Perubahan	Deskripsi	Tanggal Diubah
Support untuk File Gateway	Selain Volume Gateways dan Tape Gateway, Storage Gateway sekarang menyediakan File Gateway. File Gateway menggabungkan layanan dan perangkat lunak virtual, memungkinkan Anda untuk menyimpan dan mengambil objek di Amazon S3 menggunakan protokol file standar industri seperti Network File System (NFS). Gateway menyediakan akses ke objek di Amazon S3 sebagai file pada titik pemasangan NFS.	29 November 2016
Backup Exec 16	Tape Gateway sekarang kompatibel dengan Backup Exec 16. Anda sekarang dapat menggunakan Backup Exec 16 untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Veritas Backup Exec .	Selasa, 07 Nopember 2016
Kompatibilitas dengan Pelindung Data Fokus Mikro (HPE) 9.x	Tape Gateway sekarang kompatibel dengan Micro Focus (HPE) Data Protector 9.x. Anda sekarang dapat menggunakan HPE Data Protector untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke S3 Glacier Flexible Retrieval. Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Pelindung Data Micro Focus (HPE) .	2 November 2016
Wilayah Baru	Storage Gateway sekarang tersedia di Wilayah AS Timur (Ohio). Untuk detail informasi, lihat AWS Daerah .	17 Oktober 2016

Perubahan	Deskripsi	Tanggal Diubah
Desain ulang konsol Storage Gateway	Storage Gateway Management Console telah didesain ulang agar lebih mudah mengonfigurasi, mengelola, dan memantau gateway, volume, dan kaset virtual Anda. Antarmuka pengguna sekarang menyediakan tampilan yang dapat difilter dan menyediakan tautan langsung ke AWS layanan terintegrasi seperti CloudWatch dan Amazon EBS. Untuk informasi selengkapnya, lihat Mendaftar untuk AWS Storage Gateway .	30 Agustus 2016
Kompatibilitas dengan Veeam Backup & Replication V9 Update 2 atau yang lebih baru	Tape Gateway sekarang kompatibel dengan Veeam Backup & Replication V9 Update 2 atau yang lebih baru (yaitu, versi 9.0.0.1715 atau yang lebih baru). Anda sekarang dapat menggunakan Veeam Backup Replication V9 Update 2 atau yang lebih baru untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Cadangan & Replikasi Veeam .	Agustus 15, 2016
ID volume dan snapshot yang lebih panjang	Storage Gateway memperkenalkan ID yang lebih panjang untuk volume dan snapshot. Anda dapat mengaktifkan format ID yang lebih panjang untuk volume, snapshot, dan AWS sumber daya lain yang didukung. Untuk informasi selengkapnya, lihat Memahami Sumber Daya Storage Gateway dan ID Sumber Daya .	25 April 2016

Perubahan	Deskripsi	Tanggal Diubah
<p>Wilayah Baru</p> <p>Support untuk penyimpanan hingga ukuran 512 TiB untuk volume yang disimpan</p> <p>Pembaruan dan penyempurnaan gateway lainnya ke konsol lokal Storage Gateway</p>	<p>Tape Gateway sekarang tersedia di Wilayah Asia Pasifik (Seoul). Untuk informasi selengkapnya, lihat AWS Daerah.</p> <p>Untuk volume tersimpan, Anda sekarang dapat membuat hingga 32 volume penyimpanan hingga 16 TiB dalam ukuran masing-masing, untuk penyimpanan maksimum 512 TiB. Untuk informasi selengkapnya, lihat Arsitektur volume tersimpan dan AWS Storage Gateway kuota.</p> <p>Ukuran total semua kaset di perpustakaan pita virtual ditingkatkan menjadi 1 PiB. Untuk informasi selengkapnya, lihat AWS Storage Gateway kuota.</p> <p>Sekarang Anda dapat mengatur kata sandi untuk konsol lokal VM Anda di Storage Gateway Console. Untuk informasi, lihat Mengatur Kata Sandi Konsol Lokal dari Storage Gateway Console.</p>	<p>21 Maret 2016</p>
<p>Kompatibilitas dengan Dell EMC 8.x NetWorker</p>	<p>Tape Gateway sekarang kompatibel dengan Dell EMC 8.x NetWorker . Anda sekarang dapat menggunakan Dell EMC NetWorker untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Dell NetWorker EMC.</p>	<p>29 Februari 2016</p>

Perubahan	Deskripsi	Tanggal Diubah
Support untuk VMware ESXi Hypervisor versi 6.0 dan inisiator Red Hat Enterprise Linux 7 iSCSI	AWS Storage Gateway sekarang mendukung VMware ESXi Hypervisor versi 6.0 dan inisiator Red Hat Enterprise Linux 7 iSCSI. Lihat informasi yang lebih lengkap di Hypervisor dan persyaratan host yang didukung dan Pemrakarsa iSCSI yang didukung .	Oktober 20, 2015
Restrukturisasi konten	Rilis ini mencakup peningkatan ini: Dokumentasi sekarang menyertakan bagian Mengelola Gateway Aktif Anda yang menggabungkan tugas manajemen yang umum untuk semua solusi gateway. Berikut ini, Anda dapat menemukan petunjuk tentang bagaimana Anda dapat mengelola gateway Anda setelah Anda menerapkan dan mengaktifkannya. Untuk informasi selengkapnya, lihat Mengelola Gateway Anda .	

Perubahan	Deskripsi	Tanggal Diubah
Support untuk penyimpanan hingga 1.024 TiB dalam ukuran untuk volume cache	Untuk volume cache, Anda sekarang dapat membuat hingga 32 volume penyimpanan masing-masing hingga 32 TiB untuk penyimpanan maksimum 1.024 TiB. Untuk informasi selengkapnya, lihat Arsitektur volume cache dan AWS Storage Gateway kuota .	16 September 2015
Support untuk jenis adaptor jaringan VMXNET3 (10 GbE) di hypervisor VMware ESXI	Jika gateway Anda di-host pada hypervisor VMware ESXi, Anda dapat mengkonfigurasi ulang gateway untuk menggunakan jenis adaptor VMXNET3. Untuk informasi selengkapnya, lihat Mengkonfigurasi Adaptor Jaringan untuk Gateway Anda .	
Peningkatan kinerja	Tingkat upload maksimum untuk Storage Gateway telah meningkat menjadi 120 MB per detik, dan tingkat unduhan maksimum telah meningkat menjadi 20 MB per detik.	
Berbagai penyempurnaan dan pembaruan ke konsol lokal Storage Gateway	Konsol lokal Storage Gateway telah diperbarui dan disempurnakan dengan fitur tambahan untuk membantu Anda melakukan tugas pemeliharaan. Untuk informasi selengkapnya, lihat Mengkonfigurasi Jaringan Gateway Anda .	
Dukungan untuk penandaan	Storage Gateway sekarang mendukung penandaan sumber daya. Anda sekarang dapat menambahkan tag ke gateway, volume, dan kaset virtual untuk membuatnya lebih mudah dikelola. Untuk informasi selengkapnya, lihat Menandai Sumber Daya Storage Gateway .	

Perubahan	Deskripsi	Tanggal Diubah
Kompatibilitas dengan Quest (sebelumnya Dell) Backup 10.0 NetVault	Tape Gateway sekarang kompatibel dengan Quest NetVault Backup 10.0. Anda sekarang dapat menggunakan Quest NetVault Backup 10.0 untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan NetVault Cadangan Quest .	22 Juni 2015

Perubahan	Deskripsi	Tanggal Diubah
Support untuk volume penyimpanan 16 TiB untuk pengaturan gateway volume tersimpan	Storage Gateway sekarang mendukung volume penyimpanan 16 TiB untuk pengaturan gateway volume tersimpan. Anda sekarang dapat membuat 12 volume penyimpanan 16 TiB untuk penyimpanan maksimum 192 TiB. Untuk informasi selengkapnya, lihat Arsitektur volume tersimpan .	3 Juni 2015
Support untuk pemeriksaan sumber daya sistem pada konsol lokal Storage Gateway	Anda sekarang dapat menentukan apakah sumber daya sistem Anda (core CPU virtual, ukuran volume root, dan RAM) cukup untuk gateway Anda berfungsi dengan baik. Untuk informasi selengkapnya, lihat Melihat Status Sumber Daya Sistem Gateway Anda atau Melihat Status Sumber Daya Sistem Gateway Anda .	
Support untuk inisiator Red Hat Enterprise Linux 6 iSCSI	<p>Storage Gateway sekarang mendukung inisiator Red Hat Enterprise Linux 6 iSCSI. Untuk informasi selengkapnya, lihat Persyaratan.</p> <p>Rilis ini mencakup peningkatan dan pembaruan Storage Gateway berikut:</p> <ul style="list-style-type: none">• Dari konsol Storage Gateway, Anda sekarang dapat melihat tanggal dan waktu pembaruan perangkat lunak terakhir yang berhasil diterapkan ke gateway Anda. Untuk informasi selengkapnya, lihat Mengelola Pembaruan Gateway Menggunakan AWS Storage Gateway Konsol.• Storage Gateway sekarang menyediakan API yang dapat Anda gunakan untuk membuat daftar inisiator iSCSI yang terhubung ke volume penyimpanan	

Perubahan	Deskripsi	Tanggal Diubah
	<p>an Anda. Untuk informasi selengkapnya, lihat ListVolumelInitiators di referensi API.</p>	
<p>Support untuk Microsoft Hyper-V hypervisor versi 2012 dan 2012 R2</p>	<p>Storage Gateway sekarang mendukung Microsoft Hyper-V hypervisor versi 2012 dan 2012 R2. Ini adalah tambahan untuk dukungan untuk Microsoft Hyper-V hypervisor versi 2008 R2. Untuk informasi selengkapnya, lihat Hypervisor dan persyaratan host yang didukung.</p>	<p>30 April 2015</p>
<p>Kompatibilitas dengan Symantec Backup Exec 15</p>	<p>Tape Gateway sekarang kompatibel dengan Symantec Backup Exec 15. Anda sekarang dapat menggunakan Symantec Backup Exec 15 untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Veritas Backup Exec.</p>	<p>April 6, 2015</p>
<p>Dukungan otentikasi CHAP untuk volume penyimpanan</p>	<p>Storage Gateway sekarang mendukung konfigurasi otentikasi CHAP untuk volume penyimpanan. Untuk informasi selengkapnya, lihat Mengkonfigurasi otentikasi CHAP untuk volume Anda.</p>	<p>2 April 2015</p>
<p>Support untuk VMware ESXi Hypervisor versi 5.1 dan 5.5</p>	<p>Storage Gateway sekarang mendukung VMware ESXi Hypervisor versi 5.1 dan 5.5. Ini adalah tambahan untuk dukungan untuk VMware ESXi Hypervisor versi 4.1 dan 5.0. Untuk informasi selengkapnya, lihat Hypervisor dan persyaratan host yang didukung.</p>	<p>Maret 30, 2015</p>

Perubahan	Deskripsi	Tanggal Diubah
Dukungan untuk utilitas Windows CHKDSK	Storage Gateway sekarang mendukung utilitas Windows CHKDSK. Anda dapat menggunakan utilitas ini untuk memverifikasi integritas volume Anda dan memperbaiki kesalahan pada volume. Untuk informasi selengkapnya, lihat Memecahkan masalah volume .	Maret 04, 2015
Integrasi dengan AWS CloudTrail untuk menangkap panggilan API	<p>Storage Gateway sekarang terintegrasi dengan AWS CloudTrail. AWS CloudTrail menangkap panggilan API yang dilakukan oleh atau atas nama Storage Gateway di akun Amazon Web Services Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Untuk informasi selengkapnya, lihat Logging dan Monitoring di AWS Storage Gateway.</p> <p>Rilis ini mencakup peningkatan dan pembaruan Storage Gateway berikut:</p> <ul style="list-style-type: none">• Kaset virtual yang memiliki data kotor dalam penyimpanan cache (yaitu, yang berisi konten yang belum diunggah AWS) sekarang dipulihkan ketika drive cache gateway berubah. Untuk informasi selengkapnya, lihat Memulihkan Pita Virtual Dari Gerbang yang Tidak Dapat Dipulihkan.	Desember 16, 2014

Perubahan	Deskripsi	Tanggal Diubah
Kompatibilitas dengan perangkat lunak cadangan tambahan dan medium changer	<p>Tape Gateway sekarang kompatibel dengan perangkat lunak cadangan berikut:</p> <ul style="list-style-type: none">• Eksekutif Cadangan Symantec 2014• Manajer Perlindungan Data Microsoft System Center 2012 R2• Veeam Backup & Replikasi V7• Veeam Backup & Replikasi V8 <p>Anda sekarang dapat menggunakan empat produk perangkat lunak cadangan ini dengan pustaka pita virtual Storage Gateway (VTL) untuk mencadangkan ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menggunakan Perangkat Lunak Cadangan untuk Menguji Pengaturan Gateway Anda.</p> <p>Storage Gateway sekarang menyediakan medium changer tambahan yang bekerja dengan perangkat lunak cadangan baru.</p> <p>Rilis ini mencakup berbagai AWS Storage Gateway perbaikan dan pembaruan.</p>	November 3, 2014
Wilayah Eropa (Frankfurt)	Storage Gateway sekarang tersedia di Wilayah Eropa (Frankfurt). Untuk detail informasi, lihat AWS Daerah .	23 Oktober 2014

Perubahan	Deskripsi	Tanggal Diubah
Restrukturisasi konten	Membuat bagian Memulai yang umum untuk semua solusi gateway. Setelah itu, Anda dapat menemukan petunjuk bagi Anda untuk mengunduh, menyebarkan, dan mengaktifkan gateway. Setelah menerapkan dan mengaktifkan gateway, Anda dapat melanjutkan ke instruksi lebih lanjut khusus untuk volume tersimpan, volume cache, dan pengaturan Tape Gateway. Untuk informasi selengkapnya, lihat Membuat Gateway Tape .	19 Mei 2014
Kompatibilitas dengan Symantec Backup Exec 2012	Tape Gateway sekarang kompatibel dengan Symantec Backup Exec 2012. Anda sekarang dapat menggunakan Symantec Backup Exec 2012 untuk mencadangkan data Anda ke Amazon S3 dan mengarsipkan langsung ke penyimpanan offline (S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive). Untuk informasi selengkapnya, lihat Menguji Pengaturan Anda dengan Menggunakan Veritas Backup Exec .	28 April 2014

Perubahan	Deskripsi	Tanggal Diubah
<p>Support untuk Windows Server Failover Clustering</p> <p>Support untuk inisiator VMware ESX</p> <p>Support untuk melakukan tugas konfigurasi di konsol lokal Storage Gateway</p>	<ul style="list-style-type: none"> • Storage Gateway sekarang mendukung menghubungkan beberapa host ke volume yang sama jika host mengoordinasikan akses dengan menggunakan Windows Server Failover Clustering (WSFC). Namun, Anda tidak dapat menghubungkan beberapa host ke volume yang sama tanpa menggunakan WSFC. • Storage Gateway sekarang memungkinkan Anda untuk mengelola konektivitas penyimpanan langsung melalui host ESX Anda. Ini memberikan alternatif untuk menggunakan inisiator yang tinggal di OS tamu VM Anda. • Storage Gateway sekarang menyediakan dukungan untuk melakukan tugas konfigurasi di konsol lokal Storage Gateway. Untuk informasi tentang melakukan tugas konfigurasi pada gateway yang digunakan di lokasi, lihat atau Melakukan Tugas di Konsol Lokal VM Melakukan Tugas di Konsol Lokal VM Untuk informasi tentang melakukan tugas konfigurasi pada gateway yang digunakan pada instans EC2, lihat atau Melakukan Tugas di Konsol Lokal Amazon EC2 Melakukan Tugas di Konsol Lokal Amazon EC2 	<p>Januari 31, 2014</p>

Perubahan	Deskripsi	Tanggal Diubah
Support untuk virtual tape library (VTL) dan pengenalan API versi 2013-06-30	<p>Storage Gateway menghubungkan perangkat lunak lokal dengan penyimpanan berbasis cloud untuk mengintegrasikan lingkungan TI lokal Anda dengan infrastruktur penyimpanan. AWS Selain Volume Gateways (volume cache dan volume tersimpan), Storage Gateway sekarang mendukung gateway-virtual tape library (VTL). Anda dapat mengkonfigurasi Tape Gateway dengan hingga 10 drive tape virtual per gateway. Setiap tape drive virtual merespons set perintah SCSI, sehingga aplikasi backup lokal Anda yang ada akan bekerja tanpa modifikasi. Untuk informasi selengkapnya, lihat topik berikut di Panduan AWS Storage Gateway Pengguna.</p> <ul style="list-style-type: none">• Untuk ikhtisar arsitektur, lihat Cara kerja Tape Gateway (arsitektur).• Untuk memulai dengan Tape Gateway, lihat Membuat Gateway Tape.	5 November 2013
Support untuk Microsoft Hyper-V	<p>Storage Gateway sekarang menyediakan kemampuan untuk menyebarkan gateway lokal pada platform virtualisasi Microsoft Hyper-V. Gateway yang digunakan di Microsoft Hyper-V memiliki semua fungsi dan fitur yang sama dengan Storage Gateway lokal yang ada. Untuk mulai menerapkan gateway dengan Microsoft Hyper-V, lihat Hypervisor dan persyaratan host yang didukung</p>	April 10, 2013

Perubahan	Deskripsi	Tanggal Diubah
Support untuk menerapkan gateway di Amazon EC2	Storage Gateway sekarang menyediakan kemampuan untuk menerapkan gateway di Amazon Elastic Compute Cloud (Amazon EC2). Anda dapat meluncurkan instans gateway di Amazon EC2 menggunakan Storage Gateway AMI yang tersedia di AWS Marketplace Untuk mulai menerapkan gateway menggunakan Storage Gateway AMI, lihat Menerapkan instans Amazon EC2 untuk meng-host Tape Gateway .	Januari 15, 2013

Perubahan	Deskripsi	Tanggal Diubah
Support untuk volume cache dan pengenalan API Versi 2012-06-30	<p>Dalam rilis ini, Storage Gateway memperkenalkan dukungan untuk volume cache. Volume cache meminimalkan kebutuhan untuk menskalakan infrastruktur penyimpanan lokal Anda, sambil tetap menyediakan aplikasi Anda dengan akses latensi rendah ke data aktifnya. Anda dapat membuat volume penyimpanan hingga 32 TiB dan memasangnya sebagai perangkat iSCSI dari server aplikasi lokal Anda. Data yang ditulis ke volume cache disimpan di Amazon Simple Storage Service (Amazon S3), dengan hanya cache data yang baru saja ditulis dan baru dibaca yang disimpan secara lokal di perangkat keras penyimpanan lokal Anda. Volume cache memungkinkan Anda memanfaatkan Amazon S3 untuk data di mana latensi pengambilan yang lebih tinggi dapat diterima, seperti untuk data yang lebih lama dan jarang diakses, sambil mempertahankan penyimpanan lokal untuk data yang memerlukan akses latensi rendah.</p> <p>Dalam rilis ini, Storage Gateway juga memperkenalkan versi API baru yang, selain mendukung operasi saat ini, menyediakan operasi baru untuk mendukung volume cache.</p> <p>Untuk informasi selengkapnya tentang dua solusi Storage Gateway, lihat Cara kerja Tape Gateway (arsitektur).</p> <p>Anda juga dapat mencoba pengaturan pengujian. Untuk petunjuk, lihat Membuat Gateway Tape.</p>	Oktober 29, 2012

Perubahan	Deskripsi	Tanggal Diubah
Dukungan API dan IAM	<p>Dalam rilis ini, Storage Gateway memperkenalkan dukungan API serta dukungan untuk AWS Identity and Access Management(IAM).</p> <ul style="list-style-type: none">• Dukungan API- Anda sekarang dapat mengkonfigurasikan dan mengelola sumber daya Storage Gateway Anda secara terprogram. Untuk informasi selengkapnya tentang API, lihat Referensi API untuk Storage Gateway di Panduan AWS Storage Gateway Pengguna.• Dukungan IAM — AWS Identity and Access Management (IAM) memungkinkan Anda membuat pengguna dan mengelola akses pengguna ke sumber daya Storage Gateway Anda melalui kebijakan IAM. Untuk contoh kebijakan IAM, lihat Identity and Access Management untuk AWS Storage Gateway. Untuk informasi lebih lanjut tentang IAM, lihat halaman detail AWS Identity and Access Management (IAM).	9 Mei 2012
Dukungan IP statis	<p>Anda sekarang dapat menentukan IP statis untuk gateway lokal Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi Jaringan Gateway Anda.</p>	Maret 5, 2012
Panduan baru	<p>Ini adalah rilis pertama Panduan AWS Storage Gateway Pengguna.</p>	Januari 24, 2012

Catatan Rilis untuk Perangkat Lunak Tape Gateway Appliance

Catatan rilis ini menjelaskan fitur, peningkatan, dan perbaikan baru dan yang diperbarui yang disertakan dengan setiap versi alat Tape Gateway . Setiap versi perangkat lunak diidentifikasi berdasarkan tanggal rilis dan nomor versi unik.

Anda dapat menentukan nomor versi perangkat lunak gateway dengan memeriksa halaman Detailnya di konsol Storage Gateway, atau dengan memanggil tindakan [DescribeGatewayInformation](#) API menggunakan AWS CLI perintah yang mirip dengan berikut ini:

```
aws storagegateway describe-gateway-information --gateway-arn
"arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

Nomor versi dikembalikan di `SoftwareVersion` bidang respons API.

Note

Gateway tidak akan melaporkan informasi versi perangkat lunak dalam keadaan berikut:

- Gateway sedang offline.
- Gateway menjalankan perangkat lunak lama yang tidak mendukung pelaporan versi.
- Jenis gateway adalah FSx File Gateway.

Untuk informasi selengkapnya tentang pembaruan Tape, termasuk cara mengubah pemeliharaan otomatis default dan jadwal pembaruan untuk gateway, lihat [Mengelola Pembaruan Gateway Menggunakan Konsol Gateway AWS Storage](#) .

Tanggal rilis	Versi Perangkat Lunak	Catatan rilis
2024-04-10	2.8.1	<ul style="list-style-type: none">• Mengatasi masalah penggunaan memori yang diperkenalkan di 2.8.0• Pembaruan patch keamanan

Tanggal rilis	Versi Perangkat Lunak	Catatan rilis
		<ul style="list-style-type: none">• Proses pembaruan perangkat lunak yang ditingkatkan• Mengatasi komponen Network Time Protocol (NTP) yang hilang untuk gateway baru
2024-03-06	2.8.0	<ul style="list-style-type: none">• Pembaruan sistem operasi untuk gateway baru• Pembaruan patch keamanan• Peningkatan kinerja untuk beban kerja Backup dan Restore bersamaan
2023-12-19	2.7.0	<ul style="list-style-type: none">• Pembaruan sistem operasi untuk gateway baru
2023-12-14	2.6.6	<ul style="list-style-type: none">• Memperbaiki masalah dengan posisi relatif pada kaset yang lebih besar dari 5TiB
2023-10-19	2.6.5	<ul style="list-style-type: none">• Menambahkan perlindungan terhadap penyimpanan tape oleh klien setelah gateway dimulai ulang