Panduan Pengguna Volume Gateway

AWS Storage Gateway

Versi API 2013-06-30

AWS Storage Gateway: Panduan Pengguna Volume Gateway

Table of Contents

Apa itu Volume 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.

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

Untuk melihat berbagai kasus penggunaan yang AWS Storage Gateway membantu memungkinkan, lihat AWS Storage Gateway. Untuk informasi terkini tentang harga, lihat Harga di halaman AWS Storage Gateway detail.

AWS Storage Gateway menawarkan solusi penyimpanan berbasis file (S3 File Gateway dan FSx File Gateway), berbasis volume (Volume Gateway), dan berbasis tape (Tape Gateway).

Panduan Pengguna ini memberikan informasi terkait Volume Gateway.

Volume Gateway menyediakan volume penyimpanan yang didukung cloud yang dapat dipasang sebagai perangkat Internet Small Computer System Interface (iSCSI) dari server aplikasi lokal.

Volume Gateway mendukung konfigurasi volume berikut:

- Volume cache - Anda menyimpan data Anda di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dan menyimpan salinan subset data yang sering diakses secara lokal. Volume cache menawarkan penghematan biaya yang besar pada penyimpanan primer dan meminimalkan kebutuhan untuk menskalakan penyimpanan Anda di tempat. Anda juga mempertahankan akses latensi rendah ke data yang sering diakses.
- Volume tersimpan — Jika Anda memerlukan akses latensi rendah ke seluruh kumpulan data, konfigurasikan gateway lokal terlebih dahulu untuk menyimpan semua data secara lokal. Kemudian secara asinkron mencadangkan point-in-time snapshot data ini ke Amazon S3. Konfigurasi ini menyediakan cadangan offsite yang tahan lama dan murah yang dapat Anda pulihkan ke pusat data lokal atau Amazon Elastic Compute Cloud (Amazon). EC2 Misalnya, jika Anda memerlukan

kapasitas pengganti untuk pemulihan bencana, Anda dapat memulihkan cadangan ke Amazon. EC2

Untuk ikhtisar arsitektur, lihatCara kerja Volume Gateway.

Dalam Panduan Pengguna ini, Anda dapat menemukan bagian Memulai yang mencakup informasi penyiapan yang umum untuk semua jenis gateway. Anda juga dapat menemukan persyaratan pengaturan , dan bagian yang menjelaskan cara menerapkan, mengaktifkan, mengonfigurasi, dan mengelola Anda.

Prosedur dalam Panduan Pengguna ini terutama berfokus pada melakukan operasi gateway dengan menggunakan AWS Management Console. Jika Anda ingin menjalankan operasi ini secara terprogram, lihat Referensi AWS Storage Gateway API.

Cara kerja Volume Gateway

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

Gerbang Volume

Untuk Volume Gateways, Anda dapat menggunakan volume cache atau volume yang disimpan.

Topik

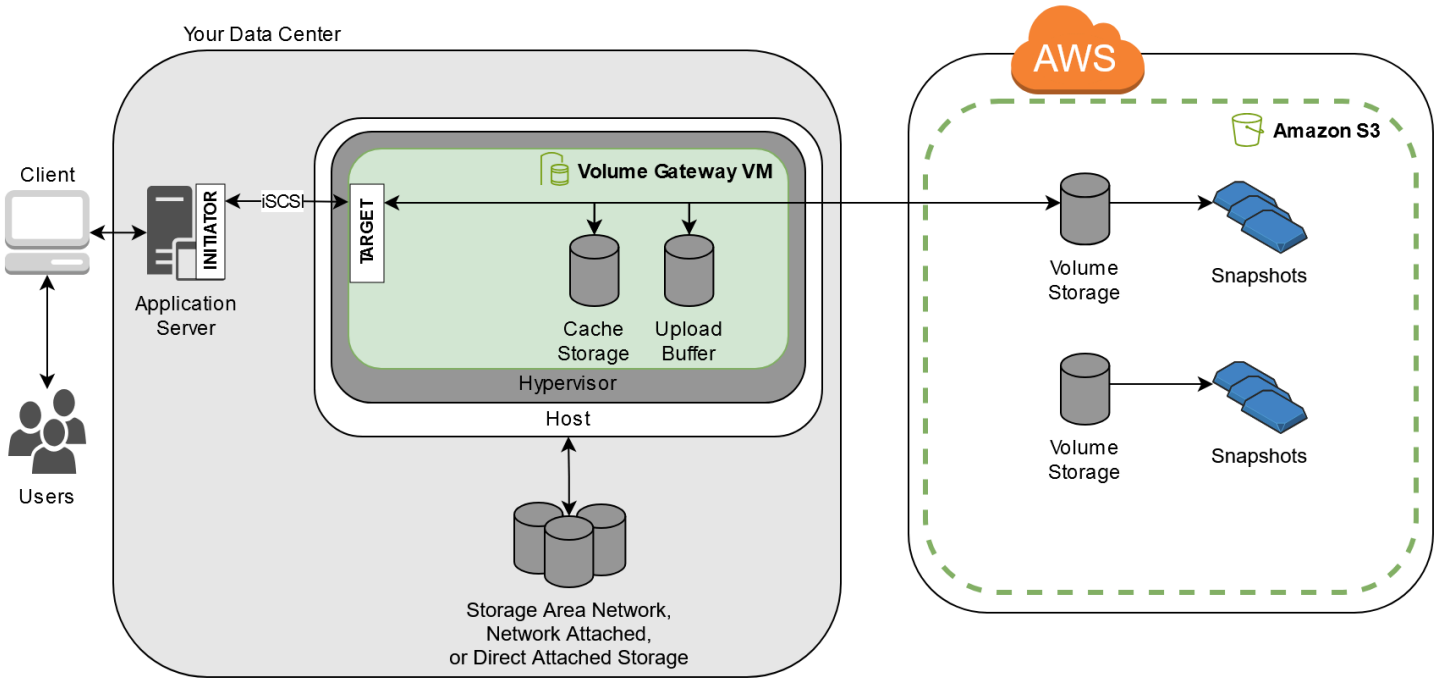
- Arsitektur volume cache
- Arsitektur volume tersimpan

Arsitektur volume cache

Dengan menggunakan volume yang di-cache, Anda dapat menggunakan Amazon S3 sebagai penyimpanan data utama, sambil mempertahankan data yang sering diakses secara lokal di Storage Gateway Anda. Volume cache meminimalkan kebutuhan untuk menskalakan infrastruktur penyimpanan lokal Anda, sambil tetap menyediakan aplikasi Anda dengan akses latensi rendah ke data yang sering diakses. Anda dapat membuat volume penyimpanan hingga 32 TiB dan melampirkannya sebagai perangkat iSCSI dari server aplikasi lokal Anda. Gateway menyimpan data yang Anda tulis ke volume ini di Amazon S3 dan menyimpan data yang baru dibaca di cache Storage Gateway lokal dan penyimpanan buffer upload.

Volume cache dapat berkisar dari 1 GiB hingga 32 TiB dalam ukuran dan harus dibulatkan ke GiB terdekat. Setiap gateway yang dikonfigurasi untuk volume cache dapat mendukung hingga 32 volume untuk total volume penyimpanan maksimum 1.024 TiB (1 PiB).

Dalam solusi volume cache, Storage Gateway menyimpan semua data aplikasi lokal Anda dalam volume penyimpanan di Amazon S3. Diagram berikut memberikan gambaran umum tentang penyebaran volume cache.



Setelah menginstal perangkat lunak Storage Gateway — VM — pada host di pusat data Anda dan mengaktifkannya, Anda menggunakan AWS Management Console untuk menyediakan volume penyimpanan yang didukung oleh Amazon S3. Anda juga dapat menyediakan volume penyimpanan secara terprogram menggunakan Storage Gateway API atau pustaka AWS SDK. Anda kemudian memasang volume penyimpanan ini ke server aplikasi lokal sebagai perangkat iSCSI.

Anda juga mengalokasikan disk lokal untuk VM. Disk lokal ini melayani tujuan berikut:

- Disk untuk digunakan oleh gateway sebagai penyimpanan cache — Saat aplikasi Anda menulis data ke volume penyimpanan AWS, gateway pertama-tama menyimpan data pada disk lokal yang digunakan untuk penyimpanan cache. Kemudian gateway mengunggah data ke Amazon S3. Penyimpanan cache bertindak sebagai penyimpanan tahan lama lokal untuk data yang menunggu untuk diunggah ke Amazon S3 dari buffer unggahan.

Penyimpanan cache juga memungkinkan gateway menyimpan data aplikasi yang baru diakses secara lokal untuk akses latensi rendah. Jika aplikasi Anda meminta data, gateway terlebih dahulu memeriksa penyimpanan cache untuk data sebelum memeriksa Amazon S3.

Anda dapat menggunakan panduan berikut untuk menentukan jumlah ruang disk yang akan dialokasikan untuk penyimpanan cache. Umumnya, Anda harus mengalokasikan setidaknya 20 persen dari ukuran penyimpanan file yang ada sebagai penyimpanan cache. Penyimpanan cache juga harus lebih besar dari buffer unggahan. Pedoman ini membantu memastikan bahwa penyimpanan cache cukup besar untuk terus menyimpan semua data di buffer unggahan yang belum diunggah ke Amazon S3.

- Disk untuk digunakan oleh gateway sebagai buffer unggahan — Untuk mempersiapkan upload ke Amazon S3, gateway Anda juga menyimpan data masuk di area pementasan, yang disebut sebagai buffer unggahan. Gateway Anda mengunggah data buffer ini melalui koneksi Secure Sockets Layer (SSL) terenkripsi AWS, tempat penyimpanan terenkripsi di Amazon S3.

Anda dapat mengambil cadangan tambahan, yang disebut snapshot, dari volume penyimpanan Anda di Amazon S3. point-in-timeSnapshot ini juga disimpan di Amazon S3 sebagai snapshot Amazon EBS. Saat Anda mengambil snapshot baru, hanya data yang telah berubah sejak snapshot terakhir Anda disimpan. Saat snapshot diambil, gateway mengunggah perubahan hingga titik snapshot, lalu membuat snapshot baru menggunakan Amazon EBS. Anda dapat memulai snapshot secara terjadwal atau satu kali. Satu volume mendukung antrian beberapa snapshot secara berurutan, tetapi setiap snapshot harus selesai dibuat sebelum yang berikutnya dapat diambil. Saat Anda menghapus snapshot, hanya data yang tidak diperlukan untuk snapshot lain yang dihapus. Untuk informasi tentang snapshot Amazon EBS, lihat snapshot Amazon EBS.

Anda dapat memulihkan snapshot Amazon EBS ke volume penyimpanan gateway jika Anda perlu memulihkan cadangan data Anda. Atau, untuk snapshot berukuran hingga 16 TiB, Anda dapat menggunakan snapshot sebagai titik awal untuk volume Amazon EBS baru. Anda kemudian dapat melampirkan volume Amazon EBS baru ini ke EC2 instans Amazon.

Semua data gateway dan data snapshot untuk volume cache disimpan di Amazon S3 dan dienkripsi saat istirahat menggunakan enkripsi sisi server (SSE). Namun, Anda tidak dapat mengakses data ini dengan Amazon S3 API atau alat lain seperti Konsol Manajemen Amazon S3.

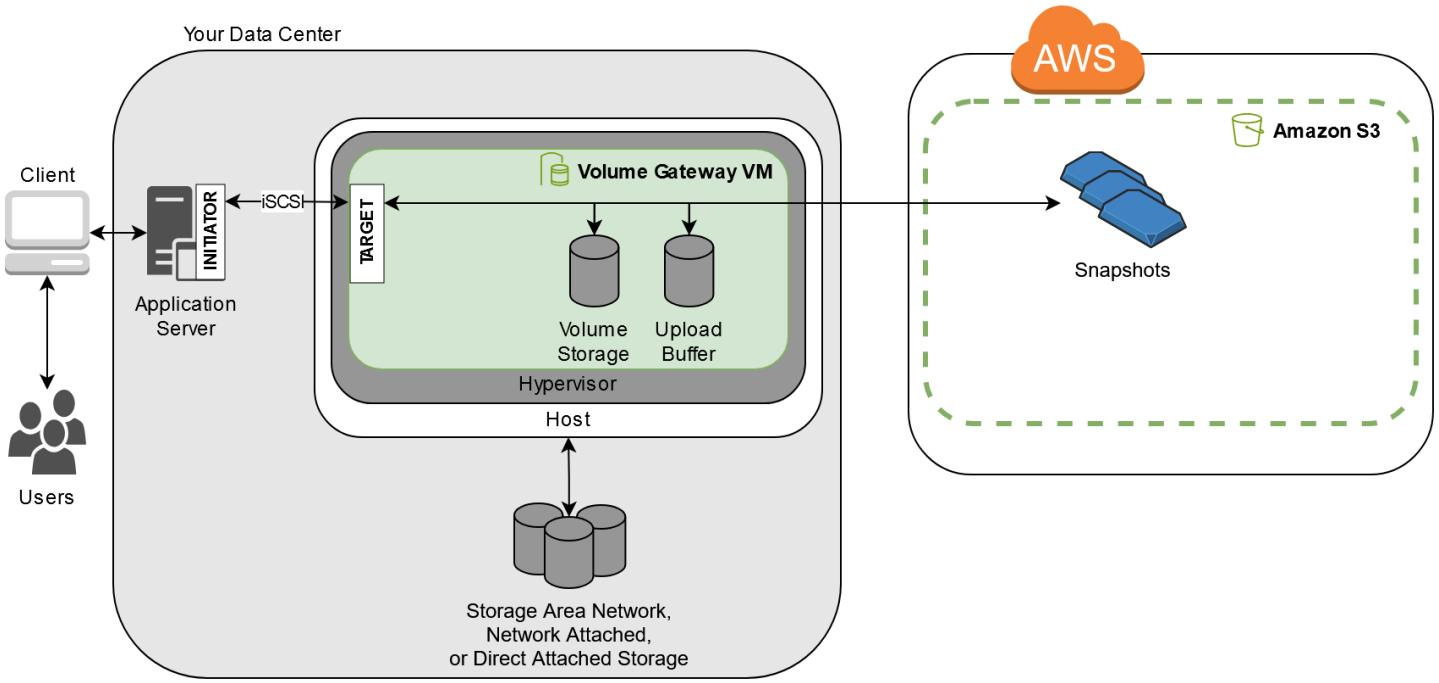
Arsitektur volume tersimpan

Dengan menggunakan volume tersimpan, Anda dapat menyimpan data primer Anda secara lokal, sambil mencadangkan data tersebut secara asinkron. AWS Volume tersimpan menyediakan aplikasi lokal Anda dengan akses latensi rendah ke seluruh kumpulan datanya. Pada saat yang sama, mereka menyediakan cadangan di luar kantor yang tahan lama. Anda dapat membuat volume penyimpanan dan memasangnya sebagai perangkat iSCSI dari server aplikasi lokal. Data yang ditulis ke volume tersimpan disimpan di perangkat keras penyimpanan lokal Anda. Data ini secara asinkron dicadangkan ke Amazon S3 sebagai snapshot Amazon Elastic Block Store (Amazon EBS).

Volume yang disimpan dapat berkisar dari 1 GiB hingga 16 TiB dan harus dibulatkan ke GiB terdekat. Setiap gateway yang dikonfigurasi untuk volume tersimpan dapat mendukung hingga 32 volume dan total volume penyimpanan 512 TiB (0,5 piB).

Dengan volume tersimpan, Anda mempertahankan penyimpanan volume lokal di pusat data Anda. Artinya, Anda menyimpan semua data aplikasi di perangkat keras penyimpanan lokal Anda. Kemudian, menggunakan fitur yang membantu menjaga keamanan data, gateway mengunggah data ke Amazon Web Services Cloud untuk pencadangan hemat biaya dan pemulihan bencana yang cepat. Solusi ini sangat ideal jika Anda ingin menyimpan data lokal di tempat, karena Anda harus memiliki akses latensi rendah ke semua data Anda, dan juga untuk mempertahankan cadangan. AWS

Diagram berikut memberikan gambaran umum tentang penyebaran volume yang disimpan.



Setelah Anda menginstal perangkat lunak Storage Gateway — VM — pada host di pusat data Anda dan mengaktifkannya, Anda dapat membuat volume penyimpanan gateway. Anda kemudian memetakannya ke disk penyimpanan terlampir langsung (DAS) atau jaringan area penyimpanan (SAN) lokal. Anda dapat mulai dengan disk baru atau disk yang sudah menyimpan data. Anda kemudian dapat memasang volume penyimpanan ini ke server aplikasi lokal sebagai perangkat iSCSI. Saat aplikasi lokal Anda menulis data ke dan membaca data dari volume penyimpanan gateway, data ini disimpan dan diambil dari disk yang ditetapkan volume.

Untuk menyiapkan data untuk diunggah ke Amazon S3, gateway Anda juga menyimpan data yang masuk di area pementasan, yang disebut sebagai buffer unggahan. Anda dapat menggunakan disk DAS atau SAN lokal untuk penyimpanan yang berfungsi. Gateway Anda mengunggah data dari buffer upload melalui koneksi Secure Sockets Layer (SSL) terenkripsi ke layanan Storage Gateway yang berjalan di Amazon Web Services Cloud. Layanan kemudian menyimpan data yang dienkripsi di Amazon S3.

Anda dapat mengambil cadangan tambahan, yang disebut snapshot, dari volume penyimpanan Anda. Gateway menyimpan snapshot ini di Amazon S3 sebagai snapshot Amazon EBS. Saat Anda mengambil snapshot baru, hanya data yang telah berubah sejak snapshot terakhir Anda disimpan. Saat snapshot diambil, gateway mengunggah perubahan hingga titik snapshot, lalu membuat snapshot baru menggunakan Amazon EBS. Anda dapat memulai snapshot secara terjadwal atau satu kali. Satu volume mendukung antrian beberapa snapshot secara berurutan, tetapi setiap snapshot harus selesai dibuat sebelum yang berikutnya dapat diambil. Saat Anda menghapus snapshot, hanya data yang tidak diperlukan untuk snapshot lain yang dihapus.

Anda dapat memulihkan snapshot Amazon EBS ke volume penyimpanan gateway lokal jika Anda perlu memulihkan cadangan data Anda. Anda juga dapat menggunakan snapshot sebagai titik awal untuk volume Amazon EBS baru, yang kemudian dapat Anda lampirkan ke instans Amazon EC2.

Memulai dengan AWS Storage Gateway

Bagian ini memberikan instruksi untuk memulai AWS. Anda memerlukan AWS akun sebelum Anda dapat mulai menggunakan AWS Storage Gateway. Anda dapat menggunakan AWS akun yang sudah ada, atau mendaftar untuk akun baru. Anda juga memerlukan pengguna IAM di AWS akun Anda yang termasuk dalam grup dengan izin administratif yang diperlukan untuk melakukan tugas Storage Gateway. Pengguna dengan hak istimewa yang sesuai dapat mengakses konsol Storage Gateway dan Storage Gateway API untuk melakukan tugas penerapan, konfigurasi, dan pemeliharaan gateway. Jika Anda adalah pengguna pertama kali, sebaiknya Anda meninjau bagian AWS Wilayah yang didukung dan persyaratan penyiapan Volume Gateway sebelum Anda bekerja dengan Storage Gateway.

Bagian ini berisi topik-topik berikut, yang memberikan informasi tambahan tentang memulai AWS Storage Gateway:

Topik

- Mendaftar untuk AWS Storage Gateway- Pelajari cara mendaftar AWS dan membuat AWS akun.
- Buat pengguna IAM dengan hak administrator- Pelajari cara membuat pengguna IAM dengan hak administratif untuk akun Anda AWS .
- Mengakses AWS Storage Gateway- Pelajari cara mengakses AWS Storage Gateway melalui konsol Storage Gateway atau secara terprogram menggunakan. AWS SDKs
- Wilayah AWS yang mendukung Storage Gateway- Pelajari AWS Wilayah mana yang dapat Anda gunakan untuk menyimpan data saat mengaktifkan gateway di Storage Gateway.

Mendaftar untuk AWS Storage Gateway

An Akun AWS adalah persyaratan mendasar untuk mengakses AWS layanan. Anda Akun AWS adalah wadah dasar untuk semua sumber AWS daya yang Anda buat sebagai AWS pengguna. Anda juga Akun AWS merupakan batas keamanan dasar untuk sumber daya Anda AWS . Sumber daya apa pun yang Anda buat di akun Anda tersedia untuk pengguna yang memiliki kredensi untuk akun tersebut. Sebelum Anda dapat mulai menggunakan AWS Storage Gateway, Anda harus mendaftar untuk Akun AWS.

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. 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.

Kami juga menyarankan agar Anda meminta pengguna Anda untuk menggunakan kredensi sementara saat mengakses. AWS Untuk memberikan kredensi sementara, Anda dapat menggunakan federasi dan penyedia identitas, seperti AWS IAM Identity Center. Jika perusahaan Anda sudah menggunakan penyedia identitas, Anda dapat menggunakannya dengan federasi untuk menyederhanakan cara Anda menyediakan akses ke sumber daya di AWS akun Anda.

Buat pengguna IAM dengan hak administrator

Setelah Anda membuat AWS akun, gunakan langkah-langkah berikut untuk membuat pengguna AWS Identity and Access Management (IAM) untuk Anda sendiri, lalu tambahkan pengguna tersebut ke grup yang memiliki izin administratif. Untuk informasi selengkapnya tentang penggunaan AWS Identity and Access Management layanan untuk mengontrol akses ke sumber daya Storage Gateway, lihatIdentity and Access Management untuk AWS Storage Gateway.

Untuk membuat pengguna administrator, pilih salah satu opsi berikut.

Pilih salah satu cara untuk mengelola administrator Anda	Untuk	Oleh	Anda juga bisa
Di Pusat Identitas IAM (Direkomendasikan)	Gunakan kredensi jangka pendek untuk mengakses. AWS Ini sejalan dengan praktik terbaik keamanan. Untuk informasi tentang praktik terbaik, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.	Mengikuti petunjuk di Memulai di Panduan AWS IAM Identity Center Pengguna.	Konfigurasikan akses terprogram dengan Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam AWS Command Line Interface Panduan Pengguna.
Di IAM (Tidak direkomendasikan)	Gunakan kredensi jangka panjang untuk mengakses. AWS	Mengikuti petunjuk di Buat pengguna IAM untuk akses darurat di Panduan Pengguna IAM.	Konfigurasikan akses terprogram dengan Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Warning

Pengguna IAM memiliki kredensi jangka panjang yang menghadirkan risiko keamanan. Untuk membantu mengurangi risiko ini, kami menyarankan agar Anda memberikan pengguna ini

hanya izin yang mereka perlukan untuk melakukan tugas dan menghapus pengguna ini ketika mereka tidak lagi diperlukan.

Mengakses AWS Storage Gateway

Anda dapat menggunakan AWS Storage Gateway konsol untuk melakukan berbagai tugas konfigurasi dan pemeliharaan gateway, termasuk mengaktifkan atau menghapus peralatan perangkat keras Storage Gateway dari penerapan, membuat, mengelola, dan menghapus berbagai jenis gateway, membuat, mengelola, dan menghapus , dan memantau kesehatan dan status berbagai elemen layanan Storage Gateway. Untuk kesederhanaan dan kemudahan penggunaan, panduan ini berfokus pada melakukan tugas menggunakan antarmuka web konsol Storage Gateway. Anda dapat mengakses konsol Storage Gateway melalui browser web Anda di:https://console.aws.amazon.com/storagegateway/home/.

Jika Anda lebih suka pendekatan terprogram, Anda dapat menggunakan AWS Storage Gateway Application Programming Interface (API) atau Command Line Interface (CLI) untuk mengatur dan mengelola sumber daya dalam penyebaran Storage Gateway Anda. Untuk informasi selengkapnya tentang tindakan, tipe data, dan sintaks yang diperlukan untuk Storage Gateway API, lihat Referensi API Storage Gateway. Untuk informasi selengkapnya tentang Storage Gateway CLI, lihat Referensi Perintah AWS CLI.

Anda juga dapat menggunakan aplikasi AWS SDKs untuk mengembangkan aplikasi yang berinteraksi dengan Storage Gateway. AWS SDKs Untuk Java, .NET, dan PHP membungkus Storage Gateway API yang mendasarinya untuk menyederhanakan tugas pemrograman Anda. Untuk informasi tentang mengunduh pustaka SDK, lihat Pusat AWS Pengembang.

Untuk informasi lebih lanjut tenngenai harga, lihat harga AWS Storage Gateway.

Wilayah AWS yang mendukung Storage Gateway

An Wilayah AWS adalah lokasi fisik di dunia di mana AWS memiliki beberapa Availability Zone. Availability Zones terdiri dari satu atau lebih pusat AWS data diskrit, masing-masing dengan daya redundan, jaringan, dan konektivitas, ditempatkan di fasilitas terpisah. Ini berarti bahwa masing-masing Wilayah AWS secara fisik terisolasi dan independen dari Daerah lain. Wilayah memberikan toleransi kesalahan, stabilitas, serta ketahanan, dan juga dapat mengurangi latensi. Sumber daya yang Anda buat di satu Wilayah tidak ada di Wilayah lain kecuali Anda secara eksplisit menggunakan fitur replikasi yang ditawarkan oleh layanan. AWS Misalnya, Amazon S3 dan Amazon

EC2 mendukung replikasi lintas wilayah. Beberapa layanan, seperti AWS Identity and Access Management, tidak memiliki sumber daya Regional. Anda dapat meluncurkan AWS sumber daya di lokasi yang memenuhi persyaratan bisnis Anda. Misalnya, Anda mungkin ingin meluncurkan EC2 instans Amazon untuk meng-host AWS Storage Gateway peralatan Anda Wilayah AWS di Eropa agar lebih dekat dengan pengguna Eropa Anda, atau untuk memenuhi persyaratan hukum. Anda Akun AWS menentukan Wilayah mana yang didukung oleh layanan tertentu yang tersedia untuk Anda gunakan.

- 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 untuk mengatur Volume Gateway

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

Topik

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 VMs

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 Volume 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, lihatAWS Storage Gateway kuota.

Persyaratan untuk jenis EC2 instans Amazon

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

> **Note**
>
> Storage Gateway AMI hanya kompatibel dengan instans berbasis x86 yang menggunakan prosesor Intel atau AMD. Instans berbasis ARM yang menggunakan prosesor Graviton tidak didukung.

Untuk Volume Gateway , EC2 instans Amazon 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 yang di-cache

- Keluarga instance tujuan umum — tipe instans m4, m5, atau m6.
- Keluarga instans yang dioptimalkan komputasi — tipe instans c4, c5, c6, atau c7. Pilih ukuran instans 2xlarge atau lebih tinggi untuk memenuhi persyaratan RAM yang diperlukan.
- Keluarga instans yang dioptimalkan untuk memori — tipe instans r3, r5, r6, atau r7.
- Keluarga instans yang dioptimalkan untuk penyimpanan — tipe instans i3, i4, atau i7.

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 Volume yang di-cache	150 GiB	64 TiB	150 GiB	2 TiB	—
Gerbang Volume Tersimpan	—	—	150 GiB	2 TiB	1 atau lebih untuk volume atau volume yang disimpan

> **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, lihatAWS 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 membatasi AWS 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

Volume Gateway memerlukan port tertentu untuk diizinkan melalui keamanan jaringan Anda agar penerapan dan pengoperasian berhasil. Beberapa port diperlukan untuk semua gateway, sementara yang lain hanya diperlukan untuk konfigurasi tertentu, seperti saat menghubungkan ke titik akhir VPC.

Persyaratan port untuk Volume Gateway

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Browser web	Perambar web Anda	Storage Gateway VM	TCP HTTP	80	✓	✓	✓	Digunakan oleh sistem

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
								lokal untuk mendapatkan kunci aktivasi Storage Gateway. Port 80 hanya digunakan selama aktivasi alat Storage Gateway. VM Storage Gateway tidak memerlukan port 80 agar dapat diakses publik. Tingkat akses yang diperlukan ke port 80 tergantung pada

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
								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.

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Browser web	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	AWS Konsol Manajemen (semua operasi lainnya)
DNS	Storage Gateway VM	Server Domain Name Service (DNS)	DNS TCP & UDP	53	✓	✓	✓	Digunakan untuk komunikasi antara Storage Gateway VM dan server DNS untuk resolusi nama IP.

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
NTP	Storage Gateway VM	Server Protokol Waktu Jaringan (NTP)	TCP & UDP NTP	123	✓	✓	✓	Digunakan oleh sistem lokal untuk menyinkronkan waktu VM ke waktu host. VM Storage Gateway dikonfigurasi untuk menggunakan server NTP berikut: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
								• 3.amazon.pool.ntp.org **Note** Tidak diperlukan untuk gateway yang dihosting di Amazon. EC2

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Storage Gateway	Storage Gateway VM	Dukungan Titik akhir	TCP SSH	22	✓	✓	✓	Memungkinkan Dukungan 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. Untuk daftar titik akhir dukungan,

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
								lihat titik Dukungan akhir.
Storage Gateway	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	Pengendalian manajemen
Amazon CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	Untuk aktivasi
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	Pengendalian manajemen * Diperlukan hanya saat menggunakan titik akhir VPC

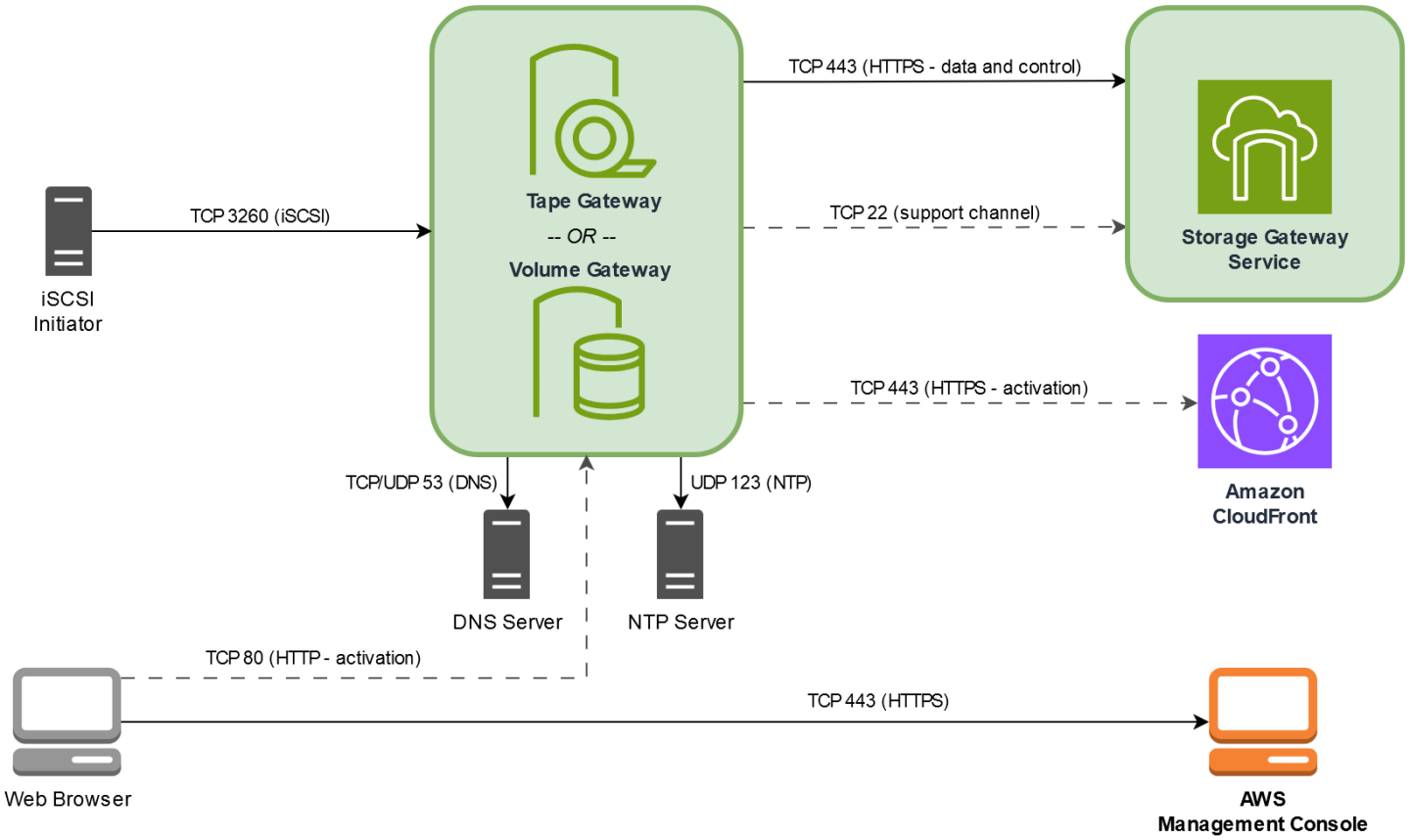
Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
VPC	Storage Gateway VM	AWS	TCP HTTPS	1026		✓	✓*	Titik akhir Bidang Kontrol * Diperlukan hanya saat menggunakan titik akhir VPC
VPC	Storage Gateway VM	AWS	TCP HTTPS	1027		✓	✓*	Anon Control Plane (untuk aktivasi) * Diperlukan hanya saat menggunakan titik akhir VPC

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
VPC	Storage Gateway VM	AWS	TCP HTTPS	1028		✓	✓*	Titik akhir proxy * Diperlukan hanya saat menggunakan titik akhir VPC
VPC	Storage Gateway VM	AWS	TCP HTTPS	1031		✓	✓*	Bidang Data * Diperlukan hanya saat menggunakan titik akhir VPC

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
VPC	Storage Gateway VM	AWS	TCP HTTPS	2222		✓	✓*	Saluran Dukungan SSH untuk VPCe * Diperlukan hanya untuk membuka saluran dukungan saat menggunakan titik akhir VPC
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	Pengendalian manajemen * Diperlukan hanya saat menggunakan titik akhir VPC

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Klien iSCSI	Klien iSCSI	Storage Gateway VM	TCP	3260	✓	✓	✓	Agar sistem lokal terhubung ke target iSCSI yang diekspos oleh gateway.

Ilustrasi berikut menunjukkan arus lalu lintas jaringan untuk penyebaran Volume Gateway dasar.



Persyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance

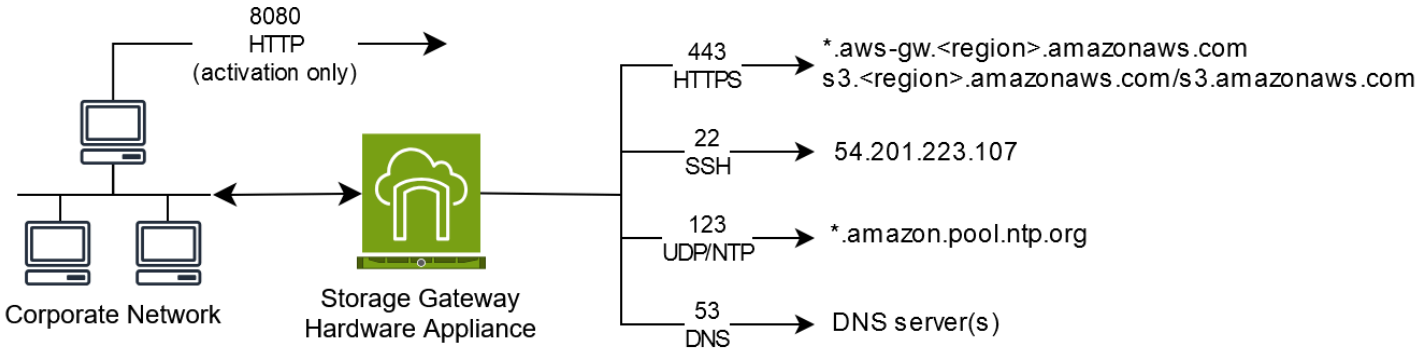
Setiap Storage Gateway Hardware Appliance memerlukan layanan jaringan berikut:

- 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 — DHCP atau IPv4 alamat statis yang ditetapkan. Anda tidak dapat menetapkan IPv6 alamat.

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.

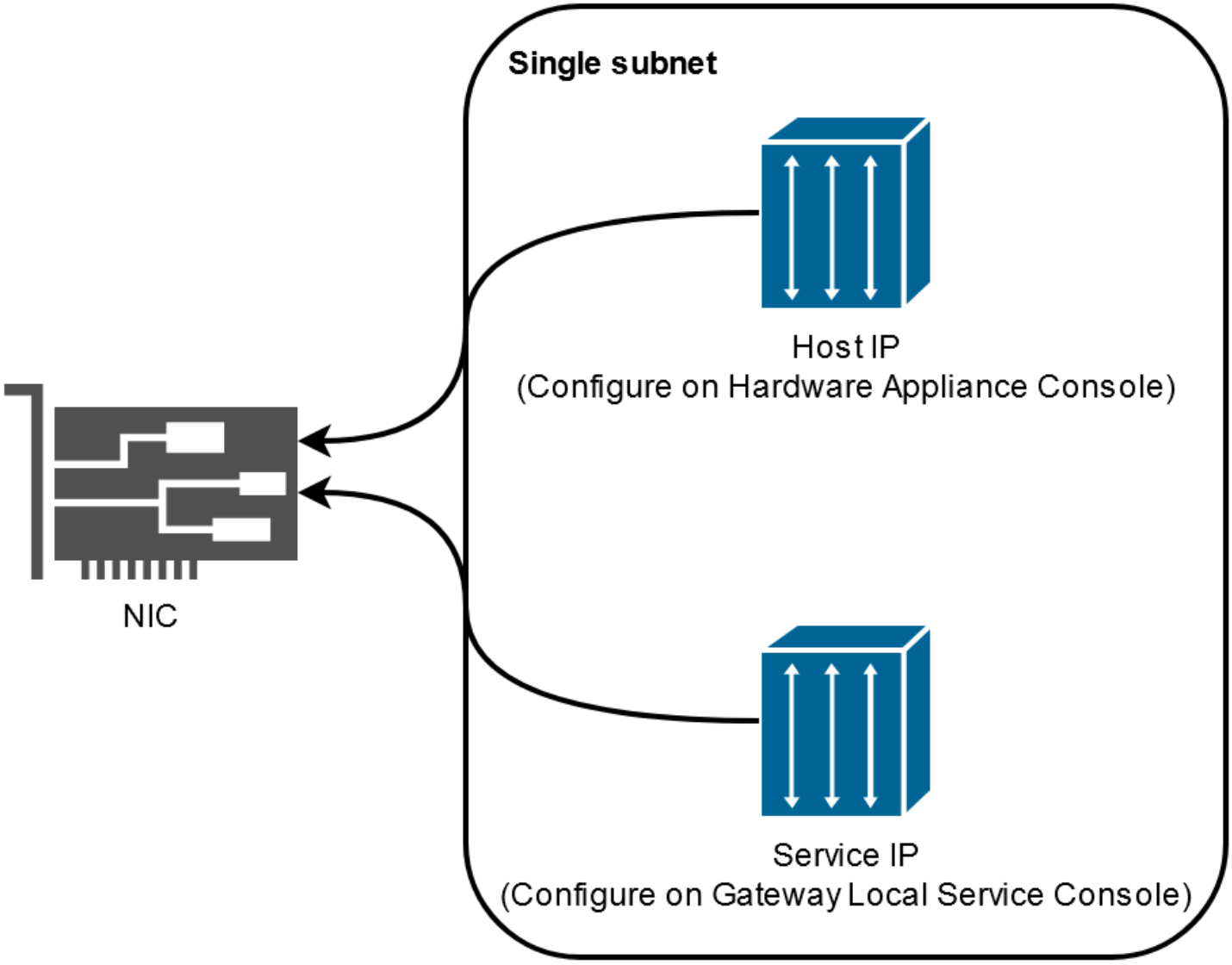
Protokol	Port	Arahan	Sumber	Tujuan	Bagaimana Digunakan
SSH	22	Ke luar	Alat perangkat keras	`54.201.223.107`	Saluran dukungan
DNS	53	Ke luar	Alat perangkat keras	Server DNS	Resolusi nama
UDP/NTP	123	Ke luar	Alat perangkat keras	`*.amazon.pool.ntp.org`	Sinkronisasi waktu
HTTPS	443	Ke luar	Alat perangkat 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:

- Konfigurasikan 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.
- Konfigurasikan setidaknya satu antarmuka jaringan untuk mendukung alat perangkat keras. Untuk informasi selengkapnya, lihat Mengkonfigurasi parameter jaringan alat perangkat keras.

> **Note**
>
> Untuk ilustrasi yang menunjukkan bagian belakang server dengan port-portnya, lihat Memasang alat perangkat keras Anda secara fisik

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 Region gateway Anda, ganti *region* di titik akhir layanan dengan string wilayah yang benar.

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
```

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 EC2 gateway Amazon Anda

Grup keamanan mengontrol lalu lintas ke instans EC2 gateway Amazon 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 EC2 host Amazon 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 Dukungan untuk tujuan pemecahan masalah. Untuk informasi selengkapnya, lihat Anda ingin Dukungan membantu memecahkan masalah gateway Anda EC2 .

Dalam beberapa kasus, Anda mungkin menggunakan EC2 instance Amazon 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, lihatPersyaratan 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) - 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.
- EC2 Instans Amazon — 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, lihatMenerapkan EC2 instans Amazon yang disesuaikan untuk Volume 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 AMI Anda. EC2 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 menerapkan volume cache atau Volume Gateway yang disimpan, Anda dapat membuat volume penyimpanan iSCSI di gateway Anda.

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

- Server Microsoft Windows 2022
- Perusahaan Topi Merah Linux 8
- Perusahaan Topi Merah Linux 9
- VMware ESX Initiator, yang menyediakan alternatif untuk menggunakan inisiator dalam sistem operasi tamu Anda VMs

> **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.

Menggunakan Storage Gateway Hardware Appliance

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

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 dalam penyebaran Anda dari halaman ikhtisar 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 Anda, proses aktivasi mengaitkan alat perangkat keras dengan perangkat keras Anda Akun AWS. Setelah aktivasi, perangkat keras Anda muncul di konsol di halaman ikhtisar perangkat keras. Anda dapat mengonfigurasi perangkat keras sebagai tipe S3 File Gateway, FSx File Gateway, Tape Gateway, atau Volume Gateway. Prosedur yang Anda gunakan untuk menerapkan jenis gateway ini pada alat perangkat keras sama dengan pada platform virtual.

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.

Di bagian berikut, Anda dapat menemukan petunjuk tentang cara mengatur, memasang rak, memberi daya, mengonfigurasi, mengaktifkan, meluncurkan, menggunakan, dan menghapus Storage Gateway Hardware Appliance.

Topik

- Mengakses konsol alat perangkat keras
- Mengkonfigurasi parameter jaringan alat perangkat keras
- Mengaktifkan Storage Gateway Hardware Appliance
- Membuat gateway pada perangkat keras Anda
- Mengkonfigurasi alamat IP gateway pada alat perangkat keras
- Menghapus perangkat lunak gateway dari alat perangkat keras Anda
- Menghapus Storage Gateway Hardware Appliance

Menyiapkan Storage Gateway Hardware Appliance Anda

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

Setelah menerima Storage Gateway Hardware Appliance, Anda menggunakan perangkat keras konsol lokal untuk mengonfigurasi jaringan guna menyediakan koneksi yang selalu aktif AWS dan mengaktifkan alat Anda. Aktivasi mengaitkan perangkat Anda dengan AWS akun yang digunakan selama proses aktivasi. Setelah alat diaktifkan, Anda dapat meluncurkan S3 File Gateway, FSx File Gateway, Tape Gateway, atau Volume Gateway dari konsol Storage Gateway.

Untuk menginstal dan mengkonfigurasi alat perangkat keras Anda

1. Pasang alat di rak, dan colokkan koneksi daya dan jaringan. Untuk informasi selengkapnya, lihat Memasang alat perangkat keras Anda secara fisik.
2. Atur alamat Internet Protocol versi 4 (IPv4) untuk perangkat keras (host). Untuk informasi selengkapnya, lihat Mengkonfigurasi parameter jaringan alat perangkat keras.
3. Aktifkan alat perangkat keras di halaman ikhtisar alat perangkat keras konsol di AWS Wilayah pilihan Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Storage Gateway Hardware Appliance.

4. Buat gateway pada alat perangkat keras Anda. Untuk informasi selengkapnya, lihat Membuat Volume Gateway.

   Anda mengatur gateway pada perangkat keras Anda dengan cara yang sama seperti Anda mengatur gateway, 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 1,92 TB SSDs (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 AWS Support untuk petunjuk tentang cara melakukan ini.
2. Tambahkan lima 1,92 TB SSDs ke alat.

Opsi kartu antarmuka jaringan

Tergantung pada model alat yang Anda pesan, mungkin dilengkapi dengan RJ45 tembaga 10G-Base-T, atau kartu jaringan 10G DA/SFP+.

- 10 konfigurasi G-Base-T NIC:
  - Gunakan CAT6 kabel 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 1 atau 10G-Base-T G-Base-T

Memasang alat perangkat keras Anda secara fisik

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

Alat Anda memiliki faktor bentuk 1U dan cocok dengan rak 19 inci yang sesuai dengan Komisi Elektroteknik Internasional (IEC) standar.

Prasyarat

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

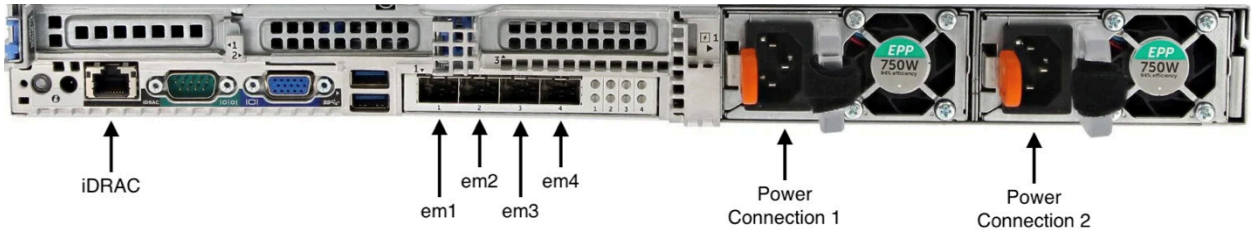
- Kabel daya: satu diperlukan, dua direkomendasikan.
- Kabel jaringan yang didukung (tergantung pada Kartu Antarmuka Jaringan (NIC) yang disertakan dalam alat perangkat keras). Twinax Copper DAC, modul optik SFP+(kompatibel dengan Intel) atau transceiver tembaga SFP ke Base-T.
- Keyboard dan monitor,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

> **Note**
>
> Sebelum Anda melakukan prosedur berikut, pastikan bahwa Anda memenuhi semua persyaratan untuk Storage Gateway Hardware Appliance seperti yang dijelaskan dalamPersyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance.

Untuk menginstal alat perangkat keras Anda secara fisik

1. Buka kotak perangkat keras Anda dan ikuti petunjuk yang terdapat di dalam kotak untuk memasang rak server.

Gambar berikut menunjukkan bagian belakang alat perangkat keras dengan port untuk menghubungkan daya, ethernet, monitor, keyboard USB, dan IDRac.
alat perangkat keras satu belakang dengan label konektor jaringan dan daya.

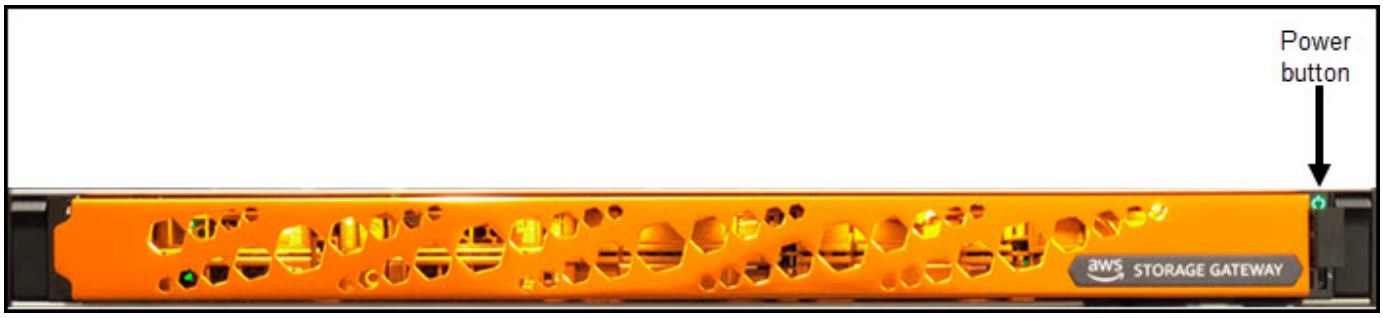


alat perangkat keras satu belakang dengan label konektor jaringan dan daya.

2. Colokkan sambungan daya ke masing-masing dari dua catu daya. Dimungkinkan untuk menyambungkan hanya ke satu koneksi daya, tetapi kami merekomendasikan koneksi daya ke kedua catu daya untuk redundansi.
3. Colokkan kabel Ethernet ke `em1` port untuk menyediakan koneksi internet yang selalu aktif. `em1`Port 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.

4. Colokkan keyboard dan monitor.
5. 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.

Langkah selanjutnya

[Mengakses konsol alat perangkat keras]

Mengakses konsol alat perangkat keras

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

Saat Anda menyalakan alat perangkat keras Anda, konsol alat perangkat keras muncul di monitor. Konsol perangkat keras menyajikan antarmuka pengguna khusus AWS yang dapat Anda gunakan untuk mengatur kata sandi administrator, mengonfigurasi parameter jaringan awal, dan membuka saluran dukungan AWS.

Untuk bekerja dengan konsol alat perangkat keras, masukkan teks dari keyboard dan gunakanUp,, `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.

Saat pertama kali konsol perangkat keras muncul, halaman Selamat Datang ditampilkan, dan Anda diminta untuk mengatur kata sandi untuk akun pengguna admin sebelum Anda dapat mengakses konsol.

Untuk mengatur kata sandi admin

- Pada prompt Harap atur kata sandi login Anda, lakukan hal berikut:

  a. Untuk Atur Kata Sandi, masukkan kata sandi, lalu tekan`Down arrow`.
  b. Untuk Konfirmasi, masukkan kembali kata sandi Anda, lalu pilih Simpan Kata Sandi.

Setelah Anda mengatur kata sandi, halaman Beranda konsol perangkat keras akan muncul. Halaman Beranda menampilkan informasi jaringan untuk antarmuka jaringan em1, em2, em3, dan em4, dan memiliki opsi menu berikut:

- Konfigurasikan Jaringan
- Buka Konsol Layanan
- Ubah Kata Sandi
- Keluar
- Buka Support Console

Langkah selanjutnya

Mengkonfigurasi parameter jaringan alat perangkat keras

Mengkonfigurasi parameter jaringan alat perangkat keras

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

Setelah perangkat keras dinyalakan dan Anda menyetel kata sandi pengguna admin di konsol perangkat keras seperti yang dijelaskan dalamMengakses konsol alat perangkat keras, gunakan prosedur berikut untuk mengonfigurasi parameter jaringan sehingga perangkat keras Anda dapat terhubung AWS.

Untuk mengatur alamat jaringan

1. Dari halaman Beranda, pilih Konfigurasi Jaringan dan kemudian tekan`Enter`. Halaman Konfigurasi Jaringan muncul. Halaman Konfigurasi Jaringan menunjukkan informasi IP dan DNS untuk masing-masing dari 4 antarmuka jaringan pada perangkat keras, dan termasuk opsi menu untuk mengonfigurasi alamat DHCP atau Statis untuk masing-masing.
2. Untuk antarmuka em1, lakukan salah satu hal berikut:

   - Pilih DHCP dan tekan `Enter` untuk menggunakan IPv4 alamat yang ditetapkan oleh server Dynamic Host Configuration Protocol (DHCP) Anda ke port jaringan fisik Anda.

Perhatikan alamat ini untuk digunakan nanti dalam langkah aktivasi.

- Pilih Statis dan tekan `Enter` untuk mengonfigurasi IPv4 alamat statis.

  Masukkan alamat IP yang valid, Subnet Mask, Gateway, dan alamat server DNS untuk antarmuka jaringan em1.

  Setelah selesai, pilih Simpan dan kemudian tekan `Enter` untuk menyimpan konfigurasi.

> **Note**
>
> Anda dapat menggunakan prosedur ini untuk mengkonfigurasi antarmuka jaringan lain selain em1. Jika Anda mengonfigurasi antarmuka lain, mereka harus menyediakan koneksi selalu aktif yang sama ke AWS titik akhir yang tercantum dalam persyaratan. Network bonding dan Link Aggregation Control Protocol (LACP) tidak didukung oleh perangkat keras atau oleh Storage Gateway.
> Kami tidak menyarankan mengonfigurasi beberapa antarmuka jaringan pada subnet yang sama karena ini terkadang dapat menyebabkan masalah perutean.

Untuk keluar dari konsol perangkat keras

1. Pilih Kembali dan tekan `Enter` untuk kembali ke halaman Beranda.
2. Pilih Logout dan tekan `Enter` untuk kembali ke halaman Selamat Datang.

Langkah selanjutnya

Mengaktifkan Storage Gateway Hardware Appliance

Mengaktifkan Storage Gateway Hardware Appliance

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk

memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

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 mendaftarkan alat ke AWS akun Anda.

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

1. Buka Konsol AWS Storage Gateway Manajemen dan masuk dengan kredensional 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 konfigurasikan untuk perangkat keras Anda, lalu pilih Connect.

   Untuk informasi selengkapnya tentang mengonfigurasi alamat IP, lihat .
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 dari mana 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 pada perangkat keras Anda

Membuat gateway pada perangkat keras Anda

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

Anda dapat membuat S3 File Gateway, FSx File Gateway, Tape Gateway, atau Volume Gateway pada Storage Gateway Hardware Appliance dalam penerapan Anda.

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/rumah.
2. Ikuti prosedur yang dijelaskan dalam Membuat Gateway Anda untuk menyiapkan, menghubungkan, dan mengonfigurasi jenis Storage Gateway yang ingin Anda gunakan.

Ketika Anda selesai membuat gateway Anda di konsol Storage Gateway, perangkat lunak Storage Gateway secara otomatis mulai menginstal pada perangkat keras. Jika Anda menggunakan Dynamic Host Configuration Protocol (DHCP), dibutuhkan waktu 5 hingga 10 menit agar gateway ditampilkan sebagai online di konsol. Untuk menetapkan alamat IP statis ke gateway yang diinstal, lihat alamat IP untuk gateway.

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 gateway pada alat perangkat keras

Mengkonfigurasi alamat IP gateway pada alat perangkat keras

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

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 perangkat keras Anda, konfigurasikan alamat IP dari konsol lokal gateway untuk gateway itu. Aplikasi Anda (seperti klien NFS atau SMB Anda) terhubung ke alamat IP ini. Anda dapat mengakses konsol lokal gateway dari konsol perangkat keras menggunakan opsi Open Service Console.

Untuk mengonfigurasi alamat IP pada alat Anda agar berfungsi dengan aplikasi

1. Pada konsol perangkat keras, pilih Open Service Console dan kemudian tekan `Enter` untuk membuka halaman login untuk konsol lokal gateway.
2. Halaman login konsol AWS Storage Gateway lokal meminta Anda untuk masuk untuk mengubah konfigurasi jaringan Anda dan pengaturan lainnya.

Akun default adalah `admin` dan kata sandi default adalah`password`.

> **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 gateway penyimpanan di konsol lokal untuk gateway lokal. Anda juga dapat mengatur kata sandi dari konsol Storage Gateway. Untuk informasi selengkapnya, lihat Mengatur Kata Sandi Konsol Lokal dari Konsol Storage Gateway.

3. Halaman AWS Appliance Activation - Configuration mencakup opsi menu berikut:

   - Konfigurasi Proksi HTTP/SOCKS
   - Konfigurasi Jaringan
   - Uji Konektivitas Jaringan
   - Lihat Pemeriksaan Sumber Daya Sistem
   - Sistem Manajemen Waktu
   - Informasi Lisensi
   - Command Prompt

   > **Note**
   >
   > Beberapa opsi hanya muncul untuk jenis gateway tertentu atau platform host.

   Masukkan angka yang sesuai untuk menavigasi ke halaman Konfigurasi Jaringan.

4. Lakukan salah satu hal berikut untuk mengonfigurasi alamat IP gateway:

   - Untuk menggunakan alamat IP yang ditetapkan oleh server Dynamic Host Configuration Protocol (DHCP), masukkan angka yang sesuai untuk Configure DHCP, lalu masukkan informasi konfigurasi DHCP yang valid di halaman berikut.
   - Untuk menetapkan alamat IP statis, masukkan angka yang sesuai untuk Konfigurasi IP Statis, lalu masukkan alamat IP dan informasi DNS yang valid di halaman berikut.

> **Note**
>
> Alamat IP yang Anda tentukan di sini harus berada di subnet yang sama dengan alamat IP yang digunakan selama aktivasi perangkat keras.

Untuk keluar dari konsol lokal gateway

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

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

Setelah perangkat keras Anda diaktifkan dan dikonfigurasi, alat Anda muncul di konsol. Sekarang Anda dapat melanjutkan prosedur penyiapan dan konfigurasi untuk gateway Anda di konsol Storage Gateway. Untuk petunjuk, lihat .

Menghapus perangkat lunak gateway dari alat perangkat keras Anda

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

Jika Anda tidak lagi memerlukan Storage Gateway tertentu yang telah digunakan pada perangkat perangkat keras, Anda dapat menghapus perangkat lunak gateway dari perangkat keras. Setelah Anda menghapus perangkat lunak gateway, Anda dapat memilih untuk menggunakan gateway baru

di tempatnya, atau menghapus perangkat keras itu sendiri dari konsol Storage Gateway. Untuk menghapus perangkat lunak gateway dari perangkat keras Anda, gunakan prosedur berikut.

Untuk menghapus gateway dari alat perangkat keras

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Perangkat Keras dari panel navigasi di sisi kiri halaman konsol, lalu pilih nama perangkat keras untuk alat tempat Anda ingin menghapus perangkat lunak gateway.
3. Dari menu tarik-turun Tindakan, pilih Hapus gateway.

   Kotak dialog konfirmasi muncul.
4. Verifikasi bahwa Anda ingin menghapus perangkat lunak gateway dari perangkat keras yang ditentukan, lalu ketikkan kata `remove` di kotak konfirmasi.
5. Pilih Hapus untuk menghapus perangkat lunak gateway secara permanen.

> **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, lihatMenghapus gateway Anda dan menghapus sumber daya terkait.

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

Menghapus Storage Gateway Hardware Appliance

> **Note**
>
> Pemberitahuan ketersediaan akhir: Mulai 12 Mei 2025, Peralatan AWS Storage Gateway Perangkat Keras tidak akan lagi ditawarkan. Pelanggan lama dengan AWS Storage Gateway Perangkat Keras dapat terus menggunakan dan menerima dukungan hingga Mei 2028. Sebagai alternatif, Anda dapat menggunakan AWS Storage Gateway layanan ini untuk memberi aplikasi Anda akses lokal dan di cloud ke penyimpanan cloud yang hampir tidak terbatas.

Jika Anda tidak lagi memerlukan Storage Gateway Hardware Appliance yang telah Anda aktifkan, 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 Dukungan untuk melakukan soft reset. Untuk informasi selengkapnya, lihat Mengaktifkan Dukungan akses untuk membantu memecahkan masalah gateway yang dihosting di 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, lihatMenghapus perangkat lunak gateway dari alat perangkat keras Anda.
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

Bagian ikhtisar pada 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 topik berikut:

- Membuat dan mengaktifkan Amazon S3 File Gateway
- Membuat dan mengaktifkan Amazon FSx File Gateway
- Membuat dan mengaktifkan Tape Gateway
- Membuat dan mengaktifkan Volume Gateway

> **Important**
>
> Amazon FSx File Gateway tidak lagi tersedia untuk pelanggan baru. Pelanggan FSx File Gateway yang ada dapat terus menggunakan layanan ini secara normal. Untuk kemampuan yang mirip dengan FSx File Gateway, kunjungi posting blog ini.

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 EC2 instans Amazon di lingkungan AWS 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 Anda 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 berbagi file Amazon S3 atau FSx Amazon untuk dikaitkan 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 Volume Gateway

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

Topik

- Siapkan Volume Gateway
- Connect Volume Gateway Anda ke AWS
- Tinjau pengaturan dan aktifkan Volume Gateway Anda
- Konfigurasikan Volume Gateway Anda

Siapkan Volume Gateway

Untuk menyiapkan Volume Gateway baru

1. Buka AWS Management Console di https://console.aws.amazon.com/storagegateway/rumah/, dan pilih di Wilayah AWS mana Anda ingin membuat gateway Anda.
2. Pilih Buat gateway untuk membuka halaman Atur 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 Volume Gateway, lalu pilih jenis volume yang akan digunakan gateway Anda. Anda dapat memilih dari opsi berikut:

   - Volume cache - Menyimpan data utama Anda di Amazon S3 dan menyimpan data yang sering diakses secara lokal dalam cache untuk akses yang lebih cepat.
   - Volume tersimpan - Menyimpan semua data Anda secara lokal sambil juga mencadangkannya secara asinkron ke Amazon S3. Gateway yang menggunakan jenis volume ini tidak dapat digunakan di Amazon. EC2
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 konfigurasikan mesin virtual gateway menggunakan VMware ESXi.
      - Microsoft Hyper-V - Unduh, gunakan, dan konfigurasikan mesin virtual gateway menggunakan Microsoft Hyper-V.

- Linux KVM - Unduh, gunakan, dan konfigurasikan mesin virtual gateway menggunakan Linux KVM.
- Amazon EC2 - Konfigurasikan dan luncurkan EC2 instans Amazon 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. Pilih Berikutnya untuk melanjutkan.

Sekarang gateway Anda sudah diatur, Anda harus memilih bagaimana Anda ingin terhubung dan berkomunikasi dengannya AWS. Untuk petunjuk, lihat Connect Volume Gateway Anda ke AWS.

Connect Volume Gateway Anda ke AWS

Untuk menghubungkan Volume Gateway baru ke AWS

1. Selesaikan prosedur yang dijelaskan dalam Mengatur Gerbang Volume 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 EC2 instans Amazon 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 Volume Gateway Anda.

Tinjau pengaturan dan aktifkan Volume Gateway Anda

Untuk mengaktifkan Volume Gateway baru

1. Lengkapi prosedur yang dijelaskan dalam topik berikut jika Anda belum melakukannya:

   - Siapkan Volume Gateway
   - Connect Volume 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 dibuat.

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 Volume Anda.

Konfigurasikan Volume Gateway Anda

Untuk melakukan konfigurasi pertama kali pada Volume Gateway baru

1. Lengkapi prosedur yang dijelaskan dalam topik berikut jika Anda belum melakukannya:

   - Siapkan Volume Gateway
   - Connect Volume Gateway Anda ke AWS
   - Tinjau pengaturan dan aktifkan Volume 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.

> **Note**
>
> Untuk menerima log kesehatan Storage Gateway, izin berikut harus ada dalam kebijakan sumber daya grup log Anda. Ganti *highlighted section* dengan informasi ResourcEarn grup log tertentu untuk penerapan Anda.
>
> ```
> "Sid": "AWSLogDeliveryWrite20150319",
>       "Effect": "Allow",
>       "Principal": {
>         "Service": [
>           "delivery.logs.amazonaws.com"
>         ]
>       },
>       "Action": [
>         "logs:CreateLogStream",
>         "logs:PutLogEvents"
>       ],
>       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
> ```
>
> Elemen “Resource” diperlukan hanya jika Anda ingin izin diterapkan secara eksplisit ke grup log individu.

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 — Konfigurasikan 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 volume untuk digunakan. Untuk petunjuk, lihat Membuat volume.

Membuat volume penyimpanan

Sebelumnya, Anda mengalokasikan disk lokal yang Anda tambahkan ke penyimpanan cache VM dan buffer unggah. Sekarang Anda membuat volume penyimpanan tempat aplikasi Anda membaca dan menulis data. Gateway mempertahankan data volume yang baru diakses secara lokal di penyimpanan cache, dan data yang ditransfer secara asinkron ke Amazon S3. Untuk volume tersimpan, Anda mengalokasikan disk lokal yang ditambahkan ke buffer unggahan VM dan data aplikasi Anda.

> **Note**
>
> Anda dapat menggunakan AWS Key Management Service (AWS KMS) untuk mengenkripsi data yang ditulis ke volume cache yang disimpan di Amazon S3. Saat ini, Anda dapat

melakukan ini dengan menggunakan Referensi AWS Storage Gateway API. Untuk informasi selengkapnya, lihat CreateCachediSCSIVolume atau create-cached-iscsi-volume.

Untuk membuat volume

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada konsol Storage Gateway, pilih Buat volume.
3. Di kotak dialog Buat volume, pilih gateway untuk Gateway.
4. Untuk volume yang di-cache, masukkan kapasitas dalam Kapasitas.

   Untuk volume yang disimpan, pilih nilai ID Disk dari daftar.
5. Untuk konten Volume, pilihan Anda bergantung pada jenis gateway yang Anda buat untuk volume.

   Untuk volume cache, Anda memiliki opsi berikut:

   - Buat volume kosong baru.
   - Buat volume berdasarkan snapshot Amazon EBS. Jika Anda memilih opsi ini, berikan nilai untuk ID snapshot EBS.

     > **Note**
     >
     > Storage Gateway tidak mendukung pembuatan volume cache dari snapshot volume. AWS Marketplace
   - Kloning dari titik pemulihan volume terakhir. Jika Anda memilih opsi ini, pilih ID volume untuk volume Sumber. Jika tidak ada volume di Wilayah, opsi ini tidak muncul.

   Untuk volume yang disimpan, Anda memiliki opsi berikut:

   - Buat volume kosong baru.
   - Buat volume berdasarkan snapshot. Jika Anda memilih opsi ini, berikan nilai untuk ID snapshot EBS.
   - Pertahankan data yang ada pada disk
6. Masukkan nama untuk nama target iSCSI.

Nama target dapat berisi huruf kecil, angka, titik (.), dan tanda hubung (-). Nama target ini muncul sebagai nama node target iSCSI di tab Target pada UI inisiator Microsoft iSCSI setelah penemuan. Misalnya, nama `target1` muncul sebagai`iqn.1007-05.com.amazon:target1`. Pastikan bahwa nama target secara global unik dalam jaringan area penyimpanan (SAN) Anda.

7. Verifikasi bahwa pengaturan antarmuka Jaringan memiliki alamat IP yang dipilih, atau pilih alamat IP untuk antarmuka Jaringan. Untuk antarmuka Jaringan, satu alamat IP muncul untuk setiap adaptor yang dikonfigurasi untuk VM gateway. Jika VM gateway dikonfigurasi hanya untuk satu adaptor jaringan, tidak ada daftar antarmuka Jaringan yang muncul karena hanya ada satu alamat IP.

   Target iSCSI Anda akan tersedia di adaptor jaringan yang Anda pilih.

   Jika Anda telah menentukan gateway Anda untuk menggunakan beberapa adaptor jaringan, pilih alamat IP yang harus digunakan aplikasi penyimpanan Anda untuk mengakses volume Anda. Untuk informasi tentang mengonfigurasi beberapa adaptor jaringan, lihatMengkonfigurasi Gateway Anda untuk Beberapa NICs.

   > **Note**
   >
   > Setelah Anda memilih adaptor jaringan, Anda tidak dapat mengubah pengaturan ini.

8. (Opsional) Untuk Tag, masukkan kunci dan nilai untuk menambahkan tag ke volume Anda. Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengelola, memfilter, dan mencari volume Anda.
9. Pilih Buat volume.

   Jika sebelumnya Anda telah membuat volume di Wilayah ini, Anda dapat melihatnya terdaftar di konsol Storage Gateway.

   Kotak dialog Configure CHAP Authentication muncul. Pada titik ini, Anda dapat mengkonfigurasi Challenge-Handshake Authentication Protocol (CHAP) untuk volume Anda, atau Anda dapat memilih Cancel dan mengkonfigurasi CHAP nanti. Untuk informasi selengkapnya tentang penyiapan CHAP, lihatKonfigurasikan otentikasi CHAP untuk volume Anda.

Jika Anda tidak ingin mengatur CHAP, mulailah menggunakan volume Anda. Untuk informasi selengkapnya, lihat Menghubungkan volume Anda ke klien Anda.

Konfigurasikan otentikasi CHAP untuk volume Anda

CHAP memberikan perlindungan terhadap serangan pemutaran dengan memerlukan otentikasi untuk mengakses target volume penyimpanan Anda. Dalam kotak dialog Configure CHAP Authentication, Anda memberikan informasi untuk mengkonfigurasi CHAP untuk volume Anda.

Untuk mengkonfigurasi CHAP

1. Pilih volume yang ingin Anda konfigurasikan CHAP.
2. Untuk Tindakan, pilih Konfigurasi otentikasi CHAP.
3. Untuk Nama Inisiator, masukkan nama inisiator Anda.
4. Untuk rahasia Inisiator, masukkan frase rahasia yang Anda gunakan untuk mengautentikasi inisiator iSCSI Anda.
5. Untuk rahasia Target, masukkan frase rahasia yang digunakan untuk mengotentikasi target Anda untuk CHAP bersama.
6. Pilih Simpan untuk menyimpan entri Anda.

   Untuk informasi selengkapnya tentang pengaturan otentikasi CHAP, lihat. Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda

Langkah selanjutnya

Menghubungkan volume Anda ke klien Anda

Menghubungkan volume Anda ke klien Anda

Anda menggunakan inisiator iSCSI di klien Anda untuk terhubung ke volume Anda. Pada akhir prosedur berikut, volume menjadi tersedia sebagai perangkat lokal pada klien Anda.

> **Important**
>
> Dengan Storage Gateway, Anda dapat menghubungkan beberapa host ke volume yang sama jika host mengoordinasikan akses dengan menggunakan Windows Server Failover Clustering (WSFC). Anda tidak dapat menghubungkan beberapa host ke volume yang sama tanpa menggunakan WSFC, misalnya dengan berbagi sistem file NTFS/ext4 yang tidak dikelompokkan.

Topik

Menghubungkan ke klien Microsoft Windows

Prosedur berikut menunjukkan ringkasan langkah-langkah yang Anda ikuti untuk terhubung ke klien Windows. Untuk informasi selengkapnya, lihat Menghubungkan Inisiator iSCSI.

Untuk terhubung ke klien Windows

1. Mulai iscsicpl.exe.
2. Di kotak dialog iSCSI Initiator Properties, pilih tab Discovery, lalu pilih Discovery Portal.
3. Di kotak dialog Discover Target Portal, ketik alamat IP target iSCSI Anda untuk alamat IP atau nama DNS.
4. Hubungkan portal target baru ke target volume penyimpanan di gateway.
5. Pilih target, lalu pilih Connect.
6. Di tab Target, pastikan status target memiliki nilai Terhubung, menunjukkan target terhubung, lalu pilih OK.

Menghubungkan ke klien Red Hat Enterprise Linux

Prosedur berikut menunjukkan ringkasan langkah-langkah yang Anda ikuti untuk terhubung ke klien Red Hat Enterprise Linux (RHEL). Untuk informasi selengkapnya, lihat Menghubungkan Inisiator iSCSI.

Untuk menghubungkan klien Linux ke target iSCSI

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, 8, atau 9, 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 akan terlihat seperti contoh output berikut.

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

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

4. Connect ke target.

Pastikan untuk menentukan yang benar *[GATEWAY_IP]* dan IQN 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
```

Kami sangat menyarankan bahwa setelah Anda mengatur inisiator Anda, Anda menyesuaikan pengaturan iSCSI Anda seperti yang dibahas di. Menyesuaikan Pengaturan iSCSI Linux Anda

Menginisialisasi dan memformat volume Anda

Setelah Anda menggunakan inisiator iSCSI di klien Anda untuk terhubung ke volume Anda, Anda menginisialisasi dan memformat volume Anda.

Topik

Menginisialisasi dan memformat volume Anda di Microsoft Windows

Gunakan prosedur berikut untuk menginisialisasi dan memformat volume Anda di Windows.

Untuk menginisialisasi dan memformat volume penyimpanan Anda

1. Mulai **`diskmgmt.msc`** membuka konsol Manajemen Disk.
2. Dalam kotak dialog Initialize Disk, inisialisasi volume sebagai partisi MBR (Master Boot Record). Saat memilih gaya partisi, Anda harus mempertimbangkan jenis volume yang Anda sambungkan — di-cache atau disimpan — seperti yang ditunjukkan pada tabel berikut.

Gaya Partisi	Gunakan dalam Ketentuan Berikut
MBR (Rekaman Boot Master)	• Jika gateway Anda adalah volume yang disimpan dan volume penyimpanan dibatasi hingga 1 TiB dalam ukuran. • Jika gateway Anda adalah volume cache dan volume penyimpanan kurang dari 2 TiB dalam ukuran.
GPT (Tabel Partisi GUID)	Jika volume penyimpanan gateway Anda berukuran 2 TiB atau lebih besar.

3. Buat volume sederhana:
   a. Bawa volume online untuk menginisialisasinya. Semua volume yang tersedia ditampilkan di konsol manajemen disk.
   b. Buka menu konteks (klik kanan) untuk disk, lalu pilih New Simple Volume.

> **Important**
>
> Berhati-hatilah untuk tidak memformat disk yang salah. Periksa untuk memastikan bahwa disk yang Anda format cocok dengan ukuran disk lokal yang Anda alokasikan ke VM gateway dan memiliki status Unallocated.

c. Tentukan ukuran disk maksimum.

d. Tetapkan huruf drive atau jalur ke volume Anda, dan format volume dengan memilih Lakukan format cepat.

> **Important**
>
> Kami sangat menyarankan menggunakan Lakukan format cepat untuk volume yang di-cache. Melakukannya menghasilkan inisialisasi I/O yang lebih sedikit, ukuran snapshot awal yang lebih kecil, dan waktu tercepat untuk volume yang dapat digunakan. Ini juga menghindari penggunaan ruang volume cache untuk proses format penuh.

> **Note**
>
> Waktu yang diperlukan untuk memformat volume tergantung pada ukuran volume. Prosesnya mungkin memakan waktu beberapa menit untuk menyelesaikannya.

Menginisialisasi dan memformat volume Anda di Red Hat Enterprise Linux

Gunakan prosedur berikut untuk menginisialisasi dan memformat volume Anda di Red Hat Enterprise Linux (RHEL).

Untuk menginisialisasi dan memformat volume penyimpanan Anda

1. Ubah direktori ke `/dev` folder.
2. Jalankan perintah `sudo cfdisk`.
3. Identifikasi volume baru Anda dengan menggunakan perintah berikut. Untuk menemukan volume baru, Anda dapat membuat daftar tata letak partisi volume Anda.

```
$ lsblk
```

Kesalahan “label volume tidak dikenal” untuk volume baru yang tidak dipartisi muncul.

4. Inisialisasi volume baru Anda. Saat memilih gaya partisi, Anda harus mempertimbangkan ukuran dan jenis volume yang Anda sambungkan — di-cache atau disimpan — seperti yang ditunjukkan pada tabel berikut.

Gaya Partisi	Gunakan dalam Ketentuan Berikut
MBR (Rekaman Boot Master)	• Jika gateway Anda adalah volume yang disimpan dan volume penyimpanan dibatasi hingga 1 TiB dalam ukuran. • Jika gateway Anda adalah volume cache dan volume penyimpanan kurang dari 2 TiB dalam ukuran.
GPT (Tabel Partisi GUID)	Jika volume penyimpanan gateway Anda berukuran 2 TiB atau lebih besar.

Untuk partisi MBR, gunakan perintah berikut: `sudo parted /dev/your volume mklabel msdos`

Untuk partisi GPT, gunakan perintah berikut: `sudo parted /dev/your volume mklabel gpt`

5. Buat partisi dengan menggunakan perintah berikut.

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

6. Tetapkan huruf drive ke partisi dan buat sistem file dengan menggunakan perintah berikut.

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

7. Pasang sistem file dengan menggunakan perintah berikut.

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

Menguji gateway Anda

Anda menguji penyiapan Volume Gateway dengan melakukan tugas-tugas berikut:

1. Tulis data ke volume.
2. Ambil snapshot.
3. Kembalikan snapshot ke volume lain.

Anda memverifikasi pengaturan untuk gateway dengan mengambil cadangan snapshot volume Anda dan menyimpan snapshot di dalamnya. AWS Anda kemudian mengembalikan snapshot ke volume baru. Gateway Anda menyalin data dari snapshot yang ditentukan AWS ke volume baru.

> **Note**
>
> Memulihkan data dari volume Amazon Elastic Block Store (Amazon EBS) yang dienkripsi tidak didukung.

Untuk membuat snapshot Amazon EBS dari volume penyimpanan di Microsoft Windows

1. Di komputer Windows Anda, salin beberapa data ke volume penyimpanan yang dipetakan.

   Jumlah data yang disalin tidak masalah untuk demonstrasi ini. File kecil sudah cukup untuk menunjukkan proses pemulihan.
2. Di panel navigasi konsol Storage Gateway, pilih Volume.
3. Pilih volume penyimpanan yang Anda buat untuk gateway.

   Gateway ini seharusnya hanya memiliki satu volume penyimpanan. Pilih volume menampilkan propertinya.
4. Untuk Tindakan, pilih Buat snapshot EBS untuk membuat snapshot volume.

   Bergantung pada jumlah data pada disk dan bandwidth unggahan, mungkin perlu beberapa detik untuk menyelesaikan snapshot. Perhatikan ID volume untuk volume tempat Anda membuat snapshot. Anda menggunakan ID untuk menemukan snapshot.
5. Di kotak dialog Create EBS Snapshot, berikan deskripsi untuk snapshot Anda.
6. (Opsional) Untuk Tag, masukkan kunci dan nilai untuk menambahkan tag ke snapshot. Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengelola, memfilter, dan mencari snapshot Anda.
7. Pilih Buat Snapshot. Snapshot Anda disimpan sebagai snapshot Amazon EBS. Catat ID snapshot Anda. Jumlah snapshot yang dibuat untuk volume Anda ditampilkan di kolom snapshot.

8. Di kolom snapshot EBS, pilih tautan untuk volume yang Anda buat snapshot untuk melihat snapshot EBS Anda di konsol Amazon. EC2

Untuk mengembalikan snapshot ke volume lain

Lihat Membuat volume penyimpanan.

Mencadangkan volume Anda

Dengan menggunakan Storage Gateway, Anda dapat membantu melindungi aplikasi bisnis lokal yang menggunakan volume Storage Gateway untuk penyimpanan yang didukung cloud. Anda dapat mencadangkan volume Storage Gateway lokal menggunakan penjadwal snapshot asli di Storage Gateway atau. AWS Backup Dalam kedua kasus tersebut, cadangan volume Storage Gateway disimpan sebagai snapshot Amazon EBS di Amazon Web Services.

Topik

- Menggunakan Storage Gateway untuk mencadangkan volume Anda
- Menggunakan AWS Backup untuk mencadangkan volume Anda

Menggunakan Storage Gateway untuk mencadangkan volume Anda

Anda dapat menggunakan Storage Gateway Management Console untuk mencadangkan volume dengan mengambil snapshot Amazon EBS dan menyimpan snapshot di Amazon Web Services. Anda dapat mengambil snapshot satu kali atau mengatur jadwal snapshot yang dikelola oleh Storage Gateway. Anda nantinya dapat mengembalikan snapshot ke volume baru dengan menggunakan konsol Storage Gateway. Untuk informasi tentang cara mencadangkan dan mengelola cadangan Anda dari Storage Gateway, lihat topik berikut:

- Menguji gateway Anda
- Membuat snapshot pemulihan
- Mengkloning volume yang di-cache dari titik pemulihan

Menggunakan AWS Backup untuk mencadangkan volume Anda

AWS Backup adalah layanan pencadangan terpusat yang memudahkan dan hemat biaya bagi Anda untuk mencadangkan data aplikasi di seluruh AWS layanan di Amazon Web Services Cloud

dan lokal. Melakukan hal ini membantu Anda memenuhi persyaratan kepatuhan cadangan bisnis dan peraturan Anda. AWS Backup membuat melindungi volume AWS penyimpanan, database, dan sistem file Anda menjadi sederhana dengan menyediakan tempat sentral di mana Anda dapat melakukan hal berikut:

- Konfigurasikan dan audit AWS sumber daya yang ingin Anda cadangkan.
- Otomatiskan penjadwalan cadangan.
- Tetapkan kebijakan penyimpanan.
- Pantau semua aktivitas backup dan pemulihan terbaru.

Karena Storage Gateway terintegrasi dengan AWS Backup, ini memungkinkan pelanggan menggunakan AWS Backup untuk mencadangkan aplikasi bisnis lokal yang menggunakan volume Storage Gateway untuk penyimpanan yang didukung cloud. AWS Backup mendukung pencadangan dan pemulihan volume cache dan tersimpan. Untuk informasi tentang AWS Backup, lihat AWS Backup dokumentasi. Untuk informasi tentang AWS Backup, lihat Apa itu AWS Backup? dalam AWS Backup User Guide.

Anda dapat mengelola operasi pencadangan dan pemulihan volume Storage Gateway dengan AWS Backup dan menghindari kebutuhan untuk membuat skrip khusus atau mengelola point-in-time cadangan secara manual. Dengan AWS Backup, Anda juga dapat memantau pencadangan volume lokal bersama AWS sumber daya in-cloud Anda dari satu dasbor. AWS Backup Anda dapat menggunakan AWS Backup untuk membuat cadangan on-demand satu kali atau menentukan rencana cadangan yang dikelola. AWS Backup

Pencadangan volume Storage Gateway yang diambil dari AWS Backup disimpan di Amazon S3 sebagai snapshot Amazon EBS. Anda dapat melihat cadangan volume Storage Gateway dari AWS Backup konsol atau konsol Amazon EBS.

Anda dapat dengan mudah memulihkan volume Storage Gateway yang dikelola melalui AWS Backup gateway lokal atau gateway di cloud. Anda juga dapat mengembalikan volume tersebut ke volume Amazon EBS yang dapat Anda gunakan dengan EC2 instans Amazon.

Manfaat Menggunakan AWS Backup untuk Mencadangkan Volume Storage Gateway

Manfaat menggunakan AWS Backup untuk mencadangkan volume Storage Gateway adalah Anda dapat memenuhi persyaratan kepatuhan, menghindari beban operasional, dan memusatkan manajemen cadangan. AWS Backup memungkinkan Anda melakukan hal berikut:

- Tetapkan kebijakan pencadangan terjadwal yang dapat disesuaikan yang memenuhi persyaratan pencadangan Anda.
- Tetapkan aturan retensi dan kedaluwarsa cadangan sehingga Anda tidak perlu lagi mengembangkan skrip khusus atau mengelola point-in-time cadangan volume Anda secara manual.
- Kelola dan pantau cadangan di beberapa gateway, dan AWS sumber daya lainnya dari tampilan pusat.

Untuk digunakan AWS Backup untuk membuat cadangan volume Anda

> **Note**
>
> AWS Backup mengharuskan Anda memilih peran AWS Identity and Access Management (IAM) yang AWS Backup dikonsumsi. Anda perlu membuat peran ini karena AWS Backup tidak membuatnya untuk Anda. Anda juga perlu menciptakan hubungan kepercayaan antara AWS Backup dan peran IAM ini. Untuk informasi tentang cara melakukannya, lihat Panduan AWS Backup Pengguna. Untuk selengkapnya tentang cara melakukannya, lihat Membuat Rencana Cadangan di Panduan AWS Backup Pengguna.

1. Buka konsol Storage Gateway dan pilih Volume dari panel navigasi di sebelah kiri.
2. Untuk Tindakan, pilih Buat cadangan sesuai permintaan dengan AWS Backup atau Buat paket AWS cadangan.

   Jika Anda ingin membuat cadangan volume Storage Gateway sesuai permintaan, pilih Buat cadangan sesuai permintaan dengan. AWS Backup Anda diarahkan AWS Backup konsol.

   Jika Anda ingin membuat AWS Backup rencana baru, pilih Buat rencana AWS cadangan. Anda diarahkan ke AWS Backup konsol.

   Di AWS Backup konsol, Anda dapat membuat paket cadangan, menetapkan volume Storage Gateway ke paket cadangan, dan membuat cadangan. Anda juga dapat melakukan tugas manajemen cadangan yang sedang berlangsung.

Menemukan dan memulihkan volume Anda dari AWS Backup

Anda dapat menemukan dan memulihkan volume Storage Gateway cadangan Anda dari AWS Backup konsol. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Backup . Untuk informasi selengkapnya, lihat Poin Pemulihan di Panduan AWS Backup Pengguna.

Untuk menemukan dan mengembalikan volume Anda

1. Buka AWS Backup konsol dan temukan cadangan volume Storage Gateway yang ingin Anda pulihkan. Anda dapat memulihkan cadangan volume Storage Gateway ke volume Amazon EBS atau ke volume Storage Gateway. Pilih opsi yang sesuai untuk persyaratan pemulihan Anda.
2. Untuk jenis Restore, pilih untuk mengembalikan volume Storage Gateway yang disimpan atau di-cache dan berikan informasi yang diperlukan:
   - Untuk volume yang disimpan, berikan informasi untuk nama Gateway, ID Disk, dan nama target iSCSI.
   - Untuk volume cache, berikan informasi untuk nama Gateway, Kapasitas, dan nama target iSCSI.
3. Pilih Pulihkan sumber daya untuk mengembalikan volume Anda.

> **Note**
>
> Anda tidak dapat menggunakan konsol Amazon EBS untuk menghapus snapshot yang dibuat oleh. AWS Backup

Dari sini, ke mana lagi?

Di bagian sebelumnya, Anda membuat dan menyediakan gateway dan kemudian menghubungkan host Anda ke volume penyimpanan gateway. Anda menambahkan data ke volume iSCSI gateway, mengambil snapshot volume, dan mengembalikannya ke volume baru, terhubung ke volume baru, dan memverifikasi bahwa data muncul di dalamnya.

Setelah Anda menyelesaikan latihan, pertimbangkan hal berikut:

- Jika Anda berencana untuk terus menggunakan gateway, baca tentang mengukur buffer unggahan dengan lebih tepat untuk beban kerja dunia nyata. Untuk informasi selengkapnya, lihat Mengukur Penyimpanan Volume Gateway Anda untuk Beban Kerja Dunia Nyata.

Bagian lain dari panduan ini mencakup informasi tentang cara melakukan hal berikut:

- Untuk mempelajari lebih lanjut tentang volume penyimpanan dan cara mengelolanya, lihatMengelola Volume Gateway Anda.
- Jika Anda tidak berencana untuk terus menggunakan gateway Anda, pertimbangkan untuk menghapus gateway untuk menghindari biaya apa pun. Untuk informasi selengkapnya, lihat Membersihkan sumber daya yang tidak perlu.
- Untuk memecahkan masalah gateway, lihat. Pemecahan masalah gateway
- Untuk mengoptimalkan gateway Anda, lihatMengoptimalkan kinerja gateway.
- Untuk mempelajari metrik Storage Gateway dan bagaimana Anda dapat memantau kinerja gateway Anda, lihatMemantau Storage Gateway.
- Untuk mempelajari lebih lanjut tentang mengonfigurasi target iSCSI gateway Anda untuk menyimpan data, lihat. Menghubungkan ke volume Anda dari klien Windows

Untuk mempelajari ukuran penyimpanan Volume Gateway Anda untuk beban kerja dunia nyata dan membersihkan sumber daya yang tidak Anda perlukan, lihat bagian berikut.

Mengukur Penyimpanan Volume Gateway Anda untuk Beban Kerja Dunia Nyata

Pada titik ini, Anda memiliki gateway yang sederhana dan berfungsi. Namun, asumsi yang digunakan untuk membuat gateway ini tidak sesuai untuk beban kerja dunia nyata. Jika Anda ingin menggunakan gateway ini untuk beban kerja dunia nyata, Anda perlu melakukan dua hal:

1. Ukur buffer unggahan Anda dengan tepat.
2. Siapkan pemantauan untuk buffer unggahan Anda, jika Anda belum melakukannya.

Setelah itu, Anda dapat menemukan cara melakukan kedua tugas ini. Jika Anda mengaktifkan gateway untuk volume cache, Anda juga perlu mengukur penyimpanan cache Anda untuk beban kerja dunia nyata.

Untuk mengukur buffer unggahan dan penyimpanan cache Anda untuk pengaturan cache gateway

- Gunakan rumus yang ditunjukkan Menentukan ukuran buffer unggahan yang akan dialokasikan untuk mengukur buffer unggahan. Kami sangat menyarankan Anda mengalokasikan setidaknya

150 GiB untuk buffer unggahan. Jika rumus buffer upload menghasilkan nilai kurang dari 150 GiB, gunakan 150 GiB sebagai buffer upload yang dialokasikan.

Rumus buffer upload memperhitungkan perbedaan antara throughput dari aplikasi Anda ke gateway dan throughput dari gateway Anda ke AWS, dikalikan dengan berapa lama Anda berharap untuk menulis data. Misalnya, asumsikan bahwa aplikasi Anda menulis data teks ke gateway Anda dengan kecepatan 40 MB per detik selama 12 jam sehari dan throughput jaringan Anda adalah 12 MB per detik. Dengan asumsi faktor kompresi 2:1 untuk data teks, rumus menentukan bahwa Anda perlu mengalokasikan sekitar 675 GiB ruang buffer unggah.

Untuk mengukur buffer unggahan Anda untuk penyiapan tersimpan

- Gunakan rumus yang dibahas diMenentukan ukuran buffer unggahan yang akan dialokasikan. Kami sangat menyarankan Anda mengalokasikan setidaknya 150 GiB untuk buffer unggahan Anda. Jika rumus buffer upload menghasilkan nilai kurang dari 150 GiB, gunakan 150 GiB sebagai buffer upload yang dialokasikan.

  Rumus buffer upload memperhitungkan perbedaan antara throughput dari aplikasi Anda ke gateway dan throughput dari gateway Anda ke AWS, dikalikan dengan berapa lama Anda berharap untuk menulis data. Misalnya, asumsikan bahwa aplikasi Anda menulis data teks ke gateway Anda dengan kecepatan 40 MB per detik selama 12 jam sehari dan throughput jaringan Anda adalah 12 MB per detik. Dengan asumsi faktor kompresi 2:1 untuk data teks, rumus menentukan bahwa Anda perlu mengalokasikan sekitar 675 GiB ruang buffer unggah.

Untuk memantau buffer unggahan Anda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih tab Gateway, pilih tab Detail, lalu temukan bidang Upload Buffer Used untuk melihat buffer upload gateway Anda saat ini.
3. Setel satu atau beberapa alarm untuk memberi tahu Anda tentang penggunaan buffer upload.

   Kami sangat menyarankan Anda membuat satu atau beberapa alarm buffer unggahan di konsol Amazon CloudWatch . Misalnya, Anda dapat mengatur alarm untuk tingkat penggunaan yang ingin Anda peringatkan dan alarm untuk tingkat penggunaan yang, jika terlampaui, adalah penyebab tindakan. Tindakannya mungkin menambahkan lebih banyak ruang buffer unggah. Untuk informasi selengkapnya, lihat Untuk menyetel alarm ambang batas atas untuk buffer unggahan gateway.

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 VPCs, 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 Menghubungkan Gateway Volume Anda 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/
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 Volume Gateway Anda

Mengelola gateway Anda mencakup tugas-tugas seperti mengonfigurasi penyimpanan cache dan mengunggah ruang buffer, bekerja dengan volume, dan melakukan pemeliharaan umum. Jika Anda belum membuat gateway, lihatMemulai dengan AWS Storage Gateway.

Volume cache adalah volume di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang diekspos sebagai target iSCSI tempat Anda dapat menyimpan data aplikasi Anda. Anda dapat menemukan informasi berikut tentang cara menambah dan menghapus volume untuk pengaturan cache Anda. Anda juga dapat mempelajari cara menambahkan dan menghapus volume Amazon Elastic Block Store (Amazon EBS) di gateway Amazon. EC2

> **Important**
>
> Jika volume cache menyimpan data primer Anda di Amazon S3, Anda harus menghindari proses yang membaca atau menulis semua data di seluruh volume. Misalnya, kami tidak menyarankan menggunakan perangkat lunak pemindaian virus yang memindai seluruh volume yang di-cache. Pemindaian semacam itu, baik dilakukan sesuai permintaan atau dijadwalkan, menyebabkan semua data yang disimpan di Amazon S3 diunduh secara lokal untuk pemindaian, yang menghasilkan penggunaan bandwidth tinggi. Alih-alih melakukan pemindaian disk penuh, Anda dapat menggunakan pemindaian virus waktu nyata — yaitu memindai data saat dibaca dari atau ditulis ke volume yang di-cache.

Mengubah ukuran volume tidak didukung. Untuk mengubah ukuran volume, buat snapshot volume, lalu buat volume cache baru dari snapshot. Volume baru bisa lebih besar dari volume dari mana snapshot dibuat. Untuk langkah-langkah yang menjelaskan cara menghapus volume, lihatUntuk menghapus volume. Untuk langkah-langkah yang menjelaskan cara menambahkan volume dan mempertahankan data yang ada, lihatMenghapus volume penyimpanan.

Semua data volume cache dan data snapshot disimpan di Amazon S3 dan dienkripsi saat istirahat menggunakan enkripsi sisi server (SSE). Namun, Anda tidak dapat mengakses data ini dengan menggunakan Amazon S3 API atau alat lain seperti Konsol Manajemen Amazon S3.

Berikut ini, Anda dapat menemukan informasi tentang cara mengelola sumber daya Volume Gateway Anda.

Topik

- Mengedit Informasi Gateway Dasar- Pelajari cara menggunakan konsol Storage Gateway untuk mengedit informasi dasar untuk gateway yang ada, termasuk nama gateway, zona waktu, dan grup CloudWatch log.
- Menambahkan dan memperluas volume- Pelajari cara menambahkan lebih banyak volume ke gateway Anda, atau memperluas ukuran volume yang ada saat kebutuhan aplikasi Anda bertambah.
- Mengkloning volume yang di-cache dari titik pemulihan- Pelajari cara membuat volume baru dari titik pemulihan volume yang ada, yang merupakan titik waktu yang disimpan ketika semua data pada volume konsisten.
- Melihat penggunaan volume- Pelajari cara melihat jumlah data yang disimpan pada volume dengan menggunakan konsol Storage Gateway.
- Menghapus volume penyimpanan- Pelajari cara menghapus volume jika aplikasi Anda perlu diubah, seperti jika Anda memigrasikan aplikasi untuk menggunakan volume penyimpanan yang lebih besar.
- Memindahkan Volume Anda ke Gateway yang Berbeda- Pelajari cara melepaskan dan memasang kembali volume, yang berguna jika Anda perlu memindahkan volume ke Volume Gateway yang berbeda karena kinerja Anda perlu berubah.
- Membuat snapshot pemulihan- Pelajari cara membuat snapshot pemulihan dari titik pemulihan volume untuk gateway, dan di mana menemukan snapshot itu di konsol Storage Gateway setelah Anda membuatnya.
- Mengedit jadwal snapshot- Pelajari cara menyesuaikan jadwal snapshot dengan mengubah waktu snapshot terjadi setiap hari atau frekuensi pengambilan snapshot.
- Menghapus snapshot dari volume penyimpanan Anda- Pelajari cara menghapus snapshot yang tidak perlu saat Anda tidak lagi membutuhkannya.
- Memahami Status Volume dan Transisi- Pelajari tentang berbagai nilai status volume yang dilaporkan Storage Gateway untuk membantu menentukan apakah volume berfungsi normal, atau jika ada masalah yang mungkin memerlukan tindakan dari pihak Anda.
- Memindahkan data Anda ke gateway baru- Pelajari cara memindahkan data antar gateway saat data dan kebutuhan kinerja Anda bertambah, atau jika Anda menerima AWS pemberitahuan untuk memigrasi gateway Anda.

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/rumah.
2. Pilih Gateway, lalu pilih gateway yang ingin Anda edit informasi dasarnya.
3. Dari menu tarik-turun Tindakan, pilih Edit informasi gateway.
4. Untuk nama Gateway, masukkan nama untuk gateway Anda. Anda dapat mencari nama ini untuk menemukan gateway Anda di halaman daftar di konsol Storage Gateway.

   > **Note**
   >
   > Nama gateway harus antara 2 dan 255 karakter, dan tidak dapat menyertakan garis miring (\atau/).
   > Mengubah nama gateway akan memutuskan CloudWatch alarm apa pun yang diatur untuk memantau gateway. Untuk menghubungkan kembali alarm, perbarui GatewayNameuntuk setiap alarm di konsol. CloudWatch

5. Untuk zona waktu Gateway, pilih zona waktu lokal untuk bagian dunia tempat Anda ingin menggunakan gateway Anda.
6. Untuk Pilih cara mengatur grup 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 daftar dropdown yang sesuai.
   - Nonaktifkan logging — Jangan gunakan Amazon CloudWatch Logs untuk memantau gateway Anda.

7. Setelah Anda selesai memodifikasi pengaturan yang ingin Anda ubah, pilih Simpan perubahan.

Menambahkan dan memperluas volume

Seiring kebutuhan aplikasi Anda tumbuh, Anda mungkin perlu menambahkan lebih banyak volume ke gateway Anda, atau memperluas ukuran volume yang ada. Saat Anda menambah atau memperluas

volume, Anda harus mempertimbangkan ukuran penyimpanan cache dan mengunggah buffer yang Anda alokasikan ke gateway. Gateway harus memiliki buffer dan ruang cache yang cukup untuk volume baru. Untuk informasi selengkapnya, lihat Menentukan ukuran buffer unggahan yang akan dialokasikan.

Anda dapat menambahkan volume menggunakan konsol Storage Gateway atau Storage Gateway API. Untuk petunjuk tentang cara menambahkan volume menggunakan konsol Storage Gateway, lihatMembuat volume penyimpanan. Untuk informasi tentang penggunaan Storage Gateway API untuk menambahkan volume, lihat CreateCachediSCSIVolume.

Anda dapat memperluas ukuran volume yang ada menggunakan salah satu metode berikut:

- Buat snapshot dari volume yang ingin Anda kembangkan dan kemudian gunakan snapshot untuk membuat volume baru dengan ukuran yang lebih besar. Untuk informasi tentang cara membuat snapshot, lihatMembuat snapshot pemulihan. Untuk informasi tentang cara menggunakan snapshot untuk membuat volume baru, lihatMembuat volume penyimpanan.
- Gunakan volume cache yang ingin Anda kembangkan untuk mengkloning volume baru dengan ukuran yang lebih besar. Untuk informasi tentang cara mengkloning volume, lihatMengkloning volume yang di-cache dari titik pemulihan. Untuk informasi tentang cara membuat volume, lihatMembuat volume penyimpanan.

Mengkloning volume yang di-cache dari titik pemulihan

Anda dapat membuat volume baru dari volume cache yang ada di AWS Wilayah yang sama. Volume baru dibuat dari titik pemulihan terbaru dari volume yang dipilih. Titik pemulihan volume adalah titik waktu di mana semua data volume konsisten. Untuk mengkloning volume, Anda memilih opsi Klon dari titik pemulihan terakhir di kotak dialog Buat volume, lalu pilih volume yang akan digunakan sebagai sumber.

Kloning dari volume yang ada lebih cepat dan lebih hemat biaya daripada membuat snapshot Amazon EBS. Kloning melakukan byte-to-byte salinan data Anda dari volume sumber ke volume baru, menggunakan titik pemulihan terbaru dari volume sumber. Storage Gateway secara otomatis membuat titik pemulihan untuk volume cache Anda. Untuk melihat kapan titik pemulihan terakhir dibuat, periksa `TimeSinceLastRecoveryPoint` metrik di Amazon CloudWatch.

Volume kloning tidak tergantung pada volume sumber. Artinya, perubahan yang dilakukan pada salah satu volume setelah kloning tidak berpengaruh pada yang lain. Misalnya, jika Anda menghapus volume sumber, itu tidak berpengaruh pada volume kloning. Anda dapat mengkloning volume sumber

saat inisiator terhubung dan sedang digunakan secara aktif. Melakukannya tidak mempengaruhi kinerja volume sumber. Untuk informasi tentang cara mengkloning volume, lihatMembuat volume penyimpanan.

Anda juga dapat menggunakan proses kloning dalam skenario pemulihan. Untuk informasi selengkapnya, lihat Gateway Cached Anda Tidak Dapat Dijangkau Dan Anda Ingin Memulihkan Data Anda.

Prosedur berikut menunjukkan kepada Anda cara mengkloning volume dari titik pemulihan volume dan menggunakan volume itu.

Untuk mengkloning dan menggunakan volume dari gateway yang tidak dapat dijangkau

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada konsol Storage Gateway, pilih Buat volume.
3. Di kotak dialog Buat volume, pilih gateway untuk Gateway.
4. Untuk Kapasitas, ketikkan kapasitas untuk volume Anda. Kapasitas harus setidaknya ukuran yang sama dengan volume sumber.
5. Pilih Clone dari titik pemulihan terakhir dan pilih ID volume untuk volume Sumber. Volume sumber dapat berupa volume cache apa pun di AWS Wilayah yang dipilih.
6. Ketik nama untuk nama target iSCSI.

   Nama target dapat berisi huruf kecil, angka, titik (.), dan tanda hubung (-). Nama target ini muncul sebagai nama node target iSCSI di tab Target pada UI inisiator Microsoft iSCSI setelah penemuan. Misalnya, nama `target1` muncul sebagai`iqn.1007-05.com.amazon:target1`. Pastikan bahwa nama target unik secara global dalam jaringan area penyimpanan (SAN) Anda.
7. Verifikasi bahwa pengaturan antarmuka Jaringan adalah alamat IP gateway Anda, atau pilih alamat IP untuk antarmuka Jaringan.

   Jika Anda telah menentukan gateway Anda untuk menggunakan beberapa adaptor jaringan, pilih alamat IP yang digunakan aplikasi penyimpanan Anda untuk mengakses volume. Setiap adaptor jaringan yang ditentukan untuk gateway mewakili satu alamat IP yang dapat Anda pilih.

   Jika VM gateway dikonfigurasi untuk lebih dari satu adaptor jaringan, kotak dialog Buat volume menampilkan daftar untuk antarmuka Jaringan. Dalam daftar ini, satu alamat IP muncul untuk setiap adaptor yang dikonfigurasi untuk VM gateway. Jika VM gateway dikonfigurasi hanya untuk satu adaptor jaringan, tidak ada daftar yang muncul karena hanya ada satu alamat IP.

8. Pilih Buat volume. Kotak dialog Configure CHAP Authentication muncul. Anda dapat mengkonfigurasi CHAP nanti. Untuk informasi, lihat Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda.

Langkah selanjutnya adalah menghubungkan volume Anda ke klien Anda. Untuk informasi selengkapnya, lihat Menghubungkan volume Anda ke klien Anda.

Melihat penggunaan volume

Saat Anda menulis data ke volume, Anda dapat melihat jumlah data yang disimpan pada volume di Storage Gateway Management Console. Tab Detail untuk setiap volume menampilkan informasi penggunaan volume.

Untuk melihat jumlah data yang ditulis ke volume

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi, pilih Volume dan kemudian pilih volume yang Anda minati.
3. Pilih tab Detail.

   Bidang berikut memberikan informasi tentang volume:

   - Ukuran: Total kapasitas volume yang dipilih.
   - Digunakan: Ukuran data yang disimpan pada volume.

   > **Note**
   >
   > Nilai-nilai ini tidak tersedia untuk volume yang dibuat sebelum 13 Mei 2015, hingga Anda menyimpan data pada volume.

Menghapus volume penyimpanan

Anda mungkin perlu menghapus volume karena aplikasi Anda perlu berubah—misalnya, jika Anda memigrasikan aplikasi untuk menggunakan volume penyimpanan yang lebih besar. Sebelum Anda menghapus volume, pastikan tidak ada aplikasi yang saat ini menulis ke volume. Juga, pastikan tidak ada snapshot yang sedang berlangsung untuk volume. Jika jadwal snapshot ditentukan untuk

volume, Anda dapat memeriksanya di tab Jadwal Snapshot di konsol Storage Gateway. Untuk informasi selengkapnya, lihat Mengedit jadwal snapshot.

Anda dapat menghapus volume menggunakan konsol Storage Gateway atau Storage Gateway API. Untuk informasi tentang penggunaan Storage Gateway API untuk menghapus volume, lihat Menghapus Volume. Prosedur berikut menunjukkan penggunaan konsol.

Sebelum Anda menghapus volume, buat cadangan data Anda atau ambil snapshot dari data penting Anda. Untuk volume yang disimpan, disk lokal Anda tidak dihapus. Setelah Anda menghapus volume, Anda tidak bisa mendapatkannya kembali.

Untuk menghapus volume

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Volume, lalu pilih satu atau beberapa volume yang akan dihapus.
3. Untuk Tindakan pilih Hapus volume. Kotak dialog konfirmasi muncul.
4. Verifikasi bahwa Anda ingin menghapus volume yang ditentukan, lalu ketik kata hapus di kotak konfirmasi dan pilih Hapus.

Memindahkan Volume Anda ke Gateway yang Berbeda

Seiring bertambahnya kebutuhan data dan kinerja, Anda mungkin ingin memindahkan volume ke Volume Gateway yang berbeda. Untuk melakukannya, Anda dapat melepaskan dan melampirkan volume dengan menggunakan konsol Storage Gateway atau API.

Dengan melepaskan dan melampirkan volume, Anda dapat melakukan hal berikut:

- Pindahkan volume Anda ke platform host yang lebih baik atau EC2 instans Amazon yang lebih baru.
- Segarkan perangkat keras yang mendasarinya untuk server Anda.
- Pindahkan volume Anda di antara tipe hypervisor.

Saat Anda melepaskan volume, gateway Anda mengunggah dan menyimpan data volume dan metadata ke layanan Storage Gateway di. AWS Anda dapat dengan mudah melampirkan volume terpisah ke gateway pada platform host yang didukung nanti.

> **Note**
>
> Volume terpisah ditagih pada tingkat penyimpanan volume standar hingga Anda menghapusnya. Untuk informasi tentang cara mengurangi tagihan Anda, lihatMengurangi jumlah penyimpanan yang ditagih pada volume.

> **Note**
>
> Ada beberapa batasan untuk melampirkan dan melepaskan volume:
>
> - Melepaskan volume bisa memakan waktu lama. Saat Anda melepaskan volume, gateway mengunggah semua data pada volume AWS sebelum volume terlepas. Waktu yang dibutuhkan untuk mengunggah untuk menyelesaikan tergantung pada berapa banyak data yang perlu diunggah dan konektivitas jaringan Anda. AWS
> - Jika Anda melepaskan volume yang di-cache, Anda tidak dapat memasangnya kembali sebagai volume yang disimpan.
> - Jika Anda melepaskan volume yang disimpan, Anda tidak dapat memasangnya kembali sebagai volume yang di-cache.
> - Volume terpisah tidak dapat digunakan sampai terpasang ke gateway.
> - Saat Anda melampirkan volume yang disimpan, volume harus dipulihkan sepenuhnya sebelum Anda dapat melampirkannya ke gateway.
> - Saat Anda mulai memasang atau melepaskan volume, Anda harus menunggu sampai operasi selesai sebelum Anda menggunakan volume.
> - Saat ini, menghapus volume secara paksa hanya didukung di API.
> - Jika Anda menghapus gateway saat volume Anda terlepas dari gateway itu, itu mengakibatkan kehilangan data. Tunggu hingga operasi pelepasan volume selesai sebelum Anda menghapus gateway.
> - Jika gateway tersimpan dalam status pemulihan, Anda tidak dapat melepaskan volume darinya.

Langkah-langkah berikut menunjukkan cara melepaskan dan melampirkan volume menggunakan konsol Storage Gateway. Untuk informasi selengkapnya tentang melakukan ini menggunakan API, lihat DetachVolumeatau AttachVolumedi Referensi AWS Storage Gateway API.

Untuk melepaskan volume dari gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Volume, pilih satu atau beberapa volume yang akan dilepas.
3. Untuk Tindakan, pilih Lepaskan volume. Kotak dialog konfirmasi muncul.
4. Verifikasi bahwa Anda ingin melepaskan volume yang ditentukan, lalu ketikkan kata lepas di kotak konfirmasi dan pilih Lepaskan.

> **Note**
>
> Jika volume yang Anda lepaskan memiliki banyak data di dalamnya, ia bertransisi dari status Terlampir ke Detaching hingga selesai mengunggah semua data. Kemudian status berubah menjadi Terpisah. Untuk sejumlah kecil data, Anda mungkin tidak melihat status Detaching. Jika volume tidak memiliki data di dalamnya, status berubah dari Terlampir ke Terpisah.

Anda sekarang dapat melampirkan volume ke gateway yang berbeda.

Untuk melampirkan volume ke gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada panel navigasi, pilih Volume. Status setiap volume yang terlepas ditampilkan sebagai Terpisah.
3. Dari daftar volume terpisah, pilih volume yang ingin Anda lampirkan. Anda hanya dapat melampirkan satu volume pada satu waktu.
4. Untuk Tindakan, pilih Lampirkan volume.
5. Dalam kotak dialog Lampirkan Volume, pilih gateway yang ingin Anda lampirkan volumenya, lalu masukkan target iSCSI yang ingin Anda sambungkan volumenya.

   Jika Anda melampirkan volume yang disimpan, masukkan pengenal disk untuk ID Disk.
6. Pilih Lampirkan volume. Jika volume yang Anda lampirkan memiliki banyak data di dalamnya, itu transisi dari Terpisah ke Terlampir jika `AttachVolume` operasi berhasil.
7. Di wizard Configure CHAP authentication yang muncul, masukkan nama Initiator, Initiator secret, dan Target secret, lalu pilih Save. Untuk informasi selengkapnya tentang bekerja dengan

otentikasi Challenge-Handshake Authentication Protocol (CHAP), lihat. Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda

Membuat snapshot pemulihan

Prosedur berikut menunjukkan cara membuat snapshot pemulihan dari titik pemulihan volume untuk gateway, dan di mana menemukan snapshot itu di konsol Storage Gateway setelah Anda membuatnya. Anda dapat mengambil snapshot pemulihan pada satu waktu, secara ad hoc atau Anda dapat mengatur jadwal snapshot untuk mengambil snapshot berulang dari volume secara berkala yang Anda tentukan.

Untuk membuat dan menggunakan snapshot pemulihan volume dari gateway yang ada

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi di sisi kiri halaman konsol, pilih Gateway.
3. Pilih gateway yang ingin Anda buat snapshot, lalu pilih tab Detail.

   Tab Detail menampilkan pesan snapshot pemulihan untuk gateway yang dipilih.
4. Pilih Buat snapshot pemulihan untuk membuka kotak dialog Buat snapshot pemulihan.
5. Dari daftar volume yang muncul, pilih volume yang ingin Anda pulihkan, lalu pilih Buat snapshot.

   Storage Gateway memulai proses snapshot untuk volume yang ditentukan. Ketika proses snapshot selesai, Anda dapat menemukan snapshot yang tercantum di kolom Snapshots saat melihat volume pada halaman Volume konsol Storage Gateway.

Mengedit jadwal snapshot

Untuk volume yang disimpan, AWS Storage Gateway buat jadwal snapshot default sekali sehari.

> **Note**
>
> Anda tidak dapat menghapus jadwal snapshot default. Volume yang disimpan memerlukan setidaknya satu jadwal snapshot. Namun, Anda dapat mengubah jadwal snapshot dengan menentukan waktu snapshot terjadi setiap hari atau frekuensi (setiap 1, 2, 4, 8, 12, atau 24 jam), atau keduanya.

Untuk volume yang di-cache, AWS Storage Gateway tidak membuat jadwal snapshot default. Tidak ada jadwal default yang dibuat karena data Anda disimpan di Amazon S3, sehingga Anda tidak memerlukan snapshot atau jadwal snapshot untuk tujuan pemulihan bencana. Namun, Anda dapat mengatur jadwal snapshot kapan saja jika perlu. Membuat snapshot untuk volume cache Anda menyediakan cara tambahan untuk memulihkan data Anda jika perlu.

Dengan menggunakan langkah-langkah berikut, Anda dapat mengedit jadwal snapshot untuk volume.

Untuk mengedit jadwal snapshot untuk volume

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi, pilih Volume, lalu pilih volume tempat snapshot dibuat.
3. Untuk Tindakan, pilih Edit jadwal snapshot.
4. Dalam kotak dialog Edit jadwal snapshot, ubah jadwal, lalu pilih Simpan.

Menghapus snapshot dari volume penyimpanan Anda

Anda dapat menghapus snapshot volume penyimpanan Anda. Misalnya, Anda mungkin ingin melakukan ini jika Anda telah mengambil banyak snapshot dari volume penyimpanan dari waktu ke waktu dan Anda tidak memerlukan snapshot yang lebih lama. Karena snapshot adalah cadangan tambahan, jika Anda menghapus snapshot, hanya data yang tidak diperlukan di snapshot lain yang dihapus.

Topik

- Menghapus Snapshot dengan Menggunakan AWS SDK for Java
- Menghapus Snapshot dengan Menggunakan AWS SDK untuk.NET
- Menghapus Snapshot dengan Menggunakan AWS Tools for Windows PowerShell

Di konsol Amazon EBS, Anda dapat menghapus snapshot satu per satu. Untuk informasi tentang cara menghapus snapshot menggunakan konsol Amazon EBS, lihat Menghapus Snapshot Amazon EBS di Panduan Pengguna Amazon. EC2

Untuk menghapus beberapa snapshot sekaligus, Anda dapat menggunakan salah satu AWS SDKs yang mendukung operasi Storage Gateway. Sebagai contoh, lihatMenghapus Snapshot dengan Menggunakan AWS SDK for Java,Menghapus Snapshot dengan Menggunakan AWS SDK untuk.NET, danMenghapus Snapshot dengan Menggunakan AWS Tools for Windows PowerShell.

Menghapus Snapshot dengan Menggunakan AWS SDK for Java

Untuk menghapus banyak snapshot yang terkait dengan volume, Anda dapat menggunakan pendekatan terprogram. Contoh berikut menunjukkan cara menghapus snapshot menggunakan AWS SDK for Java. Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan aplikasi konsol Java. Untuk informasi selengkapnya, lihat Memulai di AWS SDK for Java Developer Guide. Jika Anda hanya perlu menghapus beberapa snapshot, gunakan konsol seperti yang dijelaskan diMenghapus snapshot dari volume penyimpanan Anda.

Example : Menghapus Snapshot dengan Menggunakan AWS SDK for Java

Contoh kode Java berikut mencantumkan snapshot untuk setiap volume gateway dan apakah waktu mulai snapshot sebelum atau sesudah tanggal yang ditentukan. Ini menggunakan AWS SDK for Java API untuk Storage Gateway dan Amazon EC2. Amazon EC2 API mencakup operasi untuk bekerja dengan snapshot.

Perbarui kode untuk menyediakan titik akhir layanan, nama sumber daya Amazon gateway Anda (ARN), dan jumlah hari yang lalu Anda ingin menyimpan snapshot. Snapshot yang diambil sebelum cutoff ini dihapus. Anda juga perlu menentukan nilai Boolean`viewOnly`, yang menunjukkan apakah Anda ingin melihat snapshot yang akan dihapus atau benar-benar melakukan penghapusan snapshot. Jalankan kode terlebih dahulu hanya dengan opsi tampilan (yaitu, dengan `viewOnly` set `ketrue`) untuk melihat apa yang dihapus kode. 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 java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

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

```
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

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

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

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

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

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

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

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

        sgClient.setEndpoint(serviceURLSG);

        ec2Client = new AmazonEC2Client(new PropertiesCredentials(

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

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

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

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

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

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

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

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

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

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

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
```

```
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    ec2Client.deleteSnapshot(deleteSnapshotRequest);
                }
                else {
                    sb.append("no");
                }
                System.out.println(sb.toString());
            }
        }
    }

    private static String OutputVolumeInfo(VolumeInfo vi) {

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

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

}
```

Menghapus Snapshot dengan Menggunakan AWS SDK untuk.NET

Untuk menghapus banyak snapshot yang terkait dengan volume, Anda dapat menggunakan pendekatan terprogram. Contoh berikut menunjukkan cara menghapus snapshot menggunakan AWS SDK for .NET versi 2 dan 3. Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan aplikasi konsol.NET. Untuk informasi selengkapnya, lihat Memulai di AWS SDK

for .NET Developer Guide. Jika Anda hanya perlu menghapus beberapa snapshot, gunakan konsol seperti yang dijelaskan diMenghapus snapshot dari volume penyimpanan Anda.

Example : Menghapus Snapshot dengan Menggunakan AWS SDK untuk.NET

Dalam contoh kode C # berikut, AWS Identity and Access Management pengguna dapat membuat daftar snapshot untuk setiap volume gateway. Pengguna kemudian dapat menentukan apakah waktu mulai snapshot sebelum atau setelah tanggal tertentu (periode retensi) dan menghapus snapshot yang telah melewati periode retensi. Contoh menggunakan AWS SDK for .NET API untuk Storage Gateway dan Amazon EC2. Amazon EC2 API mencakup operasi untuk bekerja dengan snapshot.

Contoh kode berikut menggunakan AWS SDK for .NET versi 2 dan 3. Anda dapat memigrasikan versi.NET yang lebih lama ke versi yang lebih baru. Untuk informasi selengkapnya, lihat Memigrasi project Anda untuk AWS SDK for .NET.

Perbarui kode untuk menyediakan titik akhir layanan, nama sumber daya Amazon gateway Anda (ARN), dan jumlah hari yang lalu Anda ingin menyimpan snapshot. Snapshot yang diambil sebelum cutoff ini dihapus. Anda juga perlu menentukan nilai Boolean`viewOnly`, yang menunjukkan apakah Anda ingin melihat snapshot yang akan dihapus atau benar-benar melakukan penghapusan snapshot. Jalankan kode terlebih dahulu hanya dengan opsi tampilan (yaitu, dengan `viewOnly` set `ketrue`) untuk melihat apa yang dihapus kode. Untuk daftar endpoint AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat AWS Storage Gateway Endpoints dan Quotas di. Referensi Umum AWS

Pertama, Anda membuat pengguna dan melampirkan kebijakan IAM minimum ke pengguna. Kemudian Anda menjadwalkan snapshot otomatis untuk gateway Anda.

Kode berikut membuat kebijakan minimum yang memungkinkan pengguna menghapus snapshot. Dalam contoh ini, kebijakan diberi nama**`sgw-delete-snapshot`**.

JSON

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "StmtEC2Snapshots",
              "Effect": "Allow",
              "Action": [
                  "ec2:DeleteSnapshot",
```

```
                "ec2:DescribeSnapshots"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "StmtSgwListVolumes",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListVolumes"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Kode C# berikut menemukan semua snapshot di gateway yang ditentukan yang cocok dengan volume dan periode cut-off yang ditentukan dan kemudian menghapusnya.

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

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

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

        /* IAM SecretKey */
```

```
        static String AwsSecretKey = "******************************";

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

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

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

        static String SnapshotStatus = "completed";

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

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

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

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

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

            List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
            List<Snapshot> StorageGatewaySnapshots =
 ListSnapshotsForVolumes(StorageGatewayVolumes,
```

```
                                                        daysBack);
            DeleteSnapshots(StorageGatewaySnapshots);
        }

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

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

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

```
                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

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

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

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

                    DescribeSnapshotsResponse describeSnapshotsResponse =
                      ec2Client.DescribeSnapshots(describeSnapshotsRequest);

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

```
            }
            return SelectedSnapshots;
        }

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

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

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

        /*
         * Displays information related to a volume.
```

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

Menghapus Snapshot dengan Menggunakan AWS Tools for Windows PowerShell

Untuk menghapus banyak snapshot yang terkait dengan volume, Anda dapat menggunakan pendekatan terprogram. Contoh berikut menunjukkan cara menghapus snapshot menggunakan. AWS Tools for Windows PowerShell Untuk menggunakan contoh skrip, Anda harus terbiasa dengan menjalankan PowerShell skrip. Untuk informasi selengkapnya, lihat Memulai di AWS Tools for Windows PowerShell. Jika Anda perlu menghapus hanya beberapa snapshot, gunakan konsol seperti yang dijelaskan dalamMenghapus snapshot dari volume penyimpanan Anda.

Example : Menghapus Snapshot dengan Menggunakan AWS Tools for Windows PowerShell

Contoh PowerShell skrip berikut mencantumkan snapshot untuk setiap volume gateway dan apakah waktu mulai snapshot sebelum atau sesudah tanggal yang ditentukan. Ini menggunakan AWS Tools for Windows PowerShell cmdlet untuk Storage Gateway dan Amazon. EC2 Amazon EC2 API mencakup operasi untuk bekerja dengan snapshot.

Anda perlu memperbarui skrip dan memberikan gateway Anda Nama Sumber Daya Amazon (ARN) dan jumlah hari yang lalu Anda ingin menyimpan snapshot. Snapshot yang diambil sebelum cutoff ini dihapus. Anda juga perlu menentukan nilai Booleanviewonly, yang menunjukkan apakah Anda ingin melihat snapshot yang akan dihapus atau benar-benar melakukan penghapusan snapshot. Jalankan kode terlebih dahulu hanya dengan opsi tampilan (yaitu, dengan viewOnly set ketrue) untuk melihat apa yang dihapus kode.

```
<#
.DESCRIPTION
```

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

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

.EXAMPLE
    powershell.exe .\SG_DeleteSnapshots.ps1
#>

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

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

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

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

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

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
       $d = ([DateTime]::Now).AddDays(-$daysBack)
```

```
        $meetsCriteria = $false
        if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
        {
             $meetsCriteria = $true
        }

        $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
$meetsCriteria
        if (!$viewOnly -AND $meetsCriteria)
        {
            $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
            #Can get RequestId from response for troubleshooting.
            $sb = $sb + ", deleted? yes"
        }
        else {
            $sb = $sb + ", deleted? no"
        }
        Write-Output($sb)
    }
 }
```

Memahami Status Volume dan Transisi

Setiap volume memiliki status terkait yang memberi tahu Anda sekilas tentang kesehatan volume tersebut. Sebagian besar waktu, status menunjukkan bahwa volume berfungsi normal dan tidak ada tindakan yang diperlukan di pihak Anda. Dalam beberapa kasus, status menunjukkan masalah dengan volume yang mungkin atau mungkin tidak memerlukan tindakan dari pihak Anda. Anda dapat menemukan informasi berikut untuk membantu Anda memutuskan kapan Anda perlu bertindak. Anda dapat melihat status volume di konsol Storage Gateway atau dengan menggunakan salah satu operasi Storage Gateway API, misalnya DescribeCachediSCSIVolumesatau DescribeStorediSCSIVolumes.

Topik

- Memahami Status Volume
- Memahami Status Lampiran
- Memahami Transisi Status Volume yang Di-cache
- Memahami Transisi Status Volume Tersimpan

Memahami Status Volume

Tabel berikut menunjukkan status volume pada konsol Storage Gateway. Status volume muncul di kolom Status untuk setiap volume penyimpanan di gateway Anda. Volume yang berfungsi normal memiliki status Tersedia.

Dalam tabel berikut, Anda dapat menemukan deskripsi dari setiap status volume penyimpanan, dan jika dan kapan Anda harus bertindak berdasarkan setiap status. Status yang tersedia adalah status normal volume. Volume harus memiliki status ini sepanjang atau sebagian besar waktu itu digunakan.

Status	Arti
Available	Volume tersedia untuk digunakan. Status ini adalah status berjalan normal untuk sebuah volume. Ketika fase Bootstrapping selesai, volume kembali ke status Tersedia. Artinya, gateway telah menyinkronkan setiap perubahan yang dilakukan pada volume sejak pertama kali memasuki status Pass Through.
Bootstrapping	Gateway menyinkronkan data secara lokal dengan salinan data yang disimpan. AWS Anda biasanya tidak perlu mengambil tindakan untuk status ini, karena volume penyimpanan secara otomatis melihat status Tersedia dalam banyak kasus. Berikut ini adalah skenario ketika status volume Bootstrapping: • Sebuah gerbang tiba-tiba ditutup. • Buffer unggahan gateway telah terlampaui. Dalam skenario ini, bootstrap terjadi ketika volume Anda memiliki status Pass Through dan jumlah buffer unggahan gratis meningkat cukup. Anda dapat memberikan tambahan ruang buffer upload sebagai salah satu cara untuk meningkatkan persentase ruang buffer upload gratis. Dalam skenario khusus ini, volume penyimpanan beralih dari Pass Through ke Bootstrapping ke status Available. Anda dapat terus menggunak an volume ini selama periode bootstrap ini. Namun, Anda tidak dapat mengambil snapshot volume pada saat ini. •

Status	Arti
	Anda membuat Volume Gateway tersimpan dan melestarikan data disk lokal yang ada. Dalam skenario ini, gateway Anda mulai mengunggah semua data ke AWS. Volume memiliki status Bootstrap ping sampai semua data dari disk lokal disalin. AWS Anda dapat menggunakan volume selama periode bootstrap ini. Namun, Anda tidak dapat mengambil snapshot volume pada saat ini.
Creating	Volume saat ini sedang dibuat dan belum siap digunakan. Status Creating adalah transisi. Tidak ada tindakan yang diperlukan.
Deleting	Volume saat ini sedang dihapus. Status Menghapus adalah transisi. Tidak ada tindakan yang diperlukan.
Tidak dapat dipulihkan	Terjadi kesalahan dari mana volume tidak dapat pulih. Untuk informasi tentang apa yang harus dilakukan dalam situasi ini, lihatMemecahkan masalah volume.

Status	Arti
Melewati	Data yang dipelihara secara lokal tidak sinkron dengan data yang disimpan di dalamnya AWS. Data yang ditulis ke volume saat volume dalam status Pass Through tetap dalam cache sampai status volume Bootstrapping. Data ini mulai diunggah AWS saat status Bootstrapping dimulai. Status Pass Through dapat terjadi karena beberapa alasan, yang tercantum sebagai berikut: • Status Pass Through terjadi jika gateway Anda kehabisan ruang buffer upload. Aplikasi Anda dapat terus membaca dan menulis data ke volume penyimpanan Anda sementara volume memiliki status Pass Through. Namun, gateway tidak menulis data volume apa pun ke buffer unggahannya atau mengunggah data ini. AWS Gateway terus mengunggah data apa pun yang ditulis ke volume sebelum volume memasuki status Pass Through. Setiap snapshot yang tertunda atau terjadwal dari volume penyimpanan gagal sementara volume memiliki status Pass Through. Untuk informasi tentang apa yang harus dilakukan ketika volume penyimpanan Anda memiliki status Pass Through karena buffer unggahan telah terlampau i, lihat. Memecahkan masalah volume Untuk kembali ke status AKTIF, volume di Pass Through harus menyelesaikan fase Bootstrapping. Selama Bootstrapping, volume menetapkan kembali sinkronisasi di dalamnya AWS, sehingga dapat melanjutkan catatan (log) perubahan volume, dan mengaktifkan fungsionalitas. `CreateSnapshot` Selama Bootstrapping, penulisan ke volume direkam dalam buffer unggahan. • Status Pass Through terjadi ketika ada lebih dari satu bootstrapping volume penyimpanan sekaligus. Hanya satu volume penyimpanan gateway yang dapat bootstrap pada satu waktu. Misalnya, Anda membuat dua volume penyimpanan dan memilih untuk menyimpan data yang ada pada keduanya. Dalam hal ini, volume penyimpan

Status	Arti
	an kedua memiliki status Pass Through hingga volume penyimpan an pertama selesai bootstrap. Dalam skenario ini, Anda tidak perlu bertindak. Setiap volume penyimpanan berubah ke status Tersedia secara otomatis ketika selesai dibuat. Anda dapat membaca dan menulis ke volume penyimpanan saat memiliki status Pass Through atau Bootstrapping. • Jarang, status Pass Through dapat menunjukkan bahwa disk yang dialokasikan untuk penggunaan buffer upload telah gagal. Untuk informasi tentang tindakan apa yang harus diambil dalam skenario ini, lihatMemecahkan masalah volume. • Status Pass Through dapat terjadi ketika volume dalam status Aktif atau Bootstrapping. Dalam hal ini, volume menerima penulisan, tetapi buffer unggahan memiliki kapasitas yang tidak cukup untuk merekam (log) yang menulis. • Status Pass Through terjadi ketika volume dalam keadaan apa pun dan gateway tidak dimatikan dengan bersih. Jenis shutdown ini dapat terjadi karena perangkat lunak mogok atau VM dimatikan. Dalam hal ini, volume dalam keadaan apa pun beralih ke status Pass Through.
Memulihkan	Volume sedang dipulihkan dari snapshot yang ada. Status ini hanya berlaku untuk volume yang disimpan. Untuk informasi selengkapnya, lihat Cara kerja Volume Gateway. Jika Anda mengembalikan dua volume penyimpanan secara bersamaan , kedua volume penyimpanan menunjukkan Memulihkan sebagai statusnya. Setiap volume penyimpanan berubah ke status Tersedia secara otomatis ketika selesai dibuat. Anda dapat membaca dan menulis ke volume penyimpanan dan mengambil snapshot saat memiliki status Restoring.

Status	Arti
Memulihkan Pass Through	Volume sedang dipulihkan dari snapshot yang ada dan mengalami masalah buffer unggahan. Status ini hanya berlaku untuk volume yang disimpan. Untuk informasi selengkapnya, lihat Cara kerja Volume Gateway. Salah satu alasan yang dapat menyebabkan status Restoring Pass Through adalah jika gateway Anda kehabisan ruang buffer unggah. Aplikasi Anda dapat terus membaca dan menulis data ke volume penyimpanan Anda saat mereka memiliki status Restoring Pass Through. Namun, Anda tidak dapat mengambil snapshot dari volume penyimpanan selama periode status Restoring Pass Through. Untuk informasi tentang tindakan apa yang harus diambil ketika volume penyimpanan Anda memiliki status Restoring Pass Through karena kapasitas buffer upload telah terlampaui, lihat. Memecahkan masalah volume Jarang, status Restoring Pass Through dapat menunjukkan bahwa disk yang dialokasikan untuk buffer unggahan telah gagal. Untuk informasi tentang tindakan apa yang harus diambil dalam skenario ini, lihatMemecahkan masalah volume.
Unggah Buffer Tidak Dikonfigurasi	Anda tidak dapat membuat atau menggunakan volume karena gateway tidak memiliki buffer unggahan yang dikonfigurasi. Untuk informasi tentang cara menambahkan kapasitas buffer upload untuk volume dalam pengaturan volume cache, lihat. Menentukan ukuran buffer unggahan yang akan dialokasikan Untuk informasi tentang cara menambahk an kapasitas buffer upload untuk volume dalam pengaturan volume tersimpan, lihatMenentukan ukuran buffer unggahan yang akan dialokasi kan.

Memahami Status Lampiran

Anda dapat melepaskan volume dari gateway atau melampirkannya ke gateway menggunakan konsol Storage Gateway atau API. Tabel berikut menunjukkan status lampiran volume pada konsol Storage Gateway. Status lampiran volume muncul di kolom Status lampiran untuk setiap volume

penyimpanan di gateway Anda. Misalnya, volume yang terlepas dari gateway memiliki status Terpisah. Untuk informasi tentang cara melepaskan dan melampirkan volume, lihatMemindahkan Volume Anda ke Gateway yang Berbeda.

Status	Arti
Terlampir	Volume dilampirkan ke gateway.
Terpisah	Volume terlepas dari gateway.
Melepaskan	Volume sedang terlepas dari gateway. Saat Anda melepaskan volume dan volume tidak memiliki data di dalamnya, Anda mungkin tidak melihat status ini.

Memahami Transisi Status Volume yang Di-cache

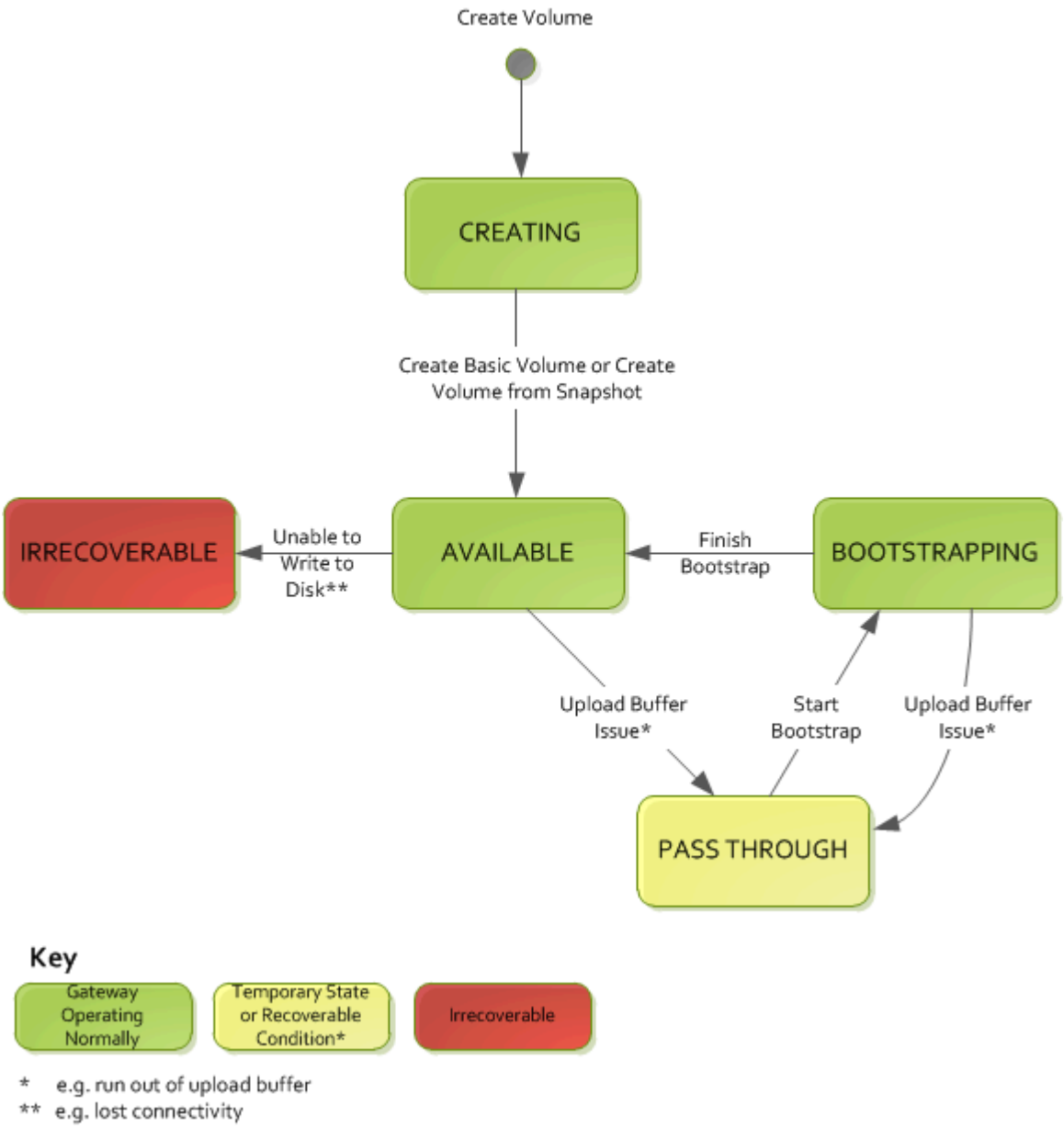
Gunakan diagram status berikut untuk memahami transisi paling umum antara status untuk volume di gateway cache. Anda tidak perlu memahami diagram secara detail untuk menggunakan gateway Anda secara efektif. Sebaliknya, diagram memberikan informasi terperinci jika Anda tertarik untuk mengetahui lebih banyak tentang cara kerja Volume Gateways.

Diagram tidak menampilkan status Upload Buffer Not Configurated atau status Deleting. Status volume dalam diagram muncul sebagai kotak hijau, kuning, dan merah. Anda dapat menafsirkan warna seperti yang dijelaskan berikut.

Warna	Status Volume
Hijau	Gateway beroperasi secara normal. Status volume tersedia atau akhirnya menjadi tersedia.
Kuning	Volume memiliki status Pass Through, yang menunjukkan ada potensi masalah dengan volume penyimpanan. Jika status ini muncul karena ruang buffer upload terisi, maka dalam beberapa kasus ruang buffer menjadi tersedia lagi. Pada saat itu, volume penyimpanan mengoreksi diri ke status Tersedia. Dalam kasus

Warna	Status Volume
	lain, Anda mungkin harus menambahkan lebih banyak ruang buffer upload ke gateway Anda untuk memungkinkan status volume penyimpanan menjadi Tersedia. Untuk informasi tentang cara memecahkan masalah ketika kapasitas buffer upload telah terlampaui, lihat. Memecahkan masalah volume Untuk informasi tentang cara menambahkan kapasitas buffer upload, lihatMenentukan ukuran buffer unggahan yang akan dialokasikan.
Merah	Volume penyimpanan memiliki status Tidak Dapat Dipulihkan. Dalam hal ini, Anda harus menghapus volume. Untuk informasi tentang cara melakukannya, lihat Untuk menghapus volume.

Dalam diagram, transisi antara dua keadaan digambarkan dengan garis berlabel. Misalnya, transisi dari status Creating ke status Available diberi label sebagai Create Basic Volume atau Create Volume from Snapshot. Transisi ini mewakili pembuatan volume cache. Untuk informasi selengkapnya tentang membuat volume penyimpanan, lihatMenambahkan dan memperluas volume.



> **Note**
>
> Status volume Pass Through muncul sebagai kuning dalam diagram ini. Namun, ini tidak cocok dengan warna ikon status ini di kotak Status konsol Storage Gateway.

Memahami Transisi Status Volume Tersimpan

Gunakan diagram status berikut untuk memahami transisi paling umum antara status untuk volume di gateway tersimpan. Anda tidak perlu memahami diagram secara detail untuk menggunakan gateway

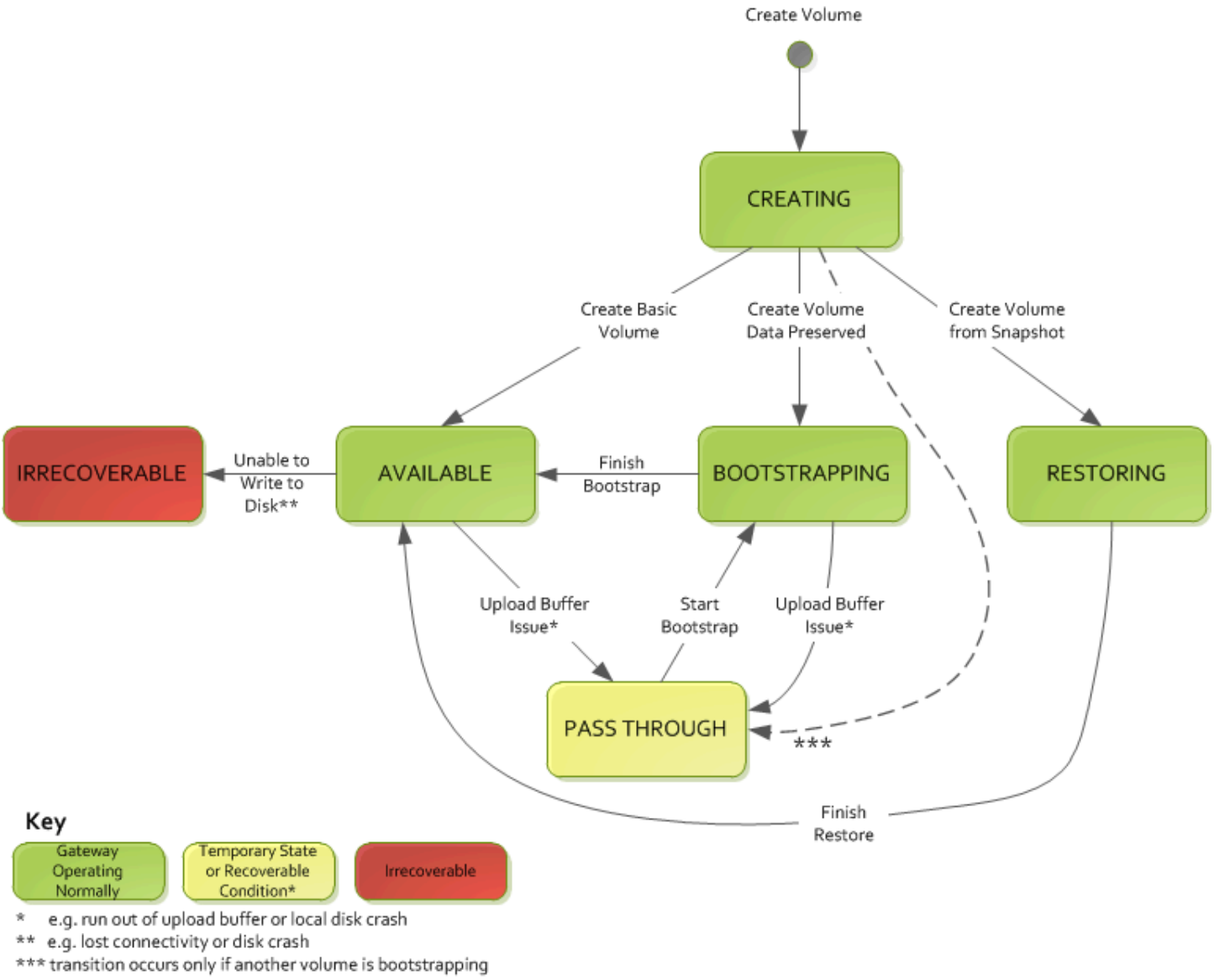
Anda secara efektif. Sebaliknya, diagram memberikan informasi terperinci jika Anda tertarik untuk memahami lebih lanjut tentang cara kerja Volume Gateways.

Diagram tidak menampilkan status Upload Buffer Not Configurated atau status Deleting. Status volume dalam diagram muncul sebagai kotak hijau, kuning, dan merah. Anda dapat menafsirkan warna seperti yang dijelaskan berikut.

Warna	Status Volume
Hijau	Gateway beroperasi secara normal. Status volume tersedia atau akhirnya menjadi tersedia.
Kuning	Saat Anda membuat volume penyimpanan dan melestarikan data, maka jalur dari status Creating ke status Pass Through terjadi jika volume lain adalah bootstrap. Dalam hal ini, volume dengan status Pass Through masuk ke status Bootstrapping dan kemudian ke status Tersedia ketika volume pertama selesai bootstrap. Selain skenario spesifik yang disebutkan, kuning (status Pass Through) menunjukkan bahwa ada potensi masalah dengan volume penyimpanan, yang paling umum adalah masalah buffer unggah. Jika kapasitas buffer upload telah terlampaui, maka dalam beberapa kasus ruang buffer menjadi tersedia lagi. Pada saat itu, volume penyimpan an mengoreksi diri ke status Tersedia. Dalam kasus lain, Anda mungkin harus menambahkan lebih banyak kapasitas buffer upload ke gateway Anda untuk mengembalikan volume penyimpan an ke status Tersedia. Untuk informasi tentang cara memecahkan masalah ketika kapasitas buffer upload telah terlampaui, lihat. Memecahka n masalah volume Untuk informasi tentang cara menambahkan kapasitas buffer upload, lihatMenentukan ukuran buffer unggahan yang akan dialokasikan.

Warna	Status Volume
Merah	Volume penyimpanan memiliki status Tidak Dapat Dipulihkan. Dalam hal ini, Anda harus menghapus volume. Untuk informasi tentang cara melakukannya, lihat Menghapus volume penyimpanan.

Dalam diagram berikut, transisi antara dua keadaan digambarkan dengan garis berlabel. Misalnya, transisi dari status Creating ke status Available diberi label sebagai Create Basic Volume. Transisi ini mewakili pembuatan volume penyimpanan tanpa menyimpan data atau membuat volume dari snapshot.



> **Note**
>
> Status volume Pass Through muncul sebagai kuning dalam diagram ini. Namun, ini tidak cocok dengan warna ikon status ini di kotak Status konsol Storage Gateway.

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 EC2 instans Amazon 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 volume tersimpan ke Volume Gateway baru yang disimpan

Untuk memindahkan volume yang tersimpan ke Volume Gateway baru yang tersimpan

1. Hentikan aplikasi apa pun yang menulis ke Volume Gateway lama yang tersimpan.
2. Gunakan langkah-langkah berikut untuk membuat snapshot volume Anda, lalu tunggu hingga snapshot selesai.

   a. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.

   b. Di panel navigasi, pilih Volume, lalu pilih volume yang ingin Anda buat snapshot.

   c. Untuk Tindakan, pilih Buat snapshot.

   d. Di kotak dialog Buat snapshot, masukkan deskripsi snapshot, lalu pilih Buat snapshot.

   Anda dapat memverifikasi bahwa snapshot dibuat menggunakan konsol. Jika data masih diunggah ke volume, tunggu hingga unggahan selesai sebelum Anda melanjutkan ke langkah berikutnya. Untuk melihat status snapshot dan memvalidasi bahwa tidak ada yang tertunda, pilih tautan snapshot pada volume.
3. Gunakan langkah-langkah berikut untuk menghentikan Volume Gateway lama yang tersimpan:

   a. Di panel navigasi, pilih Gateway, lalu pilih Volume Gateway tersimpan 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 gateway berhenti, Anda mungkin melihat pesan yang menunjukkan status gateway. Ketika gateway dimatikan, pesan dan tombol Start gateway muncul di tab Detail. Saat gateway dimatikan, status gateway adalah Shutdown.

c. Matikan VM menggunakan kontrol hypervisor.

Untuk informasi selengkapnya tentang menghentikan gateway, lihatMemulai dan Menghentikan Volume Gateway.

4. Lepaskan disk penyimpanan yang terkait dengan volume tersimpan Anda dari gateway VM. Ini tidak termasuk disk root VM.
5. Aktifkan Volume Gateway baru yang disimpan dengan image VM hypervisor baru yang tersedia dari konsol Storage Gateway di rumah. https://console.aws.amazon.com/storagegateway/
6. Pasang disk penyimpanan fisik yang Anda lepaskan dari Volume Gateway VM lama yang disimpan di langkah 5.
7. Untuk menyimpan data yang ada pada disk, gunakan langkah-langkah berikut untuk membuat volume yang disimpan.

   a. Pada konsol Storage Gateway, pilih Buat volume.

   b. Di kotak dialog Buat volume, pilih Volume Gateway tersimpan yang Anda buat di langkah 5.

   c. Pilih nilai ID Disk dari daftar.

   d. Untuk konten Volume, pilih opsi Pertahankan data yang ada pada disk.

   Untuk informasi selengkapnya tentang membuat volume, lihatMembuat volume penyimpanan.
8. (Opsional) Dalam Konfigurasi panduan otentikasi CHAP yang muncul, masukkan nama Inisiator, rahasia Inisiator, dan rahasia Target, lalu pilih Simpan.

   Untuk informasi selengkapnya tentang bekerja dengan otentikasi Challenge-Handshake Authentication Protocol (CHAP), lihat. Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda
9. Mulai aplikasi yang menulis ke volume tersimpan Anda.
10. Ketika Anda telah mengonfirmasi bahwa Volume Gateway tersimpan baru Anda berfungsi dengan benar, Anda dapat menghapus Volume Gateway lama yang tersimpan.

> **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.

Gunakan langkah-langkah berikut untuk menghapus Volume Gateway lama yang tersimpan:

> **Warning**
>
> Ketika gateway dihapus, tidak ada cara untuk memulihkannya.

a. Di panel navigasi, pilih Gateway, lalu pilih Volume Gateway tersimpan lama yang ingin Anda hapus.

b. Untuk Tindakan, pilih Hapus gateway.

c. Di kotak dialog konfirmasi yang muncul, pilih kotak centang untuk mengonfirmasi penghapusan Anda. Pastikan ID gateway yang tercantum menentukan Volume Gateway tersimpan lama yang ingin Anda hapus, lalu pilih Hapus.

11. Hapus VM gateway lama. Untuk informasi tentang menghapus VM, lihat dokumentasi untuk hypervisor Anda.

Memindahkan volume cache ke mesin virtual gateway baru

Untuk memindahkan volume cache Anda ke mesin virtual Volume Gateway (VM) yang baru di-cache

1. Hentikan aplikasi apa pun yang menulis ke Volume Gateway yang di-cache lama.
2. Lepaskan atau putuskan volume iSCSI dari klien mana pun yang menggunakannya. Ini membantu menjaga data pada volume tersebut konsisten dengan mencegah klien mengubah atau menambahkan data ke volume tersebut.
3. Gunakan langkah-langkah berikut untuk membuat snapshot volume Anda, lalu tunggu hingga snapshot selesai.

   a. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.

b. Di panel navigasi, pilih Volume, lalu pilih volume yang ingin Anda buat snapshot.

c. Untuk Tindakan, pilih Buat snapshot.

d. Di kotak dialog Buat snapshot, masukkan deskripsi snapshot, lalu pilih Buat snapshot.

Anda dapat memverifikasi bahwa snapshot dibuat menggunakan konsol. Jika data masih diunggah ke volume, tunggu hingga unggahan selesai sebelum Anda melanjutkan ke langkah berikutnya. Untuk melihat status snapshot dan memvalidasi bahwa tidak ada yang tertunda, pilih tautan snapshot pada volume.

Untuk informasi selengkapnya tentang memeriksa status volume di konsol, lihatMemahami Status Volume dan Transisi. Untuk informasi tentang status volume cache, lihatMemahami Transisi Status Volume yang Di-cache .

4. Gunakan langkah-langkah berikut untuk menghentikan Volume Gateway yang di-cache lama:

a. Di panel navigasi, pilih Gateways, lalu pilih Volume Gateway cache 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. Catat ID gateway, karena diperlukan pada langkah selanjutnya.

Saat gateway lama berhenti, Anda mungkin melihat pesan yang menunjukkan status gateway. Ketika gateway lama dimatikan, pesan dan tombol Start gateway muncul di tab Detail. Saat gateway dimatikan, status gateway adalah Shutdown.

c. Matikan VM lama menggunakan kontrol hypervisor. Untuk informasi selengkapnya tentang mematikan EC2 instans Amazon, lihat Menghentikan dan memulai instans Anda di EC2 Panduan Pengguna Amazon. Untuk informasi selengkapnya tentang mematikan KVM,, atau Hyper-V VM VMware, lihat dokumentasi hypervisor Anda.

Untuk informasi selengkapnya tentang menghentikan gateway, lihatMemulai dan Menghentikan Volume Gateway.

5. Lepaskan semua disk, termasuk disk root, disk cache, dan unggah disk buffer, dari VM gateway lama.

> **Note**
>
> Catat ID volume disk root, serta ID gateway yang terkait dengan disk root itu. Anda melepaskan disk ini dari hypervisor Storage Gateway baru di langkah selanjutnya. (Lihat langkah 11.)

Jika Anda menggunakan EC2 instans Amazon sebagai VM untuk Volume Gateway yang di-cache, lihat Melepaskan volume Amazon EBS dari instans Linux di Panduan Pengguna Amazon. EC2 Untuk informasi tentang melepaskan disk dari KVM,, atau Hyper-V VM VMware, lihat dokumentasi untuk hypervisor Anda.

6. Buat instance VM hypervisor Storage Gateway baru, tetapi jangan aktifkan sebagai gateway. Untuk informasi selengkapnya tentang membuat VM hypervisor Storage Gateway baru, lihat. Siapkan Volume Gateway Gerbang baru ini akan mengasumsikan identitas gateway lama.

   > **Note**
   >
   > Jangan tambahkan disk untuk cache atau unggah buffer ke VM baru. VM baru Anda akan menggunakan disk cache yang sama dan mengunggah disk buffer yang digunakan oleh VM lama.

7. Instans VM hypervisor Storage Gateway baru Anda harus menggunakan konfigurasi jaringan yang sama dengan VM lama. Konfigurasi jaringan default untuk gateway adalah Dynamic Host Configuration Protocol (DHCP). Dengan DHCP, gateway Anda secara otomatis diberi alamat IP.

   Jika Anda perlu mengonfigurasi alamat IP statis secara manual untuk VM baru Anda, lihat Mengkonfigurasi Jaringan Gateway Anda untuk detail selengkapnya. Jika gateway Anda harus menggunakan proxy Socket Secure versi 5 (SOCKS5) untuk terhubung ke internet, lihat Mengonfigurasi SOCKS5 proxy untuk gateway lokal Anda untuk detail selengkapnya.

8. Mulai VM baru.

9. Lampirkan disk yang Anda lepaskan dari Volume Gateway VM cache lama di langkah 5, ke Volume Gateway cache yang baru. Lampirkan mereka dalam urutan yang sama ke VM gateway baru seperti yang ada di VM gateway lama.

   Semua disk harus membuat transisi tidak berubah. Jangan mengubah ukuran volume, karena itu akan menyebabkan metadata menjadi tidak konsisten.

10. Memulai proses migrasi gateway dengan menghubungkan ke VM baru dengan URL yang menggunakan format berikut.

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

    Anda dapat menggunakan kembali alamat IP yang sama untuk VM gateway baru seperti yang Anda gunakan untuk VM gateway lama. URL Anda akan terlihat mirip dengan contoh berikut.

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

    Gunakan URL ini dari browser, atau dari baris perintah menggunakan`curl`, untuk memulai proses migrasi.

    Ketika proses migrasi gateway berhasil dimulai, Anda akan melihat pesan berikut:

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

11. Lepaskan disk root gateway lama, yang ID volumenya Anda catat di langkah 5.
12. Mulai gateway.

    Gunakan langkah-langkah berikut untuk memulai Volume Gateway cache yang baru:

    a. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
    b. Di panel navigasi, pilih Gateway dan kemudian pilih gateway baru yang ingin Anda mulai. Status gateway adalah Shutdown.
    c. Pilih Detail, lalu pilih Start gateway.

    Untuk informasi selengkapnya tentang memulai gateway, lihatMemulai dan Menghentikan Volume Gateway.
13. Volume Anda sekarang harus tersedia untuk aplikasi Anda di alamat IP VM gateway baru.
14. Konfirmasikan bahwa volume Anda tersedia, dan hapus VM gateway lama. Untuk informasi tentang menghapus VM, lihat dokumentasi untuk hypervisor Anda.

Memantau Storage Gateway

Bagian ini menjelaskan cara memantau Storage Gateway, termasuk pemantauan 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.

Untuk informasi khusus untuk memantau Gateway Volume dan sumber daya terkait, lihat Memantau Gateway Volume Anda.

Topik

- Memahami metrik 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 Volume 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 CloudWatch Metrik Amazon.

> **Note**
>
> Beberapa metrik mengembalikan titik data hanya ketika data baru telah dihasilkan selama periode pemantauan terbaru.

Metrik	Deskripsi
`AvailabilityNotifications`	Jumlah pemberitahuan kesehatan terkait ketersediaan yang dihasilkan oleh gateway. Gunakan metrik ini dengan `Sum` statistik untuk mengamati apakah gateway mengalami peristiwa terkait ketersediaan. Untuk detail tentang peristiwa , periksa grup CloudWatch log yang dikonfigurasi. Satuan: Jumlah
`CacheHitPercent`	Persentase pembacaan aplikasi disajikan dari cache. Sampel diambil pada akhir periode pelaporan. Unit: Persen

Metrik	Deskripsi
CachePercentDirty	Persentase keseluruhan cache gateway yang belum dipertahankan. AWS Sampel diambil pada akhir periode pelaporan. Gunakan metrik ini dengan Sum statistik. Idealnya, metrik ini harus tetap rendah. Unit: Persen
CacheUsed	Jumlah total byte yang digunakan dalam penyimpan an cache gateway. Sampel diambil pada akhir periode pelaporan. Unit: Bita
IoWaitPercent	Persentase waktu gateway menunggu respons dari disk lokal. Unit: Persen
MemTotalBytes	Jumlah RAM yang disediakan ke VM gateway, dalam byte. Unit: Bita
MemUsedBytes	Jumlah RAM yang saat ini digunakan oleh gateway VM, dalam byte. Unit: Bita

Metrik	Deskripsi
QueuedWrites	Biasanya, nilai ini mewakili jumlah byte yang disimpan secara lokal yang menunggu untuk ditulis AWS, tetapi juga mencerminkan proses sinkronisasi yang terjadi antara data lokal dan data cloud selama “bootstrap”, yang terjadi setiap kali gateway restart. Unit: Bita
ReadBytes	Jumlah total byte yang dibaca dari aplikasi lokal Anda dalam periode pelaporan untuk semua volume di gateway. Gunakan metrik ini dengan Sum statistik untuk mengukur throughput dan dengan Samples statistik untuk mengukur IOPS. Unit: Bita

Metrik	Deskripsi
`ReadTime`	Jumlah total milidetik yang dihabiskan untuk melakukan operasi baca dari aplikasi lokal Anda dalam periode pelaporan untuk semua volume di gateway. Gunakan metrik ini dengan `Average` statistik untuk mengukur latensi. Satuan: Milidetik
`TimeSinceLastRecoveryPoint`	Waktu sejak titik pemulihan terakhir yang tersedia. Untuk informasi selengkapnya, lihat Gateway Cached Anda Tidak Dapat Dijangkau Dan Anda Ingin Memulihkan Data Anda. Unit: Detik
`TotalCacheSize`	Ukuran total cache dalam byte. Sampel diambil pada akhir periode pelaporan. Unit: Bita
`UploadBufferPercentUsed`	Persentase penggunaan buffer unggahan gateway. Sampel diambil pada akhir periode pelaporan. Unit: Persen

Metrik	Deskripsi	
UploadBufferUsed	Jumlah total byte yang digunakan dalam buffer upload gateway. Sampel diambil pada akhir periode pelaporan. Unit: Bita	
UserCpuPercent	Persentase waktu CPU yang dihabiskan untuk pemrosesan gateway, dirata-ratakan di semua core. Unit: Persen	
WorkingStorageFree	Jumlah total ruang yang tidak terpakai di penyimpanan kerja gateway. Sampel diambil pada akhir periode pelaporan. Unit: Bita	
WorkingStoragePercentUsed	Persentase penggunaan buffer unggahan gateway. Sampel diambil pada akhir periode pelaporan. Unit: Persen	
WorkingStorageUsed	Jumlah total byte yang digunakan dalam buffer upload gateway. Sampel diambil pada akhir periode pelaporan. Unit: Bita	

Metrik	Deskripsi
`WriteBytes`	Jumlah total byte yang ditulis ke aplikasi lokal Anda dalam periode pelaporan untuk semua volume di gateway. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur IOPS. Unit: Bita
`WriteTime`	Jumlah total milidetik yang dihabiskan untuk melakukan operasi penulisan dari aplikasi lokal Anda dalam periode pelaporan untuk semua volume di gateway. Gunakan metrik ini dengan `Average` statistik untuk mengukur latensi. Satuan: Milidetik

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
`GatewayId` , `GatewayName`	Dimensi ini memfilter data yang Anda minta ke metrik khusus gateway. Anda dapat mengidentifikasi gateway untuk bekerja berdasarkan nilai untuk `GatewayId` atau`GatewayName` . Jika

Dimensi	Deskripsi
	nama gateway Anda berbeda untuk rentang waktu yang Anda minati untuk melihat metrik, gunakan. `GatewayId` 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.
`VolumeId`	Dimensi ini menyaring data yang Anda minta ke metrik spesifik volume. Identifikasi volume penyimpanan untuk bekerja dengan `VolumeId` nilainya. Untuk informasi tentang bekerja dengan metrik volume, lihat Mengukur Kinerja Antara Aplikasi dan Gateway Anda.

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 Volume Gateway.

> **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 penggunaan buffer	Gunakan `UploadBufferPercentUsed`, `UploadBufferUsed`, dan `UploadBufferFree` metrik dengan `Average` statistik. Misalnya, gunakan `UploadBufferUsed` dengan `Average` statistik untuk menganalisis penggunaan penyimpanan selama periode waktu tertentu.

Untuk mengukur persentase buffer unggahan 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. Konfigurasikan 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.

   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 Volume Gateway.

Item yang menarik	Cara Mengukur
Total penggunaan cache	Gunakan `CachePercentUsed` dan `TotalCacheSize` metrik dengan `Average` statistik. Misalnya, gunakan `CachePercentUsed` dengan `Average` statistik untuk menganalisis penggunaan cache selama periode waktu tertentu. `TotalCacheSize` Metrik berubah hanya ketika Anda menambahkan cache ke gateway.
Persentase permintaan baca yang disajikan dari cache	Gunakan `CacheHitPercent` metrik dengan `Average` statistik. Biasanya, Anda `CacheHitPercent` ingin tetap tinggi.
Persentase cache yang kotor—yaitu, berisi konten yang belum diunggah AWS	Gunakan `CachePercentDirty` metrik dengan `Average` statistik. Biasanya, Anda `CachePercentDirty` ingin tetap rendah.

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 informasi selengkapnya tentang metrik yang digunakan untuk memantau , lihat Memahami metrik gateway dan Memahami Metrik Tape Volume. 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 VMware host dengan mode HA diaktifkan, kami juga merekomendasikan alarm tambahan CloudWatch ini:

- Pemberitahuan ketersediaan: `AvailabilityNotifications` >= 1 untuk 1 titik data dalam 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, lihatMembuat CloudWatch alarm khusus untuk gateway Anda.
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 Volume Anda. 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/rumah/.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda buat alarm yang direkomendasikan. CloudWatch
3. Pada halaman detail gateway, pilih tab Monitoring.
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/rumah/.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda buat alarm.
3. Pada halaman detail gateway, pilih tab Monitoring.
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 Pemantauan.

     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 Volume Gateway Anda

Topik di bagian ini menjelaskan cara memantau Volume Gateway baik dalam volume cache atau pengaturan volume tersimpan, termasuk memantau volume yang terkait dengan gateway dan memantau buffer unggahan. Anda menggunakan metrik AWS Management Console untuk melihat 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 cloud Amazon Web Services. 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. Untuk informasi selengkapnya CloudWatch, lihat Panduan CloudWatch Pengguna Amazon.

Topik

- Mendapatkan log kesehatan Volume Gateway dengan Amazon CloudWatch Logs- Pelajari cara menggunakan Amazon CloudWatch Logs untuk mendapatkan informasi tentang kesehatan Volume Gateway dan sumber daya terkait.
- Menggunakan CloudWatch Metrik Amazon- Pelajari cara mendapatkan data pemantauan untuk gateway Anda menggunakan API AWS Management Console atau CloudWatch API.
- Mengukur Kinerja Antara Aplikasi dan Gateway- Pelajari cara mengukur throughput data, latensi data, dan operasi per detik untuk memahami kinerja antara aplikasi dan gateway Anda.
- Mengukur Kinerja Antara Gateway Anda dan AWS- Pelajari cara mengukur throughput data, latensi data, dan operasi per detik untuk memahami kinerja antara gateway Anda dan cloud. AWS
- Memahami metrik volume- Pelajari cara mengukur metrik yang menyediakan data tentang volume yang terkait dengan gateway.

Mendapatkan log kesehatan Volume Gateway dengan Amazon CloudWatch Logs

Anda dapat menggunakan Amazon CloudWatch Logs untuk mendapatkan informasi tentang kesehatan Volume Gateway dan sumber daya terkait. Anda dapat menggunakan log ini 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 Ketersediaan VMware Tinggi (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, lihatKonfigurasikan Volume Gateway 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 volume

Prosedur berikut menunjukkan cara mengkonfigurasi grup CloudWatch log setelah gateway Anda diaktifkan.

Untuk mengonfigurasi grup CloudWatch log agar berfungsi dengan gateway Anda

1. Masuk ke AWS Management Console dan buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi kiri, pilih Gateway, lalu pilih gateway yang ingin Anda konfigurasikan 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 *CustomerGatewayName* dialog 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 kiri, pilih Gateway, lalu pilih gateway yang Anda konfigurasikan untuk grup CloudWatch log.
   2. Pilih tab Detail, dan di bawah log Kesehatan, pilih CloudWatch Log. Halaman detail grup Log terbuka di CloudWatch konsol Amazon.

Menggunakan CloudWatch Metrik Amazon

Anda bisa mendapatkan data pemantauan untuk gateway Anda menggunakan API AWS Management Console atau CloudWatch API. Konsol menampilkan serangkaian grafik berdasarkan data mentah dari CloudWatch API. Anda juga dapat menggunakan CloudWatch API melalui salah satu Kit Pengembangan AWS Perangkat Lunak (SDKs) 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 `GatewayIdGatewayName`,, dan`VolumeId`. Di CloudWatch konsol, Anda dapat menggunakan `Volume Metrics` tampilan `Gateway Metrics` dan untuk dengan mudah memilih dimensi khusus gateway dan spesifik volume. 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 dapat Anda gunakan.

CloudWatch Namespace	Dimensi	Deskripsi
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Dimensi ini menyaring data metrik yang menjelaskan aspek gateway. Anda dapat mengidentifikasi gateway untuk bekerja dengan menentukan dimensi `GatewayId` dan `GatewayName` dimensi. Data throughput dan latensi gateway didasarkan pada semua volume di gateway. Data tersedia secara otomatis dalam periode 5 menit tanpa biaya.

CloudWatch Namespace	Dimensi	Deskripsi
	`VolumeId`	Dimensi ini menyaring data metrik yang spesifik untuk volume. Identifikasi volume untuk dikerjakan berdasarkan `VolumeId` dimensinya. Data tersedia secara otomatis dalam periode 5 menit tanpa biaya.

Bekerja dengan metrik gateway dan volume 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

Mengukur Kinerja Antara Aplikasi dan Gateway

Throughput data, latensi data, dan operasi per detik adalah tiga langkah yang dapat Anda gunakan untuk memahami kinerja penyimpanan aplikasi yang menggunakan gateway Anda. Bila Anda menggunakan statistik agregasi yang benar, Anda dapat menggunakan metrik Storage Gateway untuk mengukur nilai-nilai ini.

Statistik adalah agregasi metrik selama periode waktu tertentu. Saat Anda melihat nilai metrik di CloudWatch, gunakan `Average` statistik untuk latensi data (milidetik), gunakan `Sum` statistik untuk throughput data (byte per detik), 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 aplikasi dan gateway Anda.

Item yang menarik	Cara Mengukur
Throughput	Gunakan `ReadBytes` dan `WriteBytes` metrik dengan `Sum` CloudWatch statistik. Misalnya, `Sum` nilai `ReadBytes` metrik selama periode sampel

Item yang menarik	Cara Mengukur
	5 menit dibagi 300 detik memberi Anda throughput sebagai laju dalam byte per detik.
Latensi	Gunakan `ReadTime` dan `WriteTime` metrik dengan `Average` CloudWatch statistik. Misalnya, `Average` nilai `ReadTime` metrik memberi Anda latensi per operasi selama periode waktu sampel.
IOPS	Gunakan `ReadBytes` dan `WriteBytes` metrik dengan `Samples` CloudWatch statistik. Misalnya, `Samples` nilai `ReadBytes` metrik selama periode sampel 5 menit dibagi 300 detik memberi Anda IOPS.

Untuk grafik latensi rata-rata dan grafik ukuran rata-rata, rata-ratanya dihitung terhadap jumlah total operasi (baca atau tulis, mana saja yang berlaku untuk grafik) yang selesai selama periode.

Untuk mengukur throughput data dari aplikasi ke volume

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Metrik, lalu pilih tab Semua metrik dan kemudian pilih Storage Gateway.
3. Pilih dimensi metrik Volume, dan temukan volume yang ingin Anda gunakan.
4. Pilih `ReadBytes` dan `WriteBytes` 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 (satu untuk `ReadBytes` dan satu untuk`WriteBytes`), bagi setiap titik data dengan periode (dalam detik) untuk mendapatkan throughput pada titik sampel. Total throughput adalah jumlah dari throughput.

Misalnya, jika throughput baca adalah 2.384.199.680 byte selama 300 detik, maka perkiraan laju throughput untuk titik data tersebut adalah 7,9 megabyte per detik.

Untuk mengukur operasi input/output data per detik dari aplikasi ke volume

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Metrik, lalu pilih tab Semua metrik dan kemudian pilih Storage Gateway.

3. Pilih dimensi metrik Volume, dan temukan volume yang ingin Anda gunakan.
4. Pilih `ReadBytes` dan `WriteBytes` metrik.
5. Untuk Rentang Waktu, pilih nilai.
6. Pilih `Samples` statistiknya.
7. Untuk Periode, pilih nilai 5 menit atau lebih.
8. Dalam kumpulan titik data yang diurutkan waktu yang dihasilkan (satu untuk `ReadBytes` dan satu untuk`WriteBytes`), bagi setiap titik data dengan periode (dalam detik) untuk mendapatkan IOPS.

Misalnya, jika jumlah operasi tulis adalah 24.373 selama periode 300 detik, maka IOPS untuk titik data tersebut adalah 81 operasi tulis per detik.

Mengukur Kinerja Antara Gateway Anda dan AWS

Throughput data, latensi data, dan operasi per detik adalah tiga langkah yang dapat Anda gunakan untuk memahami kinerja penyimpanan aplikasi Anda menggunakan Storage Gateway. Ketiga nilai ini dapat diukur menggunakan metrik Storage Gateway yang disediakan untuk Anda saat Anda menggunakan statistik agregasi yang benar. Tabel berikut merangkum metrik dan statistik terkait yang akan digunakan untuk mengukur operasi throughput, latensi, dan input/output per detik (IOPS) antara gateway Anda dan. AWS

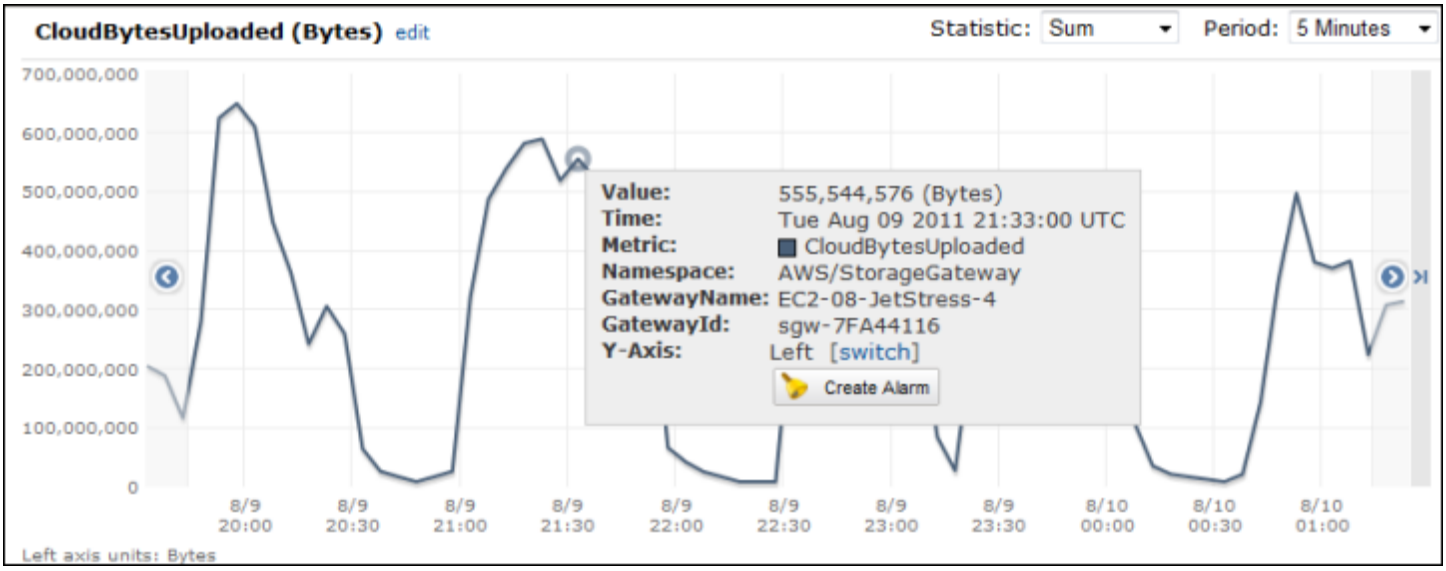
Item yang menarik	Cara Mengukur
Throughput	Gunakan `ReadBytes` dan `WriteBytes` metrik dengan `Sum` CloudWatch statistik. Misalnya, `Sum` nilai `ReadBytes` metrik selama periode sampel 5 menit dibagi 300 detik memberi Anda throughput sebagai laju dalam byte per detik.
Latensi	Gunakan `ReadTime` dan `WriteTime` metrik dengan `Average` CloudWatch statistik. Misalnya, `Average` nilai `ReadTime` metrik memberi Anda latensi per operasi selama periode waktu sampel.
IOPS	Gunakan `ReadBytes` dan `WriteBytes` metrik dengan `Samples` CloudWatch statistik. Misalnya, `Samples` nilai `ReadBytes` metrik selama periode sampel 5 menit dibagi 300 detik memberi Anda IOPS.

Item yang menarik	Cara Mengukur
Throughput ke AWS	Gunakan `CloudBytesDownloaded` dan `CloudBytesUploaded` metrik dengan `Sum` CloudWatch statistik. Misalnya, `Sum` nilai `CloudBytesDownloaded` metrik selama periode sampel 5 menit dibagi 300 detik memberi Anda throughput dari AWS gateway sebagai byte per detik.
Latensi data ke AWS	Gunakan `CloudDownloadLatency` metrik dengan `Average` statistik. Misalnya, `Average` statistik `CloudDownloadLatency` metrik memberi Anda latensi per operasi.

Untuk mengukur throughput data upload dari gateway ke AWS

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Metrik, lalu pilih tab Semua metrik dan kemudian pilih Storage Gateway.
3. Pilih dimensi metrik Gateway, dan temukan volume 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.

Memindahkan kursor ke titik data menampilkan informasi tentang titik data, termasuk nilai dan byte yang diunggah. Bagilah nilai ini dengan nilai Periode (5 menit) untuk mendapatkan throughput pada titik sampel tersebut. Misalnya, jika throughput dari gateway ke AWS adalah 555.544.576 byte selama 300 detik, maka perkiraan throughput per detik adalah 1,85 megabyte per detik.



Untuk mengukur latensi per operasi gateway

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Metrik, lalu pilih tab Semua metrik dan kemudian pilih Storage Gateway.
3. Pilih dimensi metrik Gateway, dan temukan volume yang ingin Anda gunakan.
4. Pilih `ReadTime` dan `WriteTime` metrik.
5. Untuk Rentang Waktu, pilih nilai.
6. Pilih `Average` statistiknya.
7. Untuk Periode, pilih nilai 5 menit agar sesuai dengan waktu pelaporan default.
8. Dalam kumpulan titik yang diurutkan waktu yang dihasilkan (satu untuk `ReadTime` dan satu untuk`WriteTime`), tambahkan titik data pada sampel waktu yang sama untuk mendapatkan latensi total dalam milidetik.

Untuk mengukur latensi data dari gateway ke AWS

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Metrik, lalu pilih tab Semua metrik dan kemudian pilih Storage Gateway.
3. Pilih dimensi metrik Gateway, dan temukan volume 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 mengatur alarm ambang batas atas untuk throughput gateway ke AWS

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Alarms.
3. Pilih Buat Alarm untuk memulai wizard Buat Alarm.
4. Pilih dimensi Storage Gateway, dan temukan gateway yang ingin Anda gunakan.
5. Pilih `CloudBytesUploaded` metrik.
6. Untuk menentukan alarm, tentukan 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 MB selama 60 menit.
7. Konfigurasikan tindakan yang akan diambil untuk status alarm. Misalnya, Anda dapat memiliki pemberitahuan email yang dikirimkan kepada Anda.
8. 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 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. Konfigurasikan tindakan yang akan diambil untuk status alarm. Misalnya, Anda dapat memiliki pemberitahuan email yang dikirimkan kepada Anda.
7. Pilih Buat Alarm.

Memahami metrik volume

Anda dapat menemukan informasi berikut tentang metrik Storage Gateway yang mencakup volume gateway. Setiap volume gateway memiliki satu set metrik yang terkait dengannya.

Beberapa metrik spesifik volume memiliki nama yang sama dengan metrik khusus gateway tertentu. Metrik ini mewakili jenis pengukuran yang sama tetapi mencakup volume, bukan gateway. Sebelum mulai bekerja, tentukan apakah Anda ingin bekerja dengan metrik gateway atau metrik volume. Khususnya, saat bekerja dengan metrik volume, tentukan ID volume untuk volume penyimpanan yang ingin Anda lihat metrik. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch Metrik 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 volume penyimpanan Anda.

Metrik	Deskripsi	Volume cache	Volume Tersimpan
`AvailabilityNotification`	Jumlah notifikasi ketersediaan yang dikirim oleh volume. Unit: hitung	Ya	Ya
`CacheHitPercent`	Persentase operasi membaca aplikasi dari volume yang disajikan dari cache. Sampel diambil pada akhir periode pelaporan. Ketika tidak ada operasi baca aplikasi dari volume, metrik	Ya	Tidak

Metrik	Deskripsi	Volume cache	Volume Tersimpan
	ini melaporkan 100 persen. Unit: Persen		
`CachePercentDirty`	Kontribusi volume terhadap persentase keseluruhan cache gateway yang tidak bertahan AWS. Sampel diambil pada akhir periode pelaporan. Gunakan `CachePercentDirty` metrik gateway untuk melihat persentase keseluruhan cache gateway yang tidak bertahan AWS. Untuk informasi selengkapnya, lihat Memahami metrik gateway. Unit: Persen	Ya	Ya

Metrik	Deskripsi	Volume cache	Volume Tersimpan
`CachePercentUsed`	Kontribusi volume terhadap persentase keseluruhan penggunaan penyimpanan cache gateway. Sampel diambil pada akhir periode pelaporan. Gunakan `CachePercentUsed` metrik gateway untuk melihat persentase penggunaan penyimpanan cache gateway secara keseluruhan. Untuk informasi selengkapnya, lihat Memahami metrik gateway. Unit: Persen	Ya	Tidak
`CloudBytesDownloaded`	Jumlah byte yang diunduh dari cloud ke volume. Unit: Bita	Ya	Ya
`CloudBytesUploaded`	Jumlah byte yang diunggah dari cloud ke volume. Unit: Bita	Ya	Ya

Metrik	Deskripsi	Volume cache	Volume Tersimpan
`HealthNotification`	Jumlah pemberitahuan kesehatan yang dikirim oleh volume. Unit: hitung	Ya	Ya
`IoWaitPercent`	Persentase IoWaitPercent unit yang saat ini digunakan oleh volume. Unit: Persen	Ya	Ya
`MemTotalBytes`	Persentase total memori yang saat ini digunakan oleh volume. Unit: Persen	Ya	Tidak
`MemoryUsage`	Persentase memori yang saat ini digunakan oleh volume. Unit: Persen	Ya	Tidak

Metrik	Deskripsi	Volume cache	Volume Tersimpan
`ReadBytes`	Jumlah total byte yang dibaca dari aplikasi lokal Anda dalam periode pelaporan. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur IOPS. Unit: Bita	Ya	Ya
`ReadTime`	Jumlah total milidetik yang dihabiskan untuk operasi baca dari aplikasi lokal Anda dalam periode pelaporan. Gunakan metrik ini dengan `Average` statistik untuk mengukur latensi. Unit: Milidetik	Ya	Ya

Metrik	Deskripsi	Volume cache	Volume Tersimpan
`UserCpuPercent`	Persentase unit komputasi CPU yang dialokasikan yang saat ini digunakan oleh volume. Unit: Persen	Ya	Ya
`WriteBytes`	Jumlah total byte yang ditulis ke aplikasi lokal Anda dalam periode pelaporan. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur IOPS. Unit: Bita	Ya	Ya
`WriteTime`	Jumlah total milidetik yang dihabiskan untuk operasi penulisan dari aplikasi lokal Anda dalam periode pelaporan. Gunakan metrik ini dengan `Average` statistik untuk mengukur latensi. Unit: Milidetik	Ya	Ya

Metrik	Deskripsi	Volume cache	Volume Tersimpan
`QueuedWrites`	Jumlah byte yang menunggu untuk ditulis AWS, diambil sampelnya pada akhir periode pelaporan. Unit: Bita	Ya	Ya

Mempertahankan Gateway Anda

Mempertahankan Anda mencakup tugas-tugas seperti mengukur dan mengonfigurasi disk lokal untuk penyimpanan cache dan mengunggah ruang buffer, mengelola pembaruan dan mengatur jadwal pembaruan, mengelola penggunaan bandwidth, dan mematikan atau menghapus gateway Anda dan sumber daya terkait jika perlu. Tugas-tugas ini umum untuk semua jenis gateway. Jika Anda belum membuat gateway, lihatMembuat gateway Anda.

Topik

- Mengelola disk lokal untuk Storage Gateway- Pelajari cara menilai persyaratan ukuran disk, menambahkan kapasitas cache, dan mengelola disk lokal yang Anda alokasikan ke untuk buffering dan penyimpanan.
- Mengelola Bandwidth untuk Anda- Pelajari cara membatasi throughput unggahan dari gateway Anda AWS untuk mengontrol jumlah bandwidth jaringan yang digunakan gateway.
- Mengelola pembaruan gateway- Pelajari cara mengaktifkan atau menonaktifkan pembaruan pemeliharaan, dan mengubah jadwal jendela pemeliharaan untuk Anda.
- Mematikan VM Gateway Anda- Pelajari tentang apa yang harus dilakukan jika Anda perlu mematikan atau me-reboot mesin virtual gateway Anda untuk pemeliharaan, seperti saat menerapkan tambalan ke hypervisor Anda.
- Menghapus gateway Anda dan menghapus sumber daya terkait- Pelajari cara menghapus gateway Anda menggunakan AWS Storage Gateway konsol dan membersihkan sumber daya terkait agar tidak dikenakan biaya untuk terus digunakan.

Mengelola disk lokal untuk Storage Gateway

Mesin virtual gateway (VM) menggunakan disk lokal yang Anda alokasikan di tempat untuk buffering dan penyimpanan. Gateway yang dibuat di EC2 instans Amazon menggunakan volume Amazon EBS sebagai disk lokal.

Topik

- Menentukan jumlah penyimpanan disk lokal
- 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 gunakan, gateway memerlukan penyimpanan tambahan berikut:

- Gerbang Volume:
  - Gateway yang disimpan memerlukan setidaknya satu disk untuk digunakan sebagai buffer unggahan.
  - Gateway cache 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 mengungga h data ke Amazon S3. Gateway Anda mengunggah data buffer ini melalui koneksi Secure Sockets Layer (SSL) terenkripsi ke. AWS	
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 penyimpan an cache untuk akses latensi rendah. Saat aplikasi Anda meminta data dari volume atau	

Penyimpanan lokal	Deskripsi	
	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.

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 Volume Gateways, ketika buffer unggahan mencapai kapasitasnya, volume Anda masuk ke status PASS THROUGH. Dalam status ini, data baru yang ditulis aplikasi Anda disimpan secara lokal tetapi tidak segera diunggah. AWS Dengan demikian, Anda tidak dapat mengambil foto baru. Ketika kapasitas buffer unggah dibebaskan, volume akan melalui status BOOTSTRAPPING. Dalam status ini, setiap data baru yang disimpan secara lokal diunggah ke. AWS Akhirnya, volume kembali ke status AKTIF. Storage Gateway kemudian melanjutkan sinkronisasi normal data yang disimpan secara lokal dengan salinan yang disimpan AWS, dan Anda dapat mulai mengambil snapshot baru. Untuk informasi selengkapnya tentang status volume, lihatMemahami Status Volume dan Transisi.

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.

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 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 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, lihatMenentukan 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 upload 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 Anda. EC2 Untuk informasi tentang cara menyediakan disk pada hypervisor, lihat dokumentasi hypervisor Anda. Untuk informasi tentang penyediaan volume Amazon EBS untuk EC2 instans Amazon, 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/rumah.
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.

   > **Note**
   >
   > UPLOAD BUFFER adalah satu-satunya pilihan yang tersedia untuk mengalokasikan disk pada Stored Volume Gateways.

7. Pilih Simpan perubahan untuk menyimpan pengaturan konfigurasi Anda.

Mengelola Bandwidth untuk 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 Schedule-Based Bandwidth Throttling Menggunakan Storage Gateway Console.

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
- Schedule-Based Bandwidth Throttling Menggunakan Storage Gateway Console
- Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK untuk Java
- Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK untuk .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/rumah.
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.

Schedule-Based Bandwidth Throttling Menggunakan Storage Gateway Console

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/rumah.
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-limitJadwal 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-limitInterval 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-limitInterval 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-limitinterval 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 untuk 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 untuk Java Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan aplikasi konsol Java. Untuk informasi selengkapnya, lihat Memulai di Panduan AWS SDK untuk Java Pengembang.

Example : Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK untuk 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 bandwith.\n" + ex.toString());
        }
    }
```

```
}
```

Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK untuk .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 untuk .NET Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan aplikasi konsol.NET. Untuk informasi selengkapnya, lihat Memulai di Panduan AWS SDK untuk .NET Pengembang.

Example : Memperbarui Batas Tingkat Bandwidth Gateway dengan Menggunakan AWS SDK untuk .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 bandwith.\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 Alat AWS untuk PowerShell Panduan Pengguna.

Example : Memperbarui Batas Tingkat Bandwidth Gateway dengan Menggunakan AWS Tools for Windows PowerShell

Contoh PowerShell skrip berikut memperbarui batas bandwidth-rate gateway. Untuk menggunakan skrip contoh ini, Anda harus memberikan gateway Anda Nama Sumber Daya Amazon (ARN), dan batas unggahan 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

Storage Gateway terdiri dari komponen layanan cloud terkelola dan komponen alat gateway yang Anda terapkan baik lokal, atau di EC2 instans Amazon di AWS cloud. Kedua komponen menerima pembaruan rutin. Topik di bagian ini menjelaskan irama pembaruan ini, cara penerapannya, dan cara mengonfigurasi pengaturan terkait pembaruan di gateway dalam penerapan Anda.

> **Important**
>
> 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 AWS gateway normal (misalnya, SSM atau alat hypervisor) dapat menyebabkan gateway mengalami kerusakan.

Perbarui frekuensi dan perilaku yang diharapkan

AWS memperbarui komponen layanan cloud sesuai kebutuhan tanpa menyebabkan gangguan pada gateway yang digunakan. Peralatan gateway Anda yang digunakan menerima pembaruan pemeliharaan bulanan. Pembaruan pemeliharaan bulanan dapat mencakup peningkatan sistem operasi dan perangkat lunak, perbaikan untuk mengatasi stabilitas, kinerja, dan keamanan, dan akses ke fitur-fitur baru. Semua pembaruan bersifat kumulatif, dan tingkatkan gateway ke versi saat ini saat diterapkan. Untuk informasi tentang perubahan spesifik yang disertakan dalam setiap pembaruan, lihat Catatan Rilis Volume Gateway Appliance.

Pembaruan pemeliharaan bulanan dapat menyebabkan gangguan layanan singkat. Host VM gateway tidak perlu reboot selama pembaruan, tetapi gateway tidak akan tersedia untuk waktu yang singkat sementara alat gateway diperbarui dan dimulai ulang. 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

Saat Anda menerapkan dan mengaktifkan gateway Anda, jadwal jendela pemeliharaan mingguan default ditetapkan. Anda dapat mengubah jadwal jendela pemeliharaan kapan saja. Anda juga dapat menonaktifkan pembaruan pemeliharaan bulanan, tetapi kami sarankan untuk mengaktifkannya.

> **Note**
>
> Pembaruan mendesak terkadang akan diterapkan sesuai dengan jadwal jendela pemeliharaan, bahkan jika pembaruan pemeliharaan rutin dimatikan.

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. Untuk mengubah alamat email tempat pemberitahuan pembaruan perangkat lunak dikirim, lihat Memperbarui kontak alternatif untuk AWS akun Anda di Panduan Referensi Manajemen AWS Akun.

Saat pembaruan tersedia, tab Detail gateway menampilkan pesan pemeliharaan. Anda juga dapat melihat tanggal dan waktu pembaruan terakhir yang berhasil diterapkan pada tab Detail.

Mengaktifkan atau menonaktifkan pembaruan pemeliharaan

Saat pembaruan pemeliharaan diaktifkan, gateway Anda secara otomatis menerapkan pembaruan ini sesuai dengan jadwal jendela pemeliharaan yang dikonfigurasi. Untuk informasi selengkapnya, lihat .

Jika pembaruan pemeliharaan dimatikan, gateway tidak akan menerapkan pembaruan ini secara otomatis, tetapi Anda selalu dapat menerapkannya secara manual menggunakan konsol Storage Gateway, API, atau CLI. Pembaruan mendesak terkadang akan diterapkan selama jendela pemeliharaan yang dikonfigurasi, terlepas dari pengaturan ini.

> **Note**
>
> Prosedur berikut menjelaskan cara mengaktifkan atau menonaktifkan pembaruan gateway menggunakan konsol Storage Gateway. Untuk mengubah setelan ini secara terprogram menggunakan API, lihat UpdateMaintenanceStartTimedi Referensi API Storage Gateway.

Untuk mengaktifkan atau menonaktifkan pembaruan pemeliharaan menggunakan konsol Storage Gateway:

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda konfigurasikan pembaruan pemeliharaan.
3. Pilih Tindakan, lalu pilih Edit pengaturan pemeliharaan.
4. Untuk pembaruan Pemeliharaan, pilih Aktif atau Mati.
5. Pilih Simpan perubahan setelah selesai.

Anda dapat memverifikasi pengaturan yang diperbarui pada tab Detail untuk gateway yang dipilih di konsol Storage Gateway.

Ubah jadwal jendela pemeliharaan gateway

Jika pembaruan pemeliharaan diaktifkan, gateway Anda secara otomatis menerapkan pembaruan ini sesuai jadwal jendela pemeliharaan. Pembaruan mendesak terkadang akan diterapkan selama jendela pemeliharaan yang dikonfigurasi, terlepas dari pengaturan pembaruan pemeliharaan.

> **Note**
>
> Prosedur berikut menjelaskan cara memodifikasi jadwal jendela pemeliharaan menggunakan konsol Storage Gateway. Untuk mengubah setelan ini secara terprogram menggunakan API, lihat UpdateMaintenanceStartTimedi Referensi API Storage Gateway.

Untuk mengubah jadwal jendela pemeliharaan menggunakan konsol Storage Gateway:

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.

2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda konfigurasikan pembaruan pemeliharaan.
3. Pilih Tindakan, lalu pilih Edit pengaturan pemeliharaan.
4. Di bawah waktu mulai jendela Pemeliharaan, lakukan hal berikut:

   a. Untuk Jadwal, pilih Mingguan atau Bulanan untuk mengatur irama jendela pemeliharaan.

   b. Jika Anda memilih Mingguan, ubah nilai untuk Hari dalam seminggu dan Waktu untuk mengatur titik tertentu selama setiap minggu ketika jendela pemeliharaan akan dimulai.

      Jika Anda memilih Bulanan, ubah nilai untuk Hari dalam sebulan dan Waktu untuk mengatur titik tertentu selama setiap bulan ketika jendela pemeliharaan akan dimulai.

      > **Note**
      >
      > Nilai maksimum yang dapat ditetapkan untuk hari dalam sebulan adalah 28. Tidak mungkin mengatur jadwal pemeliharaan untuk dimulai pada hari ke 29 hingga 31. Jika Anda menerima kesalahan saat mengonfigurasi pengaturan ini, itu mungkin berarti perangkat lunak gateway Anda kedaluwarsa. Pertimbangkan untuk memperbarui gateway Anda secara manual terlebih dahulu, dan kemudian mencoba mengonfigurasi jadwal jendela pemeliharaan lagi.

5. Pilih Simpan perubahan setelah selesai.

Anda dapat memverifikasi pengaturan yang diperbarui pada tab Detail untuk gateway yang dipilih di konsol Storage Gateway.

Terapkan pembaruan secara manual

Jika pembaruan perangkat lunak tersedia untuk gateway Anda, Anda dapat menerapkannya secara manual dengan mengikuti prosedur di bawah ini. Proses pembaruan manual ini mengabaikan jadwal jendela pemeliharaan dan segera menerapkan pembaruan, bahkan jika pembaruan pemeliharaan dimatikan.

> **Note**
>
> Prosedur berikut menjelaskan cara menerapkan pembaruan secara manual menggunakan konsol Storage Gateway. Untuk melakukan tindakan ini secara terprogram menggunakan API, lihat UpdateGatewaySoftwareNowdi Storage Gateway API Reference.

Untuk menerapkan pembaruan perangkat lunak gateway secara manual menggunakan konsol Storage Gateway:

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda perbarui.

   Jika pembaruan tersedia, konsol akan menampilkan spanduk notifikasi biru di tab Detail gateway, yang menyertakan opsi untuk menerapkan pembaruan.
3. Pilih Terapkan pembaruan sekarang untuk segera memperbarui gateway.

   > **Note**
   >
   > Operasi ini menyebabkan gangguan sementara pada fungsionalitas gateway saat pembaruan diinstal. Selama waktu ini, status gateway muncul OFFLINE di konsol Storage Gateway. Setelah pembaruan selesai diinstal, gateway melanjutkan operasi normal dan statusnya berubah menjadi RUNNING.

Anda dapat memverifikasi bahwa perangkat lunak gateway telah diperbarui ke versi terbaru dengan memeriksa tab Detail untuk gateway yang dipilih di konsol Storage Gateway.

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. 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 EC2 gateway Amazon 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 EC2 instance 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 Volume GatewayKonsol lokal Gateway VM—lihat.
- Storage Gateway API-—Lihat ShutdownGateway

Memulai dan Menghentikan Volume Gateway

Untuk menghentikan Volume Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
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 Volume Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi, pilih Gateway dan kemudian pilih gateway untuk memulai. Status gateway adalah Shutdown.
3. Pilih Detail. dan kemudian pilih Start gateway.

Menghapus gateway Anda 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.

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 diterapkan pada EC2 instans Amazon, instance 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 Linux Kernel-based Virtual Machine (KVM) klien 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/rumah.
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 tetap ada. EC2 Anda akan terus ditagih untuk sumber daya ini. Anda dapat memilih

untuk menghapus EC2 instans Amazon dan snapshot Amazon EBS dengan membatalkan langganan Amazon Anda. EC2 Jika Anda ingin mempertahankan EC2 langganan Amazon, 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 Volume Gateway yang Diterapkan pada VM

Jika gateway yang ingin Anda hapus digunakan pada mesin virtual (VM), kami sarankan Anda mengambil tindakan berikut untuk membersihkan sumber daya:

- Hapus gateway. Untuk petunjuk, silakan lihat Menghapus Gateway Anda dengan Menggunakan Storage Gateway Console.
- Hapus semua snapshot Amazon EBS yang tidak Anda butuhkan. Untuk petunjuk, lihat Menghapus Snapshot Amazon EBS di Panduan Pengguna Amazon EC2 .

Menghapus Sumber Daya dari Gateway yang Diterapkan di Instans Amazon EC2

Jika Anda ingin menghapus gateway yang Anda gunakan di EC2 instans Amazon, sebaiknya Anda membersihkan AWS sumber daya yang digunakan dengan gateway, khususnya EC2 instans Amazon, 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 Volume Cache Anda yang Diterapkan di Amazon EC2

Jika Anda menerapkan gateway dengan volume cache aktif EC2, kami sarankan Anda mengambil tindakan berikut untuk menghapus gateway Anda dan membersihkan sumber dayanya:

1. Di konsol Storage Gateway, hapus gateway seperti yang ditunjukkan padaMenghapus Gateway Anda dengan Menggunakan Storage Gateway Console.
2. Di EC2 konsol Amazon, hentikan EC2 instans Anda jika Anda berencana menggunakan instance lagi. Jika tidak, hentikan instance. Jika Anda berencana menghapus volume, catat perangkat blok

yang dilampirkan ke instance dan pengidentifikasi perangkat sebelum menghentikan instance. Anda akan memerlukan ini untuk mengidentifikasi volume yang ingin Anda hapus.

3. Di EC2 konsol Amazon, hapus semua volume Amazon EBS yang dilampirkan ke instans jika Anda tidak berencana menggunakannya lagi. Untuk informasi selengkapnya, lihat Membersihkan Instans dan Volume Anda di Panduan EC2 Pengguna Amazon.

Melakukan tugas pemeliharaan menggunakan konsol lokal

Bagian ini berisi topik-topik berikut, yang memberikan informasi tentang cara melakukan tugas pemeliharaan menggunakan konsol lokal alat gateway. Konsol lokal berjalan langsung pada platform host virtualisasi yang meng-host perangkat gateway Anda. Untuk gateway lokal, Anda mengakses konsol lokal melalui host virtualisasi KVM Hyper-V, atau Linux. VMware Untuk EC2 gateway Amazon, Anda mengakses konsol dengan menghubungkan ke EC2 instans Amazon menggunakan SSH. Sebagian besar tugas umum di berbagai platform host, tetapi ada juga beberapa perbedaan.

Topik

- Mengakses Konsol Lokal Gateway- Pelajari cara masuk ke konsol lokal untuk gateway lokal yang dihosting di Linux Kernel-based Virtual Machine (KVM), VMware ESXi atau platform Microsoft Hyper-V Manager.
- Melakukan Tugas di Konsol Lokal VM- Pelajari cara menggunakan konsol lokal untuk melakukan penyiapan dasar dan tugas konfigurasi lanjutan untuk gateway lokal, seperti mengonfigurasi proxy HTTP, melihat status sumber daya sistem, atau menjalankan perintah terminal.
- Melakukan Tugas di Konsol EC2 Lokal Amazon- Pelajari cara masuk ke konsol lokal untuk melakukan pengaturan dasar dan tugas konfigurasi lanjutan untuk EC2 gateway Amazon, seperti mengonfigurasi proxy HTTP, melihat status sumber daya sistem, atau menjalankan perintah terminal.

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 daftar VMs yang saat ini tersedia di KVM.

   ```
   # virsh list
   ```

   Perintah mengembalikan daftar VMs dengan Id, Nama, dan informasi Negara untuk masing-masing. Perhatikan VM yang ingin Anda luncurkan konsol lokal gateway. `Id`

2. Gunakan perintah berikut untuk mengakses konsol lokal.

   ```
   # virsh console Id
   ```

   Ganti *`Id`* dengan Id VM yang Anda catat di langkah sebelumnya.

   Konsol lokal gateway AWS Appliance meminta Anda untuk masuk untuk mengubah konfigurasi jaringan dan pengaturan lainnya.

3. Masukkan nama pengguna dan kata sandi Anda untuk masuk ke konsol lokal gateway. Untuk informasi selengkapnya, lihat lokal Volume Gateway.

   Setelah Anda masuk, menu AWS Appliance Activation - Configuration muncul. Anda dapat memilih dari opsi menu untuk melakukan tugas konfigurasi gateway. Untuk informasi selengkapnya, lihat Melakukan tugas di konsol lokal mesin virtual.

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 VM gateway dihidupkan.

> **Note**
>
> Jika VM gateway Anda dihidupkan, ikon panah hijau muncul dengan ikon VM di panel browser VM di sisi kiri jendela aplikasi. Jika VM gateway Anda tidak dihidupkan, Anda dapat menyalakannya dengan memilih ikon Power On hijau pada Toolbar di bagian atas jendela aplikasi.

3. Pilih tab Konsol di panel informasi utama di sisi kanan jendela aplikasi.

   Setelah beberapa saat, konsol lokal gateway AWS Appliance meminta Anda untuk masuk untuk mengubah konfigurasi jaringan dan pengaturan lainnya.

   > **Note**
   >
   > Untuk melepaskan kursor dari jendela konsol, tekan Ctrl+Alt.

4. Masukkan nama pengguna dan kata sandi Anda untuk masuk ke konsol lokal gateway. Untuk informasi selengkapnya, lihat lokal Volume Gateway.

   Setelah Anda masuk, menu AWS Appliance Activation - Configuration muncul. Anda dapat memilih dari opsi menu untuk melakukan tugas konfigurasi gateway. Untuk informasi selengkapnya, lihat Melakukan tugas di konsol lokal mesin virtual.

Akses Konsol Lokal Gateway dengan Microsoft Hyper-V

Untuk mengakses konsol lokal gateway Anda (Microsoft Hyper-V)

1. Pilih VM alat gateway Anda dari panel Mesin Virtual di sisi kiri jendela aplikasi Microsoft Hyper-V Manager.
2. Pastikan gateway dihidupkan.

   > **Note**
   >
   > Jika VM gateway Anda dihidupkan, `Running` ditampilkan di kolom Status untuk VM di panel Mesin Virtual di sisi kiri jendela aplikasi. Jika VM gateway Anda tidak dihidupkan,

Anda dapat menyalakannya dengan memilih Mulai di panel Tindakan di sisi kanan jendela aplikasi.

3. Pilih Connect dari panel Actions.

   Jendela Virtual Machine Connection muncul. Jika jendela otentikasi muncul, ketikkan kredensyal masuk yang diberikan kepada Anda oleh administrator hypervisor.

   Setelah beberapa saat, konsol lokal gateway AWS Appliance meminta Anda untuk masuk untuk mengubah konfigurasi jaringan dan pengaturan lainnya.

4. Masukkan nama pengguna dan kata sandi Anda untuk masuk ke konsol lokal gateway. Untuk informasi selengkapnya, lihat lokal Volume Gateway.

   Setelah Anda masuk, menu AWS Appliance Activation - Configuration muncul. Anda dapat memilih dari opsi menu untuk melakukan tugas konfigurasi gateway. Untuk informasi selengkapnya, lihat Melakukan tugas di konsol lokal mesin virtual.

Melakukan Tugas di Konsol Lokal VM

Untuk yang Anda terapkan di lokasi, Anda dapat melakukan tugas pemeliharaan berikut menggunakan konsol lokal gateway yang Anda akses dari platform host mesin virtual Anda. Tugas-tugas ini umum untuk VMware, Microsoft Hyper-V, dan Linux Kernel-based Virtual Machine (KVM) hypervisor.

Topik

- Masuk ke konsol lokal Volume Gateway- Pelajari tentang cara masuk ke konsol lokal gateway tempat Anda dapat mengonfigurasi pengaturan jaringan gateway dan mengubah kata sandi default.
- Mengonfigurasi SOCKS5 proxy untuk gateway lokal Anda- Pelajari bagaimana Anda dapat mengonfigurasi Storage Gateway untuk merutekan semua lalu lintas AWS endpoint melalui server proxy Socket Secure versi 5 (SOCKS5).
- Mengkonfigurasi Jaringan Gateway Anda- Pelajari tentang bagaimana Anda dapat mengonfigurasi gateway Anda untuk menggunakan DHCP atau menetapkan alamat IP statis.
- Menguji koneksi gateway Anda ke internet- Pelajari tentang bagaimana Anda dapat menggunakan konsol lokal gateway untuk menguji koneksi antara gateway dan internet.

- Menjalankan perintah gateway penyimpanan di konsol lokal untuk gateway lokal- Pelajari cara menjalankan perintah konsol lokal yang memungkinkan Anda melakukan tugas tambahan seperti menyimpan tabel perutean, menghubungkan Dukungan, dan banyak lagi.
- Melihat status sumber daya sistem gateway Anda- Pelajari tentang cara memeriksa inti CPU virtual, ukuran volume root, dan RAM yang tersedia untuk alat gateway Anda.

Masuk ke konsol lokal Volume Gateway

Ketika VM siap bagi Anda untuk masuk, layar login akan ditampilkan. Jika ini adalah pertama kalinya Anda masuk ke konsol lokal, Anda menggunakan kredenal masuk default untuk masuk. Kredensi 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 Konsol Storage Gateway.

Untuk masuk ke konsol lokal gateway

- Jika ini adalah pertama kalinya Anda masuk ke konsol lokal, masuk ke VM dengan kredenal 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 gateway penyimpanan di konsol lokal untuk gateway lokal. Anda juga dapat mengatur kata sandi Anda sendiri dari AWS Storage Gateway konsol. Untuk informasi selengkapnya, lihat Mengatur Kata Sandi Konsol Lokal dari Konsol Storage Gateway.

> **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.

Mengatur Kata Sandi Konsol Lokal dari Konsol Storage Gateway

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/rumah.
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, konfirmasikan 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.

Mengonfigurasi SOCKS5 proxy untuk gateway lokal Anda

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, lihatPersyaratan jaringan dan firewall.

Prosedur berikut menunjukkan cara mengkonfigurasi proxy SOCKS untuk Volume Gateway dan Tape Gateway.

Untuk mengonfigurasi SOCKS5 proxy untuk volume dan Tape Gateways

1. Masuk ke konsol lokal gateway Anda.
   - VMware ESXi — untuk informasi lebih lanjut, lihatMengakses 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
Konfigurasikan proxy SOCKS	Masukkan angka yang sesuai untuk memilih Configure SOCKS Proxy. Anda harus menyediakan nama host dan port untuk menyelesaikan konfigurasi.

Untuk Melakukan Tugas Ini	Lakukan Ini
Lihat konfigurasi proxy SOCKS saat ini	Masukkan angka yang sesuai untuk memilih Lihat Konfigurasi Proksi SOCKS Saat Ini. Jika proxy SOCKS tidak dikonfigurasi, pesan akan `SOCKS Proxy not configured` ditampilkan. Jika proxy SOCKS dikonfigurasi, nama host dan port proxy akan ditampilkan.
Hapus konfigurasi proxy SOCKS	Masukkan angka yang sesuai untuk memilih Hapus Konfigurasi Proksi SOCKS. Pesan `SOCKS Proxy Configuration Removed` ditampilkan.

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, lihatMengakses 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	Masukkan angka yang sesuai untuk memilih Deskripsikan Adaptor. 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: • Alamat kontrol akses media (MAC) • Alamat IP • Netmask • Alamat IP Gateway • Status diaktifkan DHCP Anda menggunakan nama adaptor yang tercantum di sini saat Anda mengonfigurasi alamat IP statis atau mengatur adaptor default gateway Anda.
Konfigurasikan DHCP	Masukkan angka yang sesuai untuk memilih Konfigurasi DHCP. Anda diminta untuk mengkonfigurasi antarmuka jaringan untuk menggunakan DHCP.

Untuk Melakukan Tugas Ini	Lakukan Ini
Konfigurasikan alamat IP statis untuk gateway Anda	Masukkan angka yang sesuai untuk memilih Konfigurasi IP Statis. Anda diminta untuk mengetik informasi berikut untuk mengkonfigurasi IP statis: • Nama adaptor jaringan • Alamat IP • Netmask • Alamat gateway default • Alamat Layanan Nama Domain Utama (DNS) • Alamat DNS sekunder **Important** 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. Jika gateway Anda menggunakan lebih dari satu antarmuka jaringan, Anda harus mengatur semua antarmuka yang diaktifkan untuk menggunakan DHCP atau alamat IP statis.

Untuk Melakukan Tugas Ini	Lakukan Ini
	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. Jika kedua antarmuka awalnya diatur untuk menggunakan alamat IP statis dan Anda kemudian mengatur gateway untuk menggunak an DHCP, kedua antarmuka akan menggunak an DHCP.

Untuk Melakukan Tugas Ini	Lakukan Ini
Konfigurasikan nama host untuk gateway Anda	Masukkan angka yang sesuai untuk memilih Configure Hostname. Anda diminta untuk memilih apakah gateway akan menggunakan nama host statis yang Anda tentukan, atau mendapatkannya secara otomatis melalui DCHP atau RDNs. Jika Anda memilih Statis, Anda diminta untuk memberikan nama host statis, seperti. `testgateway.example.com` Masukkan y untuk menerapkan konfigurasi. **Note** Jika Anda mengonfigurasi nama host statis untuk gateway Anda, pastikan bahwa nama host yang disediakan ada di domain tempat gateway bergabung . Anda juga harus membuat catatan A di sistem DNS Anda yang mengarahk an alamat IP gateway ke nama host statisnya.

Untuk Melakukan Tugas Ini	Lakukan Ini
Setel ulang semua konfigurasi jaringan gateway Anda ke DHCP	Masukkan angka yang sesuai untuk memilih Reset semua ke DHCP. Semua antarmuka jaringan diatur untuk menggunakan DHCP. **Important** Jika gateway Anda telah diaktifkan, Anda harus mematikan dan memulai ulang gateway Anda dari konsol Storage Gateway agar pengaturan diterapkan. Untuk informasi selengkap nya, lihat Mematikan VM Gateway Anda.
Tetapkan adaptor rute default gateway Anda	Masukkan angka yang sesuai untuk memilih Set Default Adapter. Adaptor yang tersedia untuk gateway Anda ditampilkan, dan Anda diminta untuk memilih salah satu adaptor—misalnya,. **`eth0`**
Lihat konfigurasi DNS gateway Anda	Masukkan angka yang sesuai untuk memilih Lihat Konfigurasi DNS. Alamat IP server nama DNS primer dan sekunder ditampilkan.

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, lihatMengakses 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.

Menjalankan perintah gateway penyimpanan di konsol lokal untuk gateway 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 Dukungan, dan sebagainya.

Untuk menjalankan konfigurasi atau perintah diagnostik

1. Masuk ke konsol lokal gateway Anda:
   - Untuk informasi selengkapnya tentang masuk ke konsol VMware ESXi lokal, lihatMengakses 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 AWS Appliance Activation - Configuration, 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 konfigurasikan antarmuka jaringan. **Note** Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus. Untuk petunjuk, lihat Gateway Anda.
ip	Menampilkan/memanipulasi routing, perangkat , dan terowongan. **Note** Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus. Untuk petunjuk, lihat Gateway Anda.
iptables	Alat administrasi untuk penyaringan IPv4 paket dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.

Perintah	Fungsi
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.
sslcheck	Mengembalikan output dengan penerbit sertifikat **Note** Storage Gateway menggunakan verifikasi penerbit sertifikat dan tidak mendukung inspeksi ssl. Jika perintah ini mengembalikan penerbit selain aws-appliance@amazon.com, maka kemungkinan aplikasi melakukan inspeksi ssl. Dalam hal ini, kami sarankan untuk melewati inspeksi ssl untuk alat Storage Gateway.
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 **`man`** + *`command name`* 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 VMware ESXi konsol, lihatMengakses 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
[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 menampilk an pesan yang menjelaskan hasil pemeriksaan sumber daya.
[GAGAL]	Sumber daya tidak memenuhi persyarat an minimum. Gateway Anda mungkin tidak berfungsi dengan baik. Storage Gateway

Pesan	Deskripsi
	menampilkan pesan yang menjelaskan hasil pemeriksaan sumber daya.

Konsol juga menampilkan jumlah kesalahan dan peringatan di sebelah opsi menu centang sumber daya.

Melakukan Tugas di Konsol EC2 Lokal Amazon

Beberapa tugas pemeliharaan Storage Gateway mengharuskan Anda masuk ke konsol lokal gateway untuk mendapatkan gateway yang telah digunakan di EC2 instans Amazon. Anda dapat mengakses konsol lokal gateway di EC2 instans Amazon Anda dengan menggunakan klien Secure Shell (SSH). Topik di bagian ini menjelaskan cara masuk ke konsol lokal gateway dan melakukan tugas pemeliharaan.

Topik

- Masuk ke Konsol Lokal Amazon EC2 Gateway Anda- Pelajari bagaimana Anda dapat terhubung dan masuk ke konsol lokal gateway EC2 instans Amazon Anda dengan menggunakan klien Secure Shell (SSH).
- Merutekan gateway Anda yang digunakan EC2 melalui proxy HTTP- Pelajari cara mengonfigurasi Storage Gateway untuk merutekan semua lalu lintas AWS enpoint melalui server proxy Socket Secure versi 5 (SOCKS5) ke instans EC2 gateway Amazon Anda.
- Menguji konektivitas jaringan gateway- Pelajari bagaimana Anda dapat menggunakan konsol lokal gateway untuk menguji konektivitas jaringan antara gateway Anda dan berbagai sumber daya jaringan.
- Melihat status sumber daya sistem gateway Anda- Pelajari tentang bagaimana Anda dapat menggunakan konsol lokal gateway untuk memeriksa inti CPU virtual, ukuran volume root, dan RAM yang tersedia untuk alat gateway Anda.
- Menjalankan perintah Storage Gateway di konsol lokal- Pelajari bagaimana Anda dapat menjalankan perintah konsol lokal yang memungkinkan Anda melakukan tugas tambahan seperti menyimpan tabel perutean, menghubungkan ke Dukungan, dan banyak lagi.

Masuk ke Konsol Lokal Amazon EC2 Gateway Anda

Anda dapat terhubung ke EC2 instans Amazon menggunakan klien Secure Shell (SSH). Untuk informasi selengkapnya, lihat Connect to Your Instance di Panduan EC2 Pengguna Amazon. Untuk menghubungkan dengan cara ini, Anda akan memerlukan key pair SSH yang Anda tentukan saat meluncurkan instance. Untuk informasi tentang pasangan EC2 kunci Amazon, lihat Pasangan EC2 Kunci Amazon di Panduan EC2 Pengguna Amazon.

Untuk masuk ke konsol lokal gateway

1. Masuk ke konsol lokal Anda. Jika Anda terhubung ke EC2 instans 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
Konfigurasikan proxy SOCKS untuk gateway Anda	Merutekan gateway Anda yang digunakan EC2 melalui proxy HTTP
Uji konektivitas jaringan	Menguji konektivitas jaringan gateway
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 digunakan 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, silakan lihat Masuk ke Konsol Lokal Amazon EC2 Gateway Anda.
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 proxy HTTP - Anda harus 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 ditampilkan.
   - Hapus konfigurasi proxy HTTP - Pesan `HTTP Proxy Configuration Removed` ditampilkan.

Menguji konektivitas jaringan gateway

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, silakan lihat Masuk ke Konsol Lokal Amazon EC2 Gateway Anda.
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, silakan lihat Masuk ke Konsol Lokal Amazon EC2 Gateway Anda.
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 menampilk an pesan yang menjelaskan hasil pemeriksaan sumber daya.
[GAGAL]	Sumber daya tidak memenuhi persyarat an 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 Dukungan.

Untuk menjalankan konfigurasi atau perintah diagnostik

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, silakan lihat Masuk ke Konsol Lokal Amazon EC2 Gateway Anda.
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.
-h	Tampilkan daftar perintah yang tersedia.
ifconfig	Lihat atau konfigurasikan antarmuka jaringan. **Note** Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus.
ip	Menampilkan/memanipulasi routing, perangkat , dan terowongan. **Note** Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus.
iptables	Alat administrasi untuk penyaringan IPv4 paket dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.

Perintah	Fungsi
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.
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`.

Performa dan optimasi untuk Volume Gateway

Bagian ini menjelaskan kinerja Storage Gateway.

Topik

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 24 core CPU fisik khusus
- Untuk Volume 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
- Disk 1, untuk digunakan sebagai cache gateway sebagai berikut:
  - SSD menggunakan NVMe pengontrol.
- Disk 2, untuk digunakan sebagai buffer upload gateway sebagai berikut:
  - SSD menggunakan NVMe pengontrol.
- Disk 3, untuk digunakan sebagai buffer upload gateway sebagai berikut:
  - SSD menggunakan NVMe pengontrol.
- Adaptor jaringan 1 dikonfigurasi pada jaringan VM 1:
  - Gunakan jaringan VM 1 dan tambahkan VMXnet3 (10 Gbps) yang akan 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 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 (SSDs) 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. .

> **Note**
>
> CloudWatch metrik tidak tersedia untuk semua gateway. Untuk informasi tentang metrik gateway, lihatMemantau 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 tersebut 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, konfirmasikan bahwa setiap prosesor virtual yang ditetapkan ke VM gateway didukung oleh inti CPU khusus. Selain itu, konfirmasikan bahwa Anda tidak kelebihan langganan CPUs server host.

Ketika Anda menambahkan tambahan CPUs 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. Tambahan CPUs juga membantu memastikan bahwa gateway Anda mendapatkan sumber daya CPU yang cukup saat host dibagikan dengan yang lain VMs. Menyediakan sumber daya CPU yang cukup memiliki efek umum meningkatkan throughput.

Tingkatkan bandwidth antara gateway dan AWS cloud

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.

> **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.

Ubah konfigurasi volume

Untuk Volume Gateways, jika Anda menemukan bahwa menambahkan lebih banyak volume ke gateway mengurangi throughput ke gateway, pertimbangkan untuk menambahkan volume ke gateway terpisah. Secara khusus, jika volume digunakan untuk aplikasi throughput tinggi,

pertimbangkan untuk membuat gateway terpisah untuk aplikasi throughput tinggi. Namun, sebagai aturan umum, Anda tidak boleh menggunakan satu gateway untuk semua aplikasi throughput tinggi dan gateway lain untuk semua aplikasi throughput rendah Anda. Untuk mengukur throughput volume Anda, gunakan `ReadBytes` dan `WriteBytes` metrik.

Untuk informasi selengkapnya tentang metrik ini, lihat Mengukur Kinerja Antara Aplikasi dan Gateway.

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.

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.

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 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 CPUs dapat membantu aplikasi Anda untuk menskalakan beban I/O-nya.

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 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

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 mempertahankan kendali atas konten yang di-host 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 kredensyal 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. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

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 SDKs. 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 AWS penyimpanan Anda. 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 Membuat NFSFile Bagikan di Referensi AWS Storage Gateway API.

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 cache atau disimpan, lihat CreateCachediSCSIVolumeatau CreateStorediSCSIVolumedi Referensi AWS Storage Gateway API.

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 CreateTapesdi 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 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?

Mengkonfigurasi otentikasi CHAP untuk volume Anda

Di Storage Gateway, inisiator iSCSI Anda terhubung ke volume Anda sebagai target iSCSI. Storage Gateway menggunakan Challenge-Handshake Authentication Protocol (CHAP) untuk mengautentikasi koneksi iSCSI dan inisiator. CHAP memberikan perlindungan terhadap serangan pemutaran dengan memerlukan otentikasi untuk mengakses target volume penyimpanan. Untuk setiap target volume, Anda dapat menentukan satu atau lebih kredensional CHAP. Anda dapat

melihat dan mengedit kredensi ini untuk inisiator yang berbeda di kotak dialog Konfigurasi kredensial CHAP.

Untuk mengkonfigurasi kredenal CHAP

1. Di Storage Gateway Console, pilih Volume dan pilih volume yang ingin Anda konfigurasikan kredenal CHAP.
2. Untuk Tindakan, pilih Konfigurasi otentikasi CHAP.
3. Untuk nama Inisiator, ketikkan nama inisiator Anda. Nama harus minimal 1 karakter dan paling banyak 255 karakter panjangnya.
4. Untuk rahasia Inisiator, berikan frasa rahasia yang ingin Anda gunakan untuk mengautentikasi inisiator iSCSI Anda. Frase rahasia inisiator harus setidaknya 12 karakter dan paling banyak 16 karakter panjangnya.
5. Untuk rahasia Target, berikan frasa rahasia yang ingin Anda gunakan untuk mengotentikasi target Anda untuk CHAP bersama. Frasa rahasia target harus setidaknya 12 karakter dan paling banyak 16 karakter panjangnya.
6. Pilih Simpan untuk menyimpan entri Anda.

Untuk melihat atau memperbarui kredensi CHAP, Anda harus memiliki izin peran IAM yang diperlukan yang memungkinkan Anda melakukan operasi itu.

Melihat dan mengedit kredensi CHAP

Anda dapat menambahkan, menghapus, atau memperbarui kredensi CHAP untuk setiap pengguna. Anda harus memiliki izin peran IAM yang diperlukan untuk melihat atau mengedit kredenal CHAP, dan target inisiator harus dilampirkan ke gateway yang berfungsi.

Untuk menambahkan kredensi CHAP

1. Di Storage Gateway Console, pilih Volume dan pilih volume yang ingin Anda tambahkan kredensialnya CHAP.
2. Untuk Tindakan, pilih Konfigurasi otentikasi CHAP.
3. Di halaman Konfigurasi CHAPS, berikan nama Inisiator, rahasia Inisiator, dan rahasia Target di kotak masing-masing dan pilih Simpan.

Untuk menghapus kredensi CHAP

1. Di Storage Gateway Console, pilih Volume dan pilih volume yang ingin Anda hapus kredensialnya CHAP.
2. Untuk Tindakan, pilih Konfigurasi otentikasi CHAP.
3. Klik X di samping kredenal yang ingin Anda hapus dan pilih Simpan.

Untuk memperbarui kredensi CHAP

1. Di Storage Gateway Console, pilih Volume dan pilih volume yang ingin Anda perbarui CHAP.
2. Untuk Tindakan, pilih Konfigurasi otentikasi CHAP.
3. Di halaman Configure CHAP credentials, ubah entri untuk kredensi yang akan Anda perbarui.
4. Pilih Simpan.

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

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 kredensi 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 untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar 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

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi 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 kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, 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 kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam 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 selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Autentikasi multi-faktor AWS di IAM 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. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi 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 kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan 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 Apakah itu 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, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi 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 sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan 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 dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM 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. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set 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 (prinsipal tepercaya) di akun lain untuk mengakses sumber daya 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 peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, 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 sebuah tindakan yang kemudian menginisiasi 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 Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah 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 menjalankan peran untuk melakukan 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 kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI

atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di 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 Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah 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 oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas,

lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. 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 yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola 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 tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal 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 (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnya ACLs, lihat Ringkasan daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM 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 eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs 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 suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. 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 dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu 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
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
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 oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan 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

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 tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah 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. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun

yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam 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, di mana utama dapat melakukan tindakan pada sumber daya, 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.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk 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 tersebut dengan koma.

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

Untuk melihat contoh kebijakan berbasis identitas AWS SGW, lihat. Contoh kebijakan berbasis identitas untuk Storage Gateway

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, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan 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 menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya AWS SGW dan jenisnya ARNs, lihat Sumber Daya yang Ditetapkan oleh 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

Kunci kondisi kebijakan untuk AWS SGW

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat 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 sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya 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, lihat Elemen kebijakan IAM: variabel dan tanda dalam 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

ACLs di AWS SGW

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan SGW AWS

Mendukung ABAC (tag dalam kebijakan): Sebagian

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. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `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 untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensi sementara dengan SGW AWS

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi 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 kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara 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 sebuah tindakan yang kemudian menginisiasi 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 Sesi akses maju.

Peran layanan untuk AWS SGW

Mendukung peran layanan: Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah 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 terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan 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 manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari 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

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 di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS SGW, termasuk format ARNs untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk AWS Storage Gateway di Referensi Otorisasi Layanan.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya AWS SGW di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. 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 Anda Akun AWS. 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 tugas dalam 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 melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan 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: Kondisi dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – 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 dengan IAM Access Analyzer dalam 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 meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam 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. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

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 Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan 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:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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

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 orang-orang 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 (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi 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 Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

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 Mulai Cepat 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 Wilayah AWS dan Availability Zones.

An Wilayah AWS adalah lokasi fisik di seluruh dunia di mana pusat data dikelompokkan. Setiap kelompok pusat data logis disebut Availability Zone (AZ). Masing-masing Wilayah AWS terdiri dari minimal tiga terisolasi dan terpisah secara fisik AZs dalam wilayah geografis. Tidak seperti penyedia cloud lainnya, yang sering mendefinisikan suatu wilayah sebagai pusat data tunggal, desain AZ ganda dari masing-masing Wilayah AWS menawarkan keuntungan yang berbeda. Setiap AZ memiliki daya independen, pendinginan, dan keamanan fisik dan terhubung melalui jaringan yang berlebihan. ultra-low-latency Jika penerapan Anda memerlukan fokus pada ketersediaan tinggi, Anda dapat mengonfigurasi layanan dan sumber daya ke dalam beberapa AZs untuk mencapai toleransi kesalahan yang lebih besar.

Wilayah AWS memenuhi tingkat keamanan infrastruktur, kepatuhan, dan perlindungan data tertinggi. Semua lalu lintas di antaranya AZs dienkripsi. Kinerja jaringan cukup untuk mencapai replikasi sinkron antara. AZs AZs membuat layanan partisi dan sumber daya untuk ketersediaan tinggi mudah. Jika penyebaran Anda dipartisi AZs, sumber daya Anda lebih terisolasi dan terlindungi dari masalah seperti pemadaman listrik, sambaran petir, tornado, gempa bumi, dan banyak lagi. AZs Secara fisik dipisahkan oleh jarak yang berarti dari AZ lainnya, meskipun semuanya berada dalam jarak 100 km (60 mil) satu sama lain.

Untuk informasi selengkapnya tentang Wilayah AWS 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.
- Gunakan AWS Backup untuk membuat cadangan volume Anda. Untuk informasi selengkapnya, lihat Mencadangkan volume Anda.
- Kloning volume Anda dari titik pemulihan. Untuk informasi selengkapnya, lihat Mengkloning volume yang di-cache dari titik pemulihan.

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 menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

> **Note**
>
> Anda harus memperlakukan alat AWS Storage Gateway sebagai mesin virtual terkelola, dan tidak boleh mencoba mengakses atau memodifikasi pemasangannya dengan cara apa pun. Mencoba menginstal perangkat lunak pemindaian atau memperbarui paket perangkat lunak apa pun menggunakan metode selain mekanisme pembaruan gateway normal, dapat menyebabkan gateway tidak berfungsi dan dapat memengaruhi kemampuan kami untuk mendukung atau memperbaiki gateway.
> AWS ulasan, analisis, dan remediasi CVEs secara teratur. Kami menggabungkan perbaikan untuk masalah ini ke dalam Storage Gateway sebagai bagian dari siklus rilis perangkat lunak normal kami. Perbaikan ini biasanya diterapkan sebagai bagian dari proses pembaruan gateway normal selama jendela pemeliharaan terjadwal. Untuk informasi selengkapnya tentang pembaruan gateway, lihat .

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.

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 partisi AWS 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
- Mengkonfigurasi 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 entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu 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 mana pun 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": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
```

```
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                    "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
            }]
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan ListGateways tindakan.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
```

```
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
             }]
}
```

Pemecahan masalah gateway

Berikut ini, Anda dapat menemukan informasi tentang praktik terbaik dan masalah pemecahan masalah yang terkait dengan gateway, platform host, volume, ketersediaan tinggi, pemulihan data, dan snapshot. Informasi pemecahan masalah gateway lokal mencakup gateway yang digunakan pada platform virtualisasi yang didukung. Informasi pemecahan masalah untuk masalah ketersediaan tinggi mencakup gateway yang berjalan pada platform VMware vSphere High Availability (HA).

Topik

- Pemecahan masalah: masalah offline gateway- Pelajari cara mendiagnosis masalah yang dapat menyebabkan gateway Anda muncul offline di konsol Storage Gateway.
- Pemecahan masalah: kesalahan internal selama aktivasi gateway- Pelajari apa yang harus dilakukan jika Anda menerima pesan galat internal saat mencoba mengaktifkan Storage Gateway Anda.
- Memecahkan masalah gateway lokal- Pelajari tentang masalah umum yang mungkin Anda temui saat bekerja dengan gateway lokal, dan cara mengizinkan untuk terhubung Dukungan ke gateway untuk membantu pemecahan masalah.
- Memecahkan masalah pengaturan Microsoft Hyper-V- Pelajari tentang masalah umum yang mungkin Anda temui saat menerapkan Storage Gateway di platform Microsoft Hyper-V.
- Memecahkan masalah gateway Amazon EC2 - Temukan informasi tentang masalah umum yang mungkin Anda temui saat bekerja dengan gateway yang digunakan di Amazon. EC2
- Memecahkan masalah alat perangkat keras- Pelajari cara mengatasi masalah yang mungkin Anda temui dengan Storage Gateway Hardware Appliance.
- Memecahkan masalah volume- Temukan informasi tentang sebagian besar masalah umum yang mungkin Anda temui saat bekerja dengan volume, dan tindakan yang kami sarankan untuk Anda ambil untuk memperbaikinya.
- Memecahkan masalah ketersediaan tinggi- Pelajari apa yang harus dilakukan jika Anda mengalami masalah dengan gateway yang digunakan di lingkungan HA. VMware

Pemecahan masalah: masalah offline 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.

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 .

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. Konfigurasikan ulang disk untuk penyimpanan cache.
4. Mulai ulang gateway.

Pemecahan masalah: kesalahan internal selama aktivasi 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 AMIs 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 EC2 instans Amazon, 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 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 *region* 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, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
```

```
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

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. Untuk informasi selengkapnya, lihat .

Opsi Manajemen Waktu Sistem tidak tersedia di gateway yang di-host di instans Amazon EC2 . Untuk memastikan EC2 gateway Amazon dapat menyinkronkan waktu dengan benar, konfirmasikan bahwa EC2 instans Amazon 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 titik akhir 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) terbuka. EC2 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

Untuk informasi selengkapnya, lihat .

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, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

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. Untuk informasi selengkapnya, lihat .

Opsi Manajemen Waktu Sistem tidak tersedia di gateway yang di-host di instans Amazon EC2 . Untuk memastikan EC2 gateway Amazon dapat menyinkronkan waktu dengan benar, konfirmasikan bahwa EC2 instans Amazon 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 konfirmasikan pengaturan grup keamanan terkait

Sebelum aktivasi, periksa apakah Anda memiliki proxy HTTP di Amazon yang EC2 dikonfigurasi di VM gateway lokal sebagai proxy Squid di port 3128. Dalam hal ini, konfirmasikan 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 EC2 VPC Amazon 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 enpoint 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 Dukungan untuk membantu memecahkan masalah gateway.

Tabel berikut mencantumkan masalah umum yang mungkin Anda temui saat bekerja dengan gateway lokal.

Isu	Tindakan yang Harus Dilakukan
Anda tidak dapat menemukan alamat IP gateway Anda.	Gunakan klien hypervisor untuk terhubung ke host Anda untuk menemukan alamat IP gateway. • 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. Jika Anda masih mengalami kesulitan menemukan alamat IP gateway: • 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.
Anda mengalami masalah jaringan atau firewall.	• Izinkan port yang sesuai untuk gateway Anda. • Sertifikat SSL validation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign baik 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 selengkap nya tentang persyaratan jaringan dan firewall, lihatPersyaratan jaringan dan firewall.
Aktivasi gateway Anda gagal ketika Anda mengklik tombol Lanjutkan ke Aktivasi di Storage	• Periksa apakah VM gateway dapat diakses dengan melakukan ping VM dari klien Anda.

Isu	Tindakan yang Harus Dilakukan
Gateway Management Console.	• Periksa apakah VM Anda memiliki konektivitas jaringan ke internet. Jika tidak, Anda harus mengonfigurasi proxy SOCKS. Untuk informasi selengkapnya tentang cara melakukannya, lihat Mengonfigurasi SOCKS5 proxy untuk gateway lokal Anda. • 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 VMs, lihat. Sinkronkan waktu VM dengan waktu host Hyper-V atau Linux KVM • Setelah melakukan langkah-langkah ini, Anda dapat mencoba kembali penerapan gateway menggunakan konsol Storage Gateway dan wizard Setup and Activate Gateway. • Sertifikat SSL validation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign baik 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 untuk mengatur Volume Gateway.
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
Anda perlu meningkatkan bandwidth antara gateway Anda dan AWS.	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 menghinda ri pertengkaran bandwidth, terutama selama pemulihan snapshot. Untuk kebutuhan beban kerja throughput tinggi, Anda dapat menggunakannya AWS Direct Connectuntuk membuat koneksi jaringan khusus antara gateway lokal dan gateway. AWS Untuk mengukur bandwidth koneksi dari gateway Anda ke AWS, gunakan `CloudBytesDownloaded` dan `CloudBytesUploaded` metrik gateway. Untuk lebih lanjut tentang hal ini, lihat Mengukur Kinerja Antara Gateway Anda dan AWS. Meningkatkan konektivitas internet Anda membantu memastikan bahwa buffer unggahan Anda tidak terisi.

Isu	Tindakan yang Harus Dilakukan

Throughput ke atau dari gateway Anda turun ke nol.	• Pada tab Gateway 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 padaMematikan 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 dalamMenguji koneksi gateway Anda ke internet.
	• Periksa konfigurasi adaptor jaringan gateway Anda, dan pastikan bahwa semua antarmuka yang Anda inginkan untuk diaktifka n 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.
	
	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 Gateway Anda dan AWS.

Anda mengalami masalah dalam mengimpor (menerapkan) Storage Gateway di Microsoft Hyper-V.	LihatMemecahkan 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 Dukungan.

Memungkinkan Dukungan 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 Dukungan untuk mengakses gateway Anda untuk membantu Anda mengatasi masalah gateway. Secara default, Dukungan akses ke gateway Anda dinonaktifkan. Anda menyediakan akses ini melalui konsol lokal host. Untuk memberikan Dukungan 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 Dukungan akses ke gateway Anda

1. Masuk ke konsol lokal host Anda.
   - VMware ESXi — untuk informasi lebih lanjut, lihatMengakses 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 hal berikut ini:
   - 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 ControlProtocol/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 Dukungan sehingga Dukungan 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 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
Anda mencoba mengimpor gateway dan menerima pesan galat berikut: “Kesalahan server terjadi saat mencoba mengimpor mesin virtual. Impor gagal. Tidak dapat menemukan	Kesalahan ini dapat terjadi karena alasan berikut: • Jika Anda tidak menunjuk ke root dari file sumber gateway yang tidak di-zip. Bagian terakhir dari lokasi yang Anda tentukan di kotak dialog Impor Mesin Virtual seharusnya`AWS-Storage-Gateway` . Sebagai contoh: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` .

Isu	Tindakan yang Harus Dilakukan
file impor mesin virtual di bawah lokasi [...]. Anda dapat mengimpor mesin virtual hanya jika Anda menggunakan Hyper-V untuk membuat dan mengekspornya.	• 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. Jika Anda berencana membuat beberapa gateway dari satu lokasi file sumber yang tidak di-zip, Anda harus memilih Salin mesin virtual dan centang Duplikat semua file kotak di kotak dialog Impor Mesin Virtual.
Anda mencoba mengimpor gateway dan menerima pesan galat berikut: “Kesalahan server terjadi saat mencoba mengimpor mesin virtual. Impor gagal. Tugas impor gagal menyalin file dari [...]: File ada. (0x80070050)”	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 bawah Server di panel di sisi kiri kotak dialog Pengaturan Hyper-V.

Isu	Tindakan yang Harus Dilakukan
Anda mencoba mengimpor gateway dan menerima pesan galat berikut: “Kesalahan server terjadi saat mencoba mengimpor mesin virtual. 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 Salin mesin virtual dan centang Duplikat semua file kotak di kotak dialog Impor Mesin Virtual untuk membuat ID unik baru untuk VM.
Anda mencoba memulai VM gateway dan menerima pesan galat berikut: “Terjadi kesalahan saat mencoba memulai mesin virtual yang dipilih. Pengaturan prosesor partisi anak tidak kompatibel dengan partisi induk. 'AWS-Stor age-gateway' tidak dapat diinisialisasi. (ID mesin virtual [...])”	Kesalahan ini kemungkinan disebabkan oleh perbedaan CPU antara yang diperlukan CPUs untuk gateway dan yang tersedia CPUs di host. Pastikan jumlah CPU VM didukung oleh hypervisor yang mendasarinya. Untuk informasi selengkapnya tentang persyaratan Storage Gateway, lihatPersyaratan untuk mengatur Volume Gateway.

Isu	Tindakan yang Harus Dilakukan
Anda mencoba memulai VM gateway dan menerima pesan galat berikut: “Terjadi kesalahan saat mencoba memulai mesin virtual yang dipilih. 'AWS-Storage-gateway' tidak dapat diinisialisasi. (ID mesin virtual [...]) Gagal membuat partisi: Sumber daya sistem tidak mencukupi untuk menyelesaikan layanan yang diminta. (0x800705 AA)”	Kesalahan ini kemungkinan disebabkan oleh perbedaan RAM antara RAM yang diperlukan untuk gateway dan RAM yang tersedia di host. Untuk informasi selengkapnya tentang persyaratan Storage Gateway, lihatPersyaratan untuk mengatur Volume Gateway.
Snapshot dan pembaruan perangkat lunak gateway Anda terjadi pada waktu yang sedikit berbeda dari yang diharapkan.	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 Sinkronkan waktu VM dengan waktu host Hyper-V atau Linux KVM.
Anda harus meletakkan file Microsoft Hyper-V Storage Gateway yang tidak di-zip pada sistem file host.	Akses host saat Anda melakukan server Microsoft Windows biasa. Misalnya, jika host hypervisor adalah nama`hyperv-server` , maka Anda dapat menggunakan jalur UNC berikut`\\hyperv-server\c$` , yang mengasumsikan bahwa nama tersebut `hyperv-server` dapat diselesaikan atau didefinisikan dalam file host lokal Anda.
Anda diminta untuk kredensyal saat menghubungkan ke hypervisor.	Tambahkan kredensi pengguna Anda sebagai administrator lokal untuk host hypervisor dengan menggunakan alat sconfig.cmd.

Isu	Tindakan yang Harus Dilakukan
Anda mungkin melihat kinerja jaringan yang buruk jika Anda mengaktifkan antrian mesin virtual (VMQ) untuk host Hyper-V yang menggunakan adaptor jaringan Broadcom.	Untuk informasi tentang solusinya, lihat dokumentasi Microsoft, lihat Kinerja jaringan yang buruk pada mesin virtual pada host Windows Server 2012 Hyper-V jika VMQ diaktifkan.

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 EC2 instans Amazon yang disesuaikan untuk Volume Gateway

Topik

Aktivasi gateway Anda tidak terjadi setelah beberapa saat

Periksa yang berikut ini di EC2 konsol Amazon:

- 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 EC2 Pengguna Amazon.
- Instance gateway ditandai sebagai berjalan. Di EC2 konsol Amazon, nilai Status untuk instance harus RUNNING.
- Pastikan jenis EC2 instans Amazon Anda memenuhi persyaratan minimum, seperti yang dijelaskan dalamPersyaratan penyimpanan.

Setelah memperbaiki masalah, coba aktifkan gateway lagi. Untuk melakukan ini, buka konsol Storage Gateway, pilih Deploy Gateway baru di Amazon EC2, dan masukkan kembali alamat IP instance.

Anda tidak dapat menemukan instance EC2 gateway Anda dalam 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**`aws-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 instance EC2 gateway

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 tidak dapat melampirkan inisiator ke target volume gateway Anda EC2

Periksa apakah grup keamanan tempat Anda meluncurkan instance menyertakan aturan yang memungkinkan port yang Anda gunakan untuk akses iSCSI. Port biasanya ditetapkan sebagai 3260. Untuk informasi selengkapnya tentang menghubungkan ke volume, lihatMenghubungkan ke volume Anda dari klien Windows.

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 EC2 instans Amazon yang disesuaikan untuk Volume 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-langkah di Menentukan ukuran buffer unggahan yang akan dialokasikan.

Throughput ke atau dari EC2 gateway 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 Gateway Anda dan AWS.

Anda ingin Dukungan membantu memecahkan masalah gateway Anda EC2

Storage Gateway menyediakan konsol lokal yang dapat Anda gunakan untuk melakukan beberapa tugas pemeliharaan, termasuk mengaktifkan Dukungan untuk mengakses gateway Anda untuk membantu Anda mengatasi masalah gateway. Secara default, Dukungan akses ke gateway Anda

dinonaktifkan. Anda menyediakan akses ini melalui konsol EC2 lokal Amazon. Anda masuk ke konsol EC2 lokal Amazon 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 EC2 keamanan Amazon di Panduan EC2 Pengguna Amazon.

Agar Dukungan terhubung ke gateway, pertama-tama Anda masuk ke konsol lokal untuk EC2 instans Amazon, navigasikan ke konsol Storage Gateway, lalu berikan akses.

Untuk mengaktifkan Dukungan akses ke gateway yang digunakan pada instans Amazon EC2

1. Masuk ke konsol lokal untuk EC2 instans Amazon Anda. Untuk instruksi, buka Connect to your instance di Panduan EC2 Pengguna Amazon.

   Anda dapat menggunakan perintah berikut untuk masuk ke konsol lokal EC2 instans.

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

   > **Note**
   >
   > *PRIVATE-KEY*Ini adalah `.pem` file yang berisi sertifikat pribadi dari EC2 key pair yang Anda gunakan untuk meluncurkan EC2 instance Amazon. Untuk informasi selengkapnya, lihat Mengambil kunci publik untuk key pair Anda di Panduan EC2 Pengguna Amazon.
   > *INSTANCE-PUBLIC-DNS-NAME*Ini adalah nama Sistem Nama Domain publik (DNS) dari EC2 instans Amazon Anda tempat gateway Anda berjalan. Anda mendapatkan nama DNS publik ini dengan memilih EC2 instans Amazon di EC2 konsol dan mengklik tab Deskripsi.

2. Pada prompt, masuk **`6 - Command Prompt`** untuk membuka konsol Dukungan Saluran.
3. Masukkan **h** Untuk membuka kotak dialog PERINTAH YANG TERSEDIA Jendela.
4. Lakukan salah satu hal berikut ini:

- 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 ControlProtocol/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 Dukungan sehingga Dukungan dapat memberikan bantuan pemecahan masalah.
6. Ketika sesi dukungan selesai, masukkan **`q`** untuk mengakhirinya. Jangan menutup sesi sampai Dukungan 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 instance gateway Anda menggunakan konsol EC2 serial Amazon

Anda dapat menggunakan konsol EC2 serial Amazon untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya. Untuk petunjuk dan tips pemecahan masalah, lihat Amazon EC2 Serial Console 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 i Siklus Daya DRAC9 Virtual: Siklus daya jarak jauh PowerEdge Server EMC Dell di situs web Dell Technologies. InfoHub

Di mana Anda mendapatkan dukungan Dell IDrac?

PowerEdge Server Dell 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 kredensil IDRac, lihat PowerEdge Dell - Apa kredensi 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

Anda dapat menemukan nomor seri untuk Storage Gateway Hardware Appliance menggunakan konsol Storage Gateway.

Untuk menemukan nomor seri alat perangkat keras:

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Hardware dari menu navigasi di sisi kiri halaman.
3. Pilih alat perangkat keras Anda dari daftar.
4. Temukan bidang Nomor Seri pada tab Detail untuk alat Anda.

Di mana mendapatkan dukungan alat perangkat keras

Untuk menghubungi AWS tentang dukungan teknis untuk peralatan perangkat keras Anda, lihat Dukungan.

Dukungan 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 di bagian bawah halaman utama konsol perangkat keras, lalu tekan`Enter`.

   Nomor port yang ditetapkan akan muncul dalam 30 detik jika tidak ada konektivitas jaringan atau masalah firewall. Sebagai contoh:

   Status: Buka di port 19599
3. Perhatikan nomor port dan berikan ke Dukungan.

Memecahkan masalah volume

Anda dapat menemukan informasi tentang masalah paling umum yang mungkin Anda temui saat bekerja dengan volume, dan tindakan yang kami sarankan agar Anda ambil untuk memperbaikinya.

Topik

Konsol Mengatakan bahwa Volume Anda Tidak Dikonfigurasi

Jika konsol Storage Gateway menunjukkan bahwa volume Anda memiliki status UPLOAD BUFFER TIDAK DIKONFIGURASI, tambahkan kapasitas buffer upload ke gateway Anda. Anda tidak dapat menggunakan gateway untuk menyimpan data aplikasi Anda jika buffer unggahan untuk gateway tidak dikonfigurasi. Untuk informasi selengkapnya, lihat Untuk mengonfigurasi buffer unggahan tambahan atau penyimpanan cache untuk gateway Anda.

Konsol Mengatakan Bahwa Volume Anda Tidak Dapat Dipulihkan

Untuk volume tersimpan, jika konsol Storage Gateway menunjukkan bahwa volume Anda memiliki status IRRECOVERABLE, Anda tidak dapat lagi menggunakan volume ini. Anda dapat mencoba menghapus volume di konsol Storage Gateway. Jika ada data pada volume, maka Anda dapat memulihkan data saat Anda membuat volume baru berdasarkan disk lokal VM yang awalnya

digunakan untuk membuat volume. Saat Anda membuat volume baru, pilih Pertahankan data yang ada. Pastikan untuk menghapus snapshot volume yang tertunda sebelum menghapus volume. Untuk informasi selengkapnya, lihat Menghapus snapshot dari volume penyimpanan Anda. Jika menghapus volume di konsol Storage Gateway tidak berfungsi, maka disk yang dialokasikan untuk volume mungkin telah dihapus secara tidak benar dari VM dan tidak dapat dihapus dari alat.

Untuk volume cache, jika konsol Storage Gateway menunjukkan bahwa volume Anda memiliki status IRRECOVERABLE, Anda tidak dapat lagi menggunakan volume ini. Jika ada data pada volume, Anda dapat membuat snapshot volume dan kemudian memulihkan data Anda dari snapshot atau Anda dapat mengkloning volume dari titik pemulihan terakhir. Anda dapat menghapus volume setelah memulihkan data Anda. Untuk informasi selengkapnya, lihat Gateway Cached Anda Tidak Dapat Dijangkau Dan Anda Ingin Memulihkan Data Anda.

Untuk volume yang disimpan, Anda dapat membuat volume baru dari disk yang digunakan untuk membuat volume yang tidak dapat dipulihkan. Untuk informasi selengkapnya, lihat Membuat volume penyimpanan. Untuk informasi tentang status volume, lihatMemahami Status Volume dan Transisi.

Gateway Cached Anda Tidak Dapat Dijangkau Dan Anda Ingin Memulihkan Data Anda

Ketika gateway Anda menjadi tidak dapat dijangkau (seperti saat Anda mematikannya), Anda memiliki opsi untuk membuat snapshot dari titik pemulihan volume dan menggunakan snapshot itu, atau mengkloning volume baru dari titik pemulihan terakhir untuk volume yang ada. Kloning dari titik pemulihan volume lebih cepat dan lebih hemat biaya daripada membuat snapshot. Untuk informasi lebih lanjut tentang kloning volume, lihatMengkloning volume yang di-cache dari titik pemulihan.

Storage Gateway menyediakan titik pemulihan untuk setiap volume dalam arsitektur Volume Gateway yang di-cache. Titik pemulihan volume adalah titik waktu di mana semua data volume konsisten dan dari mana Anda dapat membuat snapshot atau mengkloning volume.

Konsol Mengatakan Bahwa Volume Anda Telah Melewati Status

Dalam beberapa kasus, konsol Storage Gateway mungkin menunjukkan bahwa volume Anda memiliki status PASSTHOUGH. Volume dapat memiliki status PASSTHOUGH karena beberapa alasan. Beberapa alasan memerlukan tindakan, dan beberapa tidak.

Contoh kapan Anda harus mengambil tindakan jika volume Anda memiliki status PASS THROUGH adalah ketika gateway Anda kehabisan ruang buffer unggah. Untuk memverifikasi apakah buffer

unggahan Anda telah terlampaui sebelumnya, Anda dapat melihat `UploadBufferPercentUsed` metrik di CloudWatch konsol Amazon; untuk informasi selengkapnya, lihat. Memantau buffer unggahan Jika gateway Anda memiliki status PASS THROUGH karena telah kehabisan ruang buffer upload, Anda harus mengalokasikan lebih banyak ruang buffer upload ke gateway Anda. Menambahkan lebih banyak ruang buffer akan menyebabkan volume Anda bertransisi dari PASS THROUGH ke BOOTSTRAPPING ke AVAILABLE secara otomatis. Meskipun volume memiliki status BOOTSTRAPPING, gateway membaca data dari disk volume, mengunggah data ini ke Amazon S3, dan mengejar sesuai kebutuhan. Ketika gateway telah menangkap dan menyimpan data volume ke Amazon S3, status volume menjadi TERSEDIA dan snapshot dapat dimulai lagi. Perhatikan bahwa ketika volume Anda memiliki status PASS THROUGH atau BOOTSTRAPPING, Anda dapat terus membaca dan menulis data dari disk volume. Untuk informasi selengkapnya tentang menambahkan lebih banyak ruang buffer upload, lihatMenentukan ukuran buffer unggahan yang akan dialokasikan.

Untuk mengambil tindakan sebelum buffer unggahan terlampaui, Anda dapat menyetel alarm ambang batas pada buffer unggahan gateway. Untuk informasi selengkapnya, lihat Untuk menyetel alarm ambang batas atas untuk buffer unggahan gateway.

Sebaliknya, contoh tidak perlu mengambil tindakan ketika volume memiliki status PASS THROUGH adalah ketika volume menunggu untuk di-bootstrap karena volume lain saat ini sedang di-bootstrap. Bootstrap gateway bervolume satu per satu.

Jarang, status PASS THROUGH dapat menunjukkan bahwa disk yang dialokasikan untuk buffer unggahan telah gagal. Dalam hal ini, Anda harus menghapus disk. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya penyimpanan Volume Gateway. Untuk informasi tentang status volume, lihatMemahami Status Volume dan Transisi.

Anda Ingin Memverifikasi Integritas Volume dan Memperbaiki Kemungkinan Kesalahan

Jika Anda ingin memverifikasi integritas volume dan memperbaiki kemungkinan kesalahan, dan gateway Anda menggunakan inisiator Microsoft Windows untuk terhubung ke volumenya, Anda dapat menggunakan utilitas Windows CHKDSK untuk memverifikasi integritas volume Anda dan memperbaiki kesalahan apa pun pada volume. Windows dapat secara otomatis menjalankan alat CHKDSK ketika kerusakan volume terdeteksi, atau Anda dapat menjalankannya sendiri.

Target iSCSI Volume Anda Tidak Muncul di Konsol Manajemen Disk Windows

Jika target iSCSI volume Anda tidak muncul di Konsol Manajemen Disk di Windows, periksa apakah Anda telah mengonfigurasi buffer unggahan untuk gateway. Untuk informasi selengkapnya, lihat Untuk mengonfigurasi buffer unggahan tambahan atau penyimpanan cache untuk gateway Anda.

Anda Ingin Mengubah Nama Target iSCSI Volume Anda

Jika Anda ingin mengubah nama target iSCSI volume Anda, Anda harus menghapus volume dan menambahkannya lagi dengan nama target baru. Jika Anda melakukannya, Anda dapat menyimpan data pada volume.

Snapshot Volume Terjadwal Anda Tidak Terjadi

Jika snapshot volume yang dijadwalkan tidak muncul, periksa apakah volume Anda memiliki status PASSTHOUGH, atau apakah buffer upload gateway telah diisi sesaat sebelum waktu snapshot yang dijadwalkan. Anda dapat memeriksa `UploadBufferPercentUsed` metrik untuk gateway di CloudWatch konsol Amazon dan membuat alarm untuk metrik ini. Untuk informasi selengkapnya, silakan lihat Memantau buffer unggahan dan Untuk menyetel alarm ambang batas atas untuk buffer unggahan gateway.

Anda Perlu Menghapus atau Mengganti Disk yang Gagal

Jika Anda perlu mengganti disk volume yang gagal atau mengganti volume karena tidak diperlukan, Anda harus menghapus volume terlebih dahulu menggunakan konsol Storage Gateway. Untuk informasi selengkapnya, lihat Untuk menghapus volume. Anda kemudian menggunakan klien hypervisor untuk menghapus penyimpanan dukungan:

- Untuk VMware ESXi, hapus penyimpanan dukungan seperti yang dijelaskan dalamMenghapus volume penyimpanan.
- Untuk Microsoft Hyper-V, hapus penyimpanan dukungan.

Throughput dari Aplikasi Anda ke Volume Telah Turun ke Nol

Jika throughput dari aplikasi Anda ke volume turun menjadi nol, coba yang berikut ini:

- Jika Anda menggunakan klien VMware vSphere, periksa apakah alamat IP Host volume Anda cocok dengan salah satu alamat yang muncul di klien vSphere pada tab Ringkasan. Anda dapat menemukan alamat IP Host untuk volume penyimpanan di konsol Storage Gateway di tab Detail untuk volume. Perbedaan dalam alamat IP dapat terjadi, misalnya, ketika Anda menetapkan alamat IP statis baru ke gateway Anda. Jika ada perbedaan, restart gateway Anda dari konsol Storage Gateway seperti yang ditunjukkan pada. Mematikan VM Gateway Anda Setelah restart, alamat IP Host di tab Info Target ISCSI untuk volume penyimpanan harus cocok dengan alamat IP yang ditunjukkan di klien vSphere pada tab Ringkasan untuk gateway.
- Jika tidak ada alamat IP di kotak IP Host untuk volume dan gateway online. Misalnya, ini bisa terjadi jika Anda membuat volume yang terkait dengan alamat IP adaptor jaringan gateway yang memiliki dua atau lebih adapter jaringan. Saat Anda menghapus atau menonaktifkan adaptor jaringan yang terkait dengan volume, alamat IP mungkin tidak muncul di kotak IP Host. Untuk mengatasi masalah ini, hapus volume dan kemudian buat ulang untuk mempertahankan data yang ada.
- Periksa apakah inisiator iSCSI yang digunakan aplikasi Anda dipetakan dengan benar ke target iSCSI untuk volume penyimpanan. Untuk informasi selengkapnya tentang menghubungkan ke volume penyimpanan, lihatMenghubungkan ke volume Anda dari klien Windows.

Anda dapat melihat throughput untuk volume dan membuat alarm dari konsol Amazon CloudWatch. Untuk informasi selengkapnya tentang mengukur throughput dari aplikasi ke volume, lihatMengukur Kinerja Antara Aplikasi dan Gateway.

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, konfigurasikan 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.

Snapshot Volume Memiliki Status PENDING Lebih Lama Dari yang Diharapkan

Jika snapshot volume tetap dalam status PENDING lebih lama dari yang diharapkan, VM gateway mungkin mengalami crash secara tak terduga atau status volume mungkin telah berubah menjadi PASS THROUGH atau IRRECOVERABLE. Jika salah satu dari ini terjadi, snapshot tetap dalam status PENDING dan snapshot tidak berhasil diselesaikan. Dalam kasus ini, kami sarankan Anda menghapus snapshot. Untuk informasi selengkapnya, lihat Menghapus snapshot dari volume penyimpanan Anda.

Ketika volume kembali ke status AVAILABLE, buat snapshot baru dari volume. Untuk informasi tentang status volume, lihatMemahami Status Volume dan Transisi.

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, lihatMemecahkan 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

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 tanda masalah apa pun. 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 VMware gateway, 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 VMware peristiwa 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 VMware gateway.

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 Dukungan.

Pemberitahuan: AvailabilityMonitorTest

Untuk gateway di VMware vSphere HA, Anda bisa mendapatkan `AvailabilityMonitorTest` pemberitahuan ketika Anda menjalankan pengujian 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 Volume Gateway

Bagian ini berisi topik-topik berikut, yang memberikan informasi tentang praktik terbaik untuk bekerja dengan gateway, disk lokal, snapshot, dan data. Kami menyarankan Anda membiasakan diri dengan informasi yang diuraikan di bagian ini, dan mencoba mengikuti panduan ini untuk menghindari masalah dengan Anda AWS Storage Gateway. Untuk panduan tambahan tentang mendiagnosis dan memecahkan masalah umum yang mungkin Anda temui dengan penerapan Anda, lihat. Pemecahan masalah gateway

Topik

Praktik terbaik: 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 Amazon EC2 Machine Image (AMI) Anda. Jika VM gateway Anda tidak berfungsi, aktifkan gateway baru dan pulihkan data Anda ke gateway itu menggunakan instruksi berikut.

Topik

- Memulihkan data Anda dari sistem file yang rusak
- 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.
- Fungsionalitas ini memastikan bahwa data yang disimpan secara lokal Anda terus disinkronkan. AWS Untuk informasi lebih lanjut tentang status ini, lihat Memahami Status Volume dan Transisi.
- 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 gateway atau mesin virtual Anda tidak berfungsi, Anda dapat memulihkan data yang telah diunggah AWS dan disimpan pada volume di Amazon S3. Untuk gateway volume cache, Anda memulihkan data dari snapshot pemulihan. Untuk gateway volume tersimpan, Anda dapat memulihkan data dari snapshot Amazon EBS terbaru dari volume. Untuk Tape Gateways, Anda memulihkan satu atau lebih kaset dari titik pemulihan ke Tape Gateway baru.

Jika gateway volume cache tidak dapat dijangkau, Anda dapat menggunakan langkah-langkah berikut untuk memulihkan data dari snapshot pemulihan:

1. Di AWS Management Console, pilih gateway yang tidak berfungsi, pilih volume yang ingin Anda pulihkan, lalu buat snapshot pemulihan darinya.
2. Terapkan dan aktifkan Volume Gateway baru. Atau, jika Anda memiliki Volume Gateway yang berfungsi, Anda dapat menggunakan gateway itu untuk memulihkan data volume Anda.
3. Temukan snapshot yang Anda buat dan kembalikan ke volume baru di gateway yang berfungsi.
4. Pasang volume baru sebagai perangkat iSCSI di server aplikasi lokal Anda.

Untuk informasi rinci tentang cara memulihkan data volume cache dari snapshot pemulihan, lihat. Gateway Cached Anda Tidak Dapat Dijangkau Dan Anda Ingin Memulihkan Data Anda

Memulihkan data Anda dari volume yang tidak dapat dipulihkan

Jika status volume Anda IRRECOVERABLE, Anda tidak dapat lagi menggunakan volume ini.

Untuk volume tersimpan, Anda dapat mengambil data dari volume yang tidak dapat dipulihkan ke volume baru dengan menggunakan langkah-langkah berikut:

1. Buat volume baru dari disk yang digunakan untuk membuat volume yang tidak dapat dipulihkan.
2. Pertahankan data yang ada saat Anda membuat volume baru.
3. Hapus semua pekerjaan snapshot yang tertunda untuk volume yang tidak dapat dipulihkan.
4. Hapus volume yang tidak dapat dipulihkan dari gateway.

Untuk volume yang di-cache, sebaiknya gunakan titik pemulihan terakhir untuk mengkloning volume baru.

Untuk informasi terperinci tentang cara mengambil data Anda dari volume yang tidak dapat dipulihkan ke volume baru, lihat. Konsol Mengatakan Bahwa Volume Anda 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.

Memulihkan data Anda dari sistem file yang rusak

Jika sistem file Anda rusak, Anda dapat menggunakan **`fsck`** perintah untuk memeriksa sistem file Anda untuk kesalahan dan memperbaikinya. Jika Anda dapat memperbaiki sistem file, Anda kemudian dapat memulihkan data Anda dari volume pada sistem file, seperti yang dijelaskan berikut:

1. Matikan mesin virtual Anda dan gunakan Storage Gateway Management Console untuk membuat snapshot pemulihan. Snapshot ini mewakili data terbaru yang disimpan di AWS.

   > **Note**
   >
   > Anda menggunakan snapshot ini sebagai fallback jika sistem file Anda tidak dapat diperbaiki atau proses pembuatan snapshot tidak dapat diselesaikan dengan sukses.

   Untuk informasi tentang cara membuat snapshot pemulihan, lihatGateway Cached Anda Tidak Dapat Dijangkau Dan Anda Ingin Memulihkan Data Anda.

2. Gunakan **`fsck`** perintah untuk memeriksa sistem file Anda untuk kesalahan dan mencoba perbaikan.
3. Mulai ulang VM gateway Anda.
4. Saat host hypervisor Anda mulai boot, tekan dan tahan tombol shift untuk masuk ke menu boot grub.
5. Dari menu, tekan **`e`** untuk mengedit.
6. Pilih baris kernel (baris kedua), lalu tekan **`e`** untuk mengedit.
7. Tambahkan opsi berikut ke baris perintah kernel:**`init=/bin/bash`**. Gunakan spasi untuk memisahkan opsi sebelumnya dari opsi yang baru saja Anda tambahkan.
8. Hapus kedua `console=` baris, pastikan untuk menghapus semua nilai mengikuti = simbol, termasuk yang dipisahkan dengan koma.
9. Tekan **`Return`** untuk menyimpan perubahan.
10. Tekan **`b`** untuk mem-boot komputer Anda dengan opsi kernel yang dimodifikasi. Komputer Anda akan boot ke `bash#` prompt.
11. Masukkan **`/sbin/fsck -f`** ***`/dev/sda1`*** untuk menjalankan perintah ini secara manual dari prompt, untuk memeriksa dan memperbaiki sistem file Anda. Jika perintah tidak bekerja dengan `/dev/sda1` jalur, Anda dapat menggunakan **`lsblk`** untuk menentukan perangkat sistem file root untuk `/` dan menggunakan jalur itu sebagai gantinya.
12. Ketika pemeriksaan dan perbaikan sistem file selesai, reboot instance. Pengaturan grub akan kembali ke nilai asli, dan gateway akan boot secara normal.
13. Tunggu snapshot yang sedang berlangsung dari gateway asli selesai, lalu validasi data snapshot.

Anda dapat terus menggunakan volume asli apa adanya, atau Anda dapat membuat gateway baru dengan volume baru berdasarkan snapshot pemulihan atau snapshot yang sudah selesai. Atau, Anda dapat membuat volume baru dari snapshot Anda yang sudah selesai dari volume ini.

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 di EC2 instans Amazon. Jika Anda tidak memiliki akses ke pusat data lain, sebaiknya buat gateway di EC2 instans Amazon. Langkah-langkah yang Anda ikuti tergantung pada jenis gateway tempat Anda meliput datanya.

Untuk memulihkan data dari Volume Gateway di pusat data yang tidak dapat diakses

1. Buat dan aktifkan Volume Gateway baru di EC2 host Amazon. Untuk informasi selengkapnya, lihat Menerapkan EC2 instans Amazon yang disesuaikan untuk Volume Gateway.

   > **Note**
   >
   > Volume tersimpan gateway tidak dapat dihosting di EC2 instans Amazon.

2. Buat volume baru dan pilih EC2 gateway sebagai gateway target. Untuk informasi selengkapnya, lihat Membuat volume penyimpanan.

   Buat volume baru berdasarkan snapshot Amazon EBS atau kloning dari titik pemulihan terakhir dari volume yang ingin Anda pulihkan.

   Jika volume Anda didasarkan pada snapshot, berikan id snapshot.

   Jika Anda mengkloning volume dari titik pemulihan, pilih volume sumber.

Membersihkan sumber daya yang tidak perlu

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

Untuk membersihkan sumber daya yang tidak Anda butuhkan

1. Hapus snapshot apa pun. Untuk petunjuk, silakan lihat Menghapus snapshot dari volume penyimpanan Anda.

2. Kecuali Anda berencana untuk terus menggunakan gateway, hapuslah. Untuk informasi selengkapnya, lihat Menghapus gateway Anda dan menghapus sumber daya terkait.
3. Hapus VM Storage Gateway dari host lokal Anda. Jika Anda membuat gateway di EC2 instans Amazon, hentikan instance.

Mengurangi jumlah penyimpanan yang ditagih pada volume

Menghapus file dari sistem file Anda tidak selalu menghapus data dari perangkat blok yang mendasarinya atau mengurangi jumlah data yang disimpan pada volume Anda. Jika Anda ingin mengurangi jumlah penyimpanan yang ditagih pada volume Anda, kami sarankan untuk menimpa file Anda dengan nol untuk mengompres penyimpanan ke jumlah penyimpanan aktual yang dapat diabaikan. Storage Gateway mengenakan biaya untuk penggunaan volume berdasarkan penyimpanan terkompresi.

> **Note**
>
> Jika Anda menggunakan alat hapus yang menimpa data pada volume Anda dengan data acak, penggunaan Anda tidak akan berkurang. Ini karena data acak tidak dapat dimampatkan.

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

- Menyebarkan dan mengonfigurasi host VM gateway- Pelajari cara menerapkan dan mengonfigurasi host mesin virtual untuk gateway Anda.
- Bekerja dengan sumber daya penyimpanan Volume Gateway- Pelajari tentang prosedur yang terkait dengan sumber daya penyimpanan Volume Gateway, seperti menghapus disk lokal dan mengelola volume Amazon EBS pada instans Amazon EC2 gateway.
- Mendapatkan kunci aktivasi untuk gateway Anda- Pelajari di mana menemukan kunci aktivasi yang perlu Anda berikan saat Anda menerapkan gateway baru.
- Menghubungkan Inisiator iSCSI- Pelajari cara bekerja dengan volume atau perangkat pustaka pita virtual (VTL) yang diekspos sebagai target Internet Small Computer System Interface (iSCSI).
- Menggunakan AWS Direct Connect dengan Storage Gateway- Pelajari cara membuat koneksi jaringan khusus antara gateway lokal dan AWS cloud.
- Mendapatkan alamat IP untuk alat gateway Anda- Pelajari di mana menemukan alamat IP host mesin virtual gateway, yang perlu Anda berikan saat Anda menggunakan gateway baru.
- Memahami Sumber Daya dan Sumber Daya Storage Gateway IDs- Pelajari cara AWS mengidentifikasi sumber daya dan subresource yang dibuat oleh Storage Gateway.
- Menandai Sumber Daya Storage Gateway- Pelajari cara menggunakan tag metadata untuk mengkategorikan sumber daya Anda dan membuatnya lebih mudah dikelola.
- Bekerja dengan komponen open-source untuk Storage Gateway- Pelajari tentang alat dan lisensi pihak ketiga yang digunakan untuk memberikan fungsionalitas Storage Gateway.
- AWS Storage Gateway kuota- Pelajari tentang batas dan kuota untuk Volume Gateway, termasuk batasan maksimum untuk ukuran dan kuantitas volume, dan rekomendasi ukuran disk lokal.

Menyebarkan dan mengonfigurasi host VM gateway

Topik di bagian ini menjelaskan cara menyiapkan dan mengelola host mesin virtual untuk alat Storage Gateway Anda, termasuk peralatan lokal yang berjalan di, Hyper-V VMware, atau Linux KVM, dan peralatan yang berjalan di instans Amazon EC2 di cloud. AWS

Topik

- Menerapkan EC2 host Amazon default untuk Volume Gateway- Pelajari cara menerapkan dan mengaktifkan pada instans Amazon Elastic Compute Cloud EC2 (Amazon) menggunakan spesifikasi default.
- Menerapkan EC2 instans Amazon yang disesuaikan untuk Volume Gateway- Pelajari cara menerapkan dan mengaktifkan pada instans Amazon Elastic Compute Cloud EC2 (Amazon) menggunakan pengaturan yang disesuaikan.
- Ubah opsi EC2 metadata instans Amazon- Pelajari cara mengonfigurasi instans EC2 gateway Amazon Anda untuk menerima permintaan metadata masuk yang menggunakan IMDS Versi 1 (IMDSv1) atau mengharuskan semua permintaan metadata menggunakan IMDS Versi 2 (). IMDSv2
- Sinkronkan waktu VM dengan waktu host Hyper-V atau Linux KVM- Pelajari cara melihat dan menyinkronkan waktu mesin virtual gateway Hyper-V atau Linux KVM lokal ke server Network Time Protocol (NTP).
- Sinkronisasi waktu VM dengan waktu host VMware- Pelajari tentang cara memeriksa waktu host untuk mesin virtual VMware gateway dan, jika perlu, atur waktu dan konfigurasikan host untuk menyinkronkan waktunya secara otomatis ke server Network Time Protocol (NTP).
- Mengkonfigurasi paravirtualisasi pada host VMware - Pelajari tentang bagaimana Anda dapat mengonfigurasi platform VMware host untuk alat Storage Gateway Anda untuk menggunakan pengontrol Internet Small Computer System Interface Protocol (iSCSI) paravirtual.
- Mengkonfigurasi adapter jaringan untuk gateway Anda- Pelajari tentang bagaimana Anda dapat mengkonfigurasi ulang gateway Anda untuk menggunakan adaptor jaringan VMXNET3 (10 GbE), atau menggunakan lebih dari satu adaptor jaringan sehingga dapat diakses dari alamat IP nultiple.
- Menggunakan VMware VSphere Ketersediaan Tinggi dengan Storage Gateway- Pelajari tentang cara melindungi beban kerja penyimpanan Anda terhadap kegagalan perangkat keras, hypervisor, atau jaringan dengan mengonfigurasi Storage Gateway untuk bekerja dengan VMware vSphere High Availability.

Menerapkan EC2 host Amazon default untuk Volume Gateway

Topik ini mencantumkan langkah-langkah untuk menerapkan EC2 host Amazon menggunakan spesifikasi default.

Anda dapat menerapkan dan mengaktifkan di instans Amazon Elastic Compute Cloud EC2 (Amazon). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai AMI komunitas.

> **Note**
>
> Komunitas AMIs Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.

1. Untuk mengatur Amazon EC2instance, pilih Amazon EC2 sebagai platform Host di bagian Opsi platform pada alur kerja. Untuk petunjuk cara mengonfigurasi EC2 instans Amazon, lihat Amazon untuk meng-host Gateway Volume Anda.
2. Pilih Launch instance untuk membuka template AWS Storage Gateway AMI di EC2 konsol Amazon 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 EC2 instance Amazon dengan konfigurasi default.

   EC2 Instans Amazon 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 EC2 instans Anda.
     - Untuk Subnet, tentukan subnet tempat EC2 instance Anda harus diluncurkan.

       > **Note**
       >
       > Subnet VPC akan muncul di drop-down hanya jika mereka mengaktifkan pengaturan IPv4 alamat publik penetapan otomatis dari konsol manajemen VPC.

     - Tetapkan IP Publik secara otomatis - Diaktifkan

   Grup EC2 keamanan dibuat dan dikaitkan dengan EC2 instance. Grup keamanan memiliki aturan port masuk berikut:

   > **Note**
   >
   > Anda akan membutuhkan Port 80 terbuka selama aktivasi gateway. Port ditutup segera setelah aktivasi. Setelah itu, EC2 instance 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 EC2 instans Amazon, 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				

- Konfigurasikan penyimpanan

Pengaturan Default	Volume Akar AMI	Volume 2 Cache	Volume 3 Cache			
Nama perangkat		'/dev/sdb'	'/dev/sdc'			
Size	80 Gib	165 GiB	150 GiB			
Jenis Volume	gp3	gp3	gp3			
IOPS	3000	3000	3000			

Pengaturan Default	Volume Akar AMI	Volume 2 Cache	Volume 3 Cache			
Hapus saat penghentian	Ya	Ya	Ya			
Dienkripsi	Tidak	Tidak	Tidak			
Throughput	125	125	125			

Menerapkan EC2 instans Amazon yang disesuaikan untuk Volume Gateway

Anda dapat menerapkan dan mengaktifkan di instans Amazon Elastic Compute Cloud EC2 (Amazon). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai komunitas AMI.

> **Note**
>
> Komunitas AMIs Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.
> Volume Gateway AMIs menggunakan konvensi penamaan berikut. Nomor versi yang ditambahkan ke nama AMI berubah dengan setiap rilis versi.
> `aws-storage-gateway-CLASSIC-2.9.0`

Untuk menerapkan EC2 instans Amazon untuk meng-host Volume Gateway Anda

1. Mulai menyiapkan gateway baru menggunakan konsol Storage Gateway. Untuk petunjuk, lihat Volume. Saat Anda mencapai bagian Opsi platform, pilih Amazon EC2 sebagai platform Host, lalu gunakan langkah-langkah berikut untuk meluncurkan EC2 instans Amazon yang akan meng-host Anda.

> **Note**
>
> Platform EC2 host Amazon hanya mendukung volume yang di-cache. Gateway volume tersimpan tidak dapat digunakan pada instance. EC2

2. Pilih Launch instance untuk membuka template AWS Storage Gateway AMI di EC2 konsol Amazon, tempat Anda dapat mengonfigurasi pengaturan tambahan.

   Gunakan Quicklaunch untuk meluncurkan EC2 instans Amazon dengan pengaturan default. Untuk informasi selengkapnya tentang sepsifikasi default Amazon EC2 Quicklaunch, lihat untuk Amazon. EC2 Spesifikasi Konfigurasi Quicklaunch untuk Amazon EC2.

3. Untuk Nama, masukkan nama untuk EC2 instance Amazon. Setelah instance diterapkan, Anda dapat mencari nama ini untuk menemukan instance Anda di halaman daftar di EC2 konsol Amazon.

4. Di bagian Jenis instans, untuk tipe Instance, pilih konfigurasi perangkat keras untuk instance 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 EC2 instans Amazon.

   Anda dapat mengubah ukuran instance Anda setelah meluncurkan, jika perlu. Untuk informasi selengkapnya, lihat Mengubah ukuran instans Anda di Panduan EC2 Pengguna Amazon.

   > **Note**
   >
   > Jenis instans tertentu, terutama i3 EC2, menggunakan NVMe disk SSD. Ini dapat menyebabkan masalah ketika Anda memulai atau menghentikan Volume Gateway; misalnya, Anda dapat kehilangan data dari cache. Pantau CloudWatch metrik `CachePercentDirty` Amazon, dan hanya mulai atau hentikan sistem Anda saat parameter itu`0`. 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 Anda. EC2 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 EC2 instans Amazon 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 instance Anda. Untuk informasi selengkapnya tentang port yang diperlukan untuk Volume Gateway, lihat port. Untuk informasi selengkapnya tentang menambahkan aturan firewall, lihat Aturan grup keamanan di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

   > **Note**
   >
   > Volume Gateway membutuhkan port TCP 80 agar 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, sebaiknya alokasikan

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 Launch instance untuk meluncurkan instans EC2 gateway Amazon baru Anda dengan pengaturan yang dikonfigurasi.
13. Untuk memverifikasi bahwa instans baru berhasil diluncurkan, buka halaman Instans di EC2 konsol Amazon dan cari instance 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 IPv4alamat Publik dari bagian ringkasan Instance, lalu kembali ke halaman Pengaturan gateway di konsol Storage Gateway untuk melanjutkan pengaturan Anda.

Anda dapat menentukan ID AMI yang akan digunakan untuk meluncurkan 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 Volume. Saat Anda mencapai bagian Opsi platform, pilih Amazon EC2 sebagai platform Host, lalu pilih Launch instance untuk membuka template AWS Storage Gateway AMI di EC2 konsol Amazon.

  Anda diarahkan ke halaman AMI EC2 komunitas, 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/CACHED/latest` untuk Cached Volume Gateways atau `/aws/service/storagegateway/ami/STORED/latest` untuk Stored Volume Gateways. 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/
STORED/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/
STORED/latest",
        "Name": "/aws/service/storagegateway/ami/STORED/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Ubah opsi EC2 metadata instans Amazon

Layanan metadata instance (IMDS) adalah komponen on-instance yang menyediakan akses aman ke metadata instans Amazon. EC2 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 selengkapnya IMDSv2, lihat Cara Kerja Layanan Metadata Instans Versi 2 di Panduan Pengguna Amazon Elastic Compute Cloud.

Sebaiknya Anda mewajibkan IMDSv2 semua EC2 instans Amazon yang meng-host Storage Gateway. IMDSv2 diperlukan secara default pada semua instance gateway yang baru diluncurkan. Jika Anda memiliki instans yang masih dikonfigurasi untuk menerima permintaan IMDSv1 metadata, lihat Memerlukan penggunaan IMDSv2 dalam Panduan Pengguna Amazon Elastic Compute Cloud untuk petunjuk mengubah opsi metadata instans Anda agar memerlukan penggunaan. IMDSv2 Menerapkan perubahan ini tidak memerlukan reboot instance.

Sinkronkan waktu VM dengan waktu host Hyper-V atau Linux KVM

Untuk gateway yang digunakan VMware ESXi, mengatur waktu host hypervisor dan menyinkronkan waktu mesin virtual ke host sudah cukup untuk menghindari penyimpangan waktu. Untuk informasi selengkapnya, lihat Sinkronisasi waktu VM dengan waktu host VMware. Untuk gateway yang digunakan di Microsoft Hyper-V atau Linux KVM, kami sarankan Anda memeriksa waktu mesin virtual secara berkala menggunakan prosedur yang dijelaskan berikut.

Untuk melihat dan menyinkronkan waktu mesin virtual gateway hypervisor ke server Network Time Protocol (NTP)

1. Masuk ke konsol lokal gateway Anda:

   - 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 Virtual Machine (KVM), lihat. Mengakses Konsol Lokal Gateway dengan Linux KVM
2. Pada layar menu utama Storage Gateway Configuration, masukkan angka yang sesuai untuk memilih System Time Management.
3. Pada Manajemen Waktu Sistem layar menu, masukkan angka yang sesuai untuk memilih Lihat dan Sinkronisasi Waktu Sistem.

   Konsol lokal gateway menampilkan waktu sistem saat ini dan membandingkannya dengan waktu yang dilaporkan oleh server NTP, kemudian melaporkan perbedaan yang tepat antara dua kali dalam detik.
4. Jika perbedaan waktu lebih besar dari 60 detik, masukkan **y** untuk menyinkronkan waktu sistem dengan waktu NTP. Jika tidak, masukkan**n**.

   Sinkronisasi waktu mungkin memakan waktu beberapa saat.

Sinkronisasi waktu VM dengan waktu host VMware

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. Konfigurasikan waktu VM Anda.

a. Di klien vSphere, klik kanan pada nama gateway VM Anda di panel di sisi kiri jendela aplikasi untuk membuka menu konteks untuk VM, dan kemudian pilih Edit Pengaturan.

   Kotak dialog Virtual Machine Properties terbuka.

b. Pilih tab Opsi, lalu pilih VMware Alat dari daftar opsi.

c. Centang Sinkronisasi waktu tamu dengan host pilihan di Advanced bagian di sisi kanan kotak dialog Virtual Machine Properties, lalu pilih OK.

   VM menyinkronkan waktunya dengan host.

2. Konfigurasikan 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 bawah Tanggal dan Waktu, atur tanggal dan waktu untuk host vSphere Anda.

   d. Konfigurasikan 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` nama domain.

      iv. Dalam kotak dialog Opsi Daemon NTP (ntpd), pilih Umum di panel kiri.

      v. Di bawah 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 paravirtualisasi pada host VMware

Prosedur berikut menjelaskan cara mengkonfigurasi platform VMware host untuk alat Storage Gateway Anda untuk menggunakan pengontrol Internet Small Computer System Interface Protocol (iSCSI) paravirtual. Pengontrol iSCSI paravirtual adalah pengontrol penyimpanan kinerja tinggi yang dapat menghasilkan throughput yang lebih besar dan penggunaan CPU yang lebih rendah. Pengontrol ini paling cocok untuk lingkungan penyimpanan berkinerja tinggi. Saat Anda mengonfigurasi pengontrol iSCSI dengan cara ini, mesin virtual Storage Gateway bekerja dengan sistem operasi host untuk memungkinkan konsol gateway mengidentifikasi disk virtual yang Anda tambahkan ke mesin virtual Anda.

> **Note**
>
> Anda harus menyelesaikan langkah ini untuk menghindari masalah dalam mengidentifikasi disk ini saat Anda mengonfigurasinya di konsol gateway.

Untuk mengonfigurasi platform VMware host Anda agar menggunakan pengontrol paravirtualisasi

1. Di klien VMware vSphere, klik kanan pada nama mesin virtual gateway Anda di panel navigasi di sisi kiri jendela aplikasi untuk membuka menu konteks, lalu pilih Edit Pengaturan.
2. Di kotak dialog Virtual Machine Properties, pilih tab Hardware.
3. Pada tab Hardware, pilih SCSI controller 0, dan kemudian pilih Change Type.
4. Dalam kotak dialog Change SCSI Controller Type, pilih tipe pengontrol SCSI VMware Paravirtual, lalu pilih OK untuk menyimpan konfigurasi.

Mengkonfigurasi adapter 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 VMXNET3 Jaringan

- Mengkonfigurasi Gateway Anda untuk Beberapa NICs

Mengkonfigurasi Gateway Anda untuk Menggunakan Adaptor VMXNET3 Jaringan

Storage Gateway mendukung jenis adaptor jaringan E1000 di keduanya VMware ESXi dan host hypervisor Microsoft Hyper-V. Namun, jenis adaptor jaringan VMXNET3 (10 GbE) hanya didukung di VMware ESXi hypervisor. Jika gateway Anda di-host di VMware ESXi hypervisor, Anda dapat mengonfigurasi ulang gateway Anda untuk menggunakan jenis adaptor (VMXNET3 10 GbE). Untuk informasi selengkapnya tentang adaptor ini, lihat Memilih adaptor jaringan untuk mesin virtual Anda di situs web Broadcom (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 VMXNET3 adaptor:

1. Hapus adaptor E1000 default.
2. Tambahkan VMXNET3 adaptor.
3. Mulai ulang gateway Anda.
4. Konfigurasikan 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 VMXNET3 adaptor.
4. Pilih adaptor jaringan E1000, lalu pilih Hapus. Dalam contoh ini, adaptor jaringan E1000 adalah Adaptor jaringan 1.

> **Note**
>
> Meskipun Anda dapat menjalankan E1000 dan adaptor VMXNET3 jaringan di gateway Anda pada saat yang sama, 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 VMXNET3, lalu pilih OK.
9. Di VMware VSphere klien, matikan gateway Anda.
10. Di VMware VSphere klien, restart gateway Anda.

Setelah gateway Anda restart, konfigurasikan ulang adaptor yang baru saja Anda tambahkan untuk memastikan konektivitas jaringan ke internet terjalin.

Untuk mengkonfigurasi adaptor untuk jaringan

1. Di VSphere klien, pilih tab Konsol untuk memulai konsol lokal. Gunakan kredenal login default untuk masuk ke konsol lokal gateway untuk tugas konfigurasi ini. Untuk selengkapnya tentang cara masuk menggunakan kredensial default, lihat .
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 NICs

Jika Anda mengkonfigurasi gateway Anda untuk menggunakan beberapa adapter jaringan (NICs), 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 yang digunakan 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 dimaksud 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 beberapa adapter jaringan pada host VMware ESXi
- Mengkonfigurasi beberapa adaptor jaringan pada host Microsoft Hyper-V

Mengkonfigurasi beberapa adapter jaringan pada host VMware ESXi

Prosedur berikut mengasumsikan bahwa VM gateway Anda sudah memiliki satu adaptor jaringan yang ditentukan, dan menjelaskan cara menambahkan adaptor. VMware ESXi

Untuk mengkonfigurasi gateway Anda untuk menggunakan adaptor jaringan tambahan di VMware ESXi host

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 VMXNET3 jaringan dengan Storage Gateway. Untuk informasi selengkapnya tentang jenis adaptor yang mungkin muncul di daftar adaptor, lihat Jenis Adaptor Jaringan di Dokumentasi Server vCenter 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 beberapa adaptor jaringan pada host Microsoft Hyper-V

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.
2. Di Microsoft Hyper-V Manager, pilih VM gateway Anda dari panel Mesin Virtual.
3. Jika VM gateway belum dimatikan, klik kanan nama VM untuk membuka menu konteks, lalu pilih Matikan.
4. Klik kanan nama VM gateway untuk membuka menu konteks, lalu pilih Pengaturan.
5. Di kotak dialog Settings, di bawah Hardware, pilih Add Hardware.
6. Di panel Add Hardware di sisi kanan kotak dialog Pengaturan, pilih Adaptor Jaringan, lalu pilih Tambah untuk menambahkan perangkat.
7. Konfigurasikan adaptor jaringan, lalu pilih Terapkan untuk menerapkan pengaturan.
8. Di kotak dialog Pengaturan, di bawah Perangkat Keras, konfirmasikan bahwa adaptor jaringan baru ditambahkan ke daftar perangkat keras, lalu pilih OK.
9. Nyalakan gateway menggunakan konsol Storage Gateway.
10. Di panel Navigasi konsol Storage Gateway, pilih Gateways, lalu 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

Menggunakan VMware VSphere Ketersediaan Tinggi dengan Storage Gateway

Storage Gateway menyediakan ketersediaan tinggi VMware melalui serangkaian pemeriksaan kesehatan tingkat aplikasi yang terintegrasi dengan VMware vSphere High Availability (HA). VMware 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 menggunakan Storage Gateway dengan VMware HA, sebaiknya lakukan hal-hal berikut:
>
> - Menerapkan paket `.ova` download VMware ESX yang berisi Storage Gateway VM 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.

Topik berikut menjelaskan cara menerapkan Storage Gateway di klaster VMware HA:

Topik

Konfigurasikan Cluster HA vSphere VMware Anda

Pertama, jika Anda belum membuat VMware cluster, buat satu. Untuk informasi tentang cara membuat VMware klaster, lihat Membuat Cluster HA vSphere di VMware dokumentasi.

Selanjutnya, konfigurasikan VMware cluster Anda untuk bekerja dengan Storage Gateway.

Untuk mengonfigurasi VMware klaster Anda

1. Pada halaman Edit Pengaturan Cluster di VMware vSphere, pastikan bahwa pemantauan VM dikonfigurasi untuk pemantauan VM dan aplikasi. Untuk melakukannya, atur nilai berikut untuk setiap opsi:
   - Respon Kegagalan Host: Mulai Ulang VMs
   - Respons untuk Isolasi Host: Matikan dan mulai ulang VMs
   - Datastore dengan PDL: Dinonaktifkan
   - Datastore dengan APD: Dinonaktifkan
   - Pemantauan VM: VM dan Pemantauan Aplikasi
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 yang lain yang VMs 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 menyetel nilai-nilai ini, lihat(Opsional) Tambahkan Opsi Override untuk Lainnya VMs 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 Volume.

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 Change SCSI Controller Type, pilih tipe pengontrol SCSI VMware Paravirtual, lalu pilih OK.

(Opsional) Tambahkan Opsi Override untuk Lainnya VMs di Cluster Anda

Jika Anda memiliki yang lain yang VMs berjalan di cluster Anda, Anda mungkin ingin mengatur nilai cluster secara khusus untuk setiap VM. Untuk petunjuk, lihat Menyesuaikan Mesin Virtual Individu di dokumentasi online VMware vSphere.

Untuk menambahkan opsi penggantian untuk yang lain VMs di klaster 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.

   Mengatur nilai-nilai berikut untuk setiap pilihan di bawah vSphere HA - VM Monitoring:

   - Pemantauan VM: Ganti Diaktifkan - VM dan Pemantauan Aplikasi
   - Sensitivitas pemantauan VM: Ganti Diaktifkan - VM dan Pemantauan Aplikasi
   - Pemantauan VM: Kustom
   - Interval kegagalan: **30** detik
   - Waktu aktif minimum: detik **120**
   - Reset per-VM maksimum: **5**
   - Jendela waktu reset maksimum: Dalam beberapa jam **1**

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-topik berikut:

  a. Connect Volume Gateway Anda ke AWS
  b. Tinjau pengaturan dan aktifkan Volume Gateway
  c. Konfigurasikan Volume Gateway

Uji Konfigurasi Ketersediaan VMware Tinggi Anda

Setelah Anda mengaktifkan gateway Anda, uji konfigurasi Anda.

Untuk menguji konfigurasi VMware HA Anda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada panel navigasi, pilih Gateways, lalu pilih gateway yang ingin Anda uji untuk HA. VMware
3. Untuk Tindakan, pilih Verifikasi VMware HA.
4. Di kotak Verifikasi Konfigurasi Ketersediaan VMware Tinggi 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 Volume Gateway dengan Grup CloudWatch Log.

Bekerja dengan sumber daya penyimpanan Volume Gateway

Topik di bagian ini menjelaskan bagaimana Anda dapat mengelola sumber daya penyimpanan yang terkait dengan alat Volume Gateway Anda dan platform host virtualnya. Ini termasuk sumber

daya seperti disk fisik yang terpasang pada platform host hypervisor gateway, dengan prosedur khusus untuk menghapus disk dari host virtualisasi VMware ESXi vSphere, Microsoft Hyper-V, atau Linux Kernel-based Virtual Machine (KVM). Ini juga termasuk mengelola volume Amazon EBS yang dilampirkan ke EC2 instance Amazon gateway untuk gateway yang dihosting di Amazon EC2 di cloud. AWS

Topik

- Menghapus Disk dari Gateway Anda- Pelajari tentang apa yang harus dilakukan jika Anda perlu menghapus disk dari platform host virtualisasi VMware vSphere, ESXi Microsoft Hyper-V, atau Linux Kernel-based Virtual Machine (KVM) untuk gateway Anda, misalnya jika Anda mengalami kegagalan disk fisik.
- Mengelola volume Amazon EBS di gateway Amazon EC2- Pelajari cara menambah atau mengurangi jumlah volume Amazon EBS yang dialokasikan untuk digunakan sebagai buffer unggahan atau penyimpanan cache untuk gateway yang di-host di EC2 instans Amazon, misalnya, jika kebutuhan penyimpanan aplikasi Anda bertambah atau berkurang seiring waktu.

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 Hosted on VMware ESXi

Anda dapat menggunakan prosedur berikut untuk menghapus disk dari gateway Anda yang dihosting di VMware hypervisor.

Untuk menghapus disk yang dialokasikan untuk buffer upload () 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.

Mengelola volume Amazon EBS di gateway Amazon EC2

Saat pertama kali mengonfigurasi gateway untuk dijalankan sebagai EC2 instans Amazon, 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

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 danMenentukan 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 EC2 Panduan Pengguna Amazon.
2. Lampirkan volume Amazon EBS ke EC2 instans Amazon Anda. Untuk petunjuk, lihat Melampirkan Volume Amazon EBS ke Instans di EC2 Panduan Pengguna Amazon.
3. Konfigurasikan volume Amazon EBS yang Anda tambahkan sebagai buffer unggahan atau penyimpanan cache. Untuk petunjuk, silakan lihat Mengelola disk lokal untuk Storage Gateway.

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.

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 EC2 Panduan Pengguna Amazon.
3. Hapus volume Amazon EBS. Untuk petunjuk, lihat Menghapus Volume Amazon EBS di EC2 Panduan Pengguna Amazon.
4. Mulai gateway dengan mengikuti pendekatan yang dijelaskan di Mematikan VM Gateway Anda bagian.

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 ActivateGatewaydi 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 EC2 Amazon 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)

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*- IPv4 Alamat gateway Anda, misalnya `172.31.29.201`
> - *gateway_type*- Jenis gateway yang ingin Anda aktifkan, seperti`STORED`,, `CACHEDVTL`,`FILE_S3`, atau`FILE_FSX_SMB`.
> - *region_code*- Wilayah tempat Anda ingin mengaktifkan gateway Anda. Lihat titik akhir Regional di Panduan Referensi AWS Umum. Jika parameter ini tidak ditentukan, atau jika nilai yang diberikan salah eja atau tidak cocok dengan wilayah yang valid, perintah akan default ke wilayah tersebut`us-east-1`.
> - *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 EC2 instans Amazon Anda 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 ke volume Anda dari klien Windows
- Menghubungkan volume 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 di Windows Server 2022. Inisiator dibangun ke dalam sistem operasi.

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.

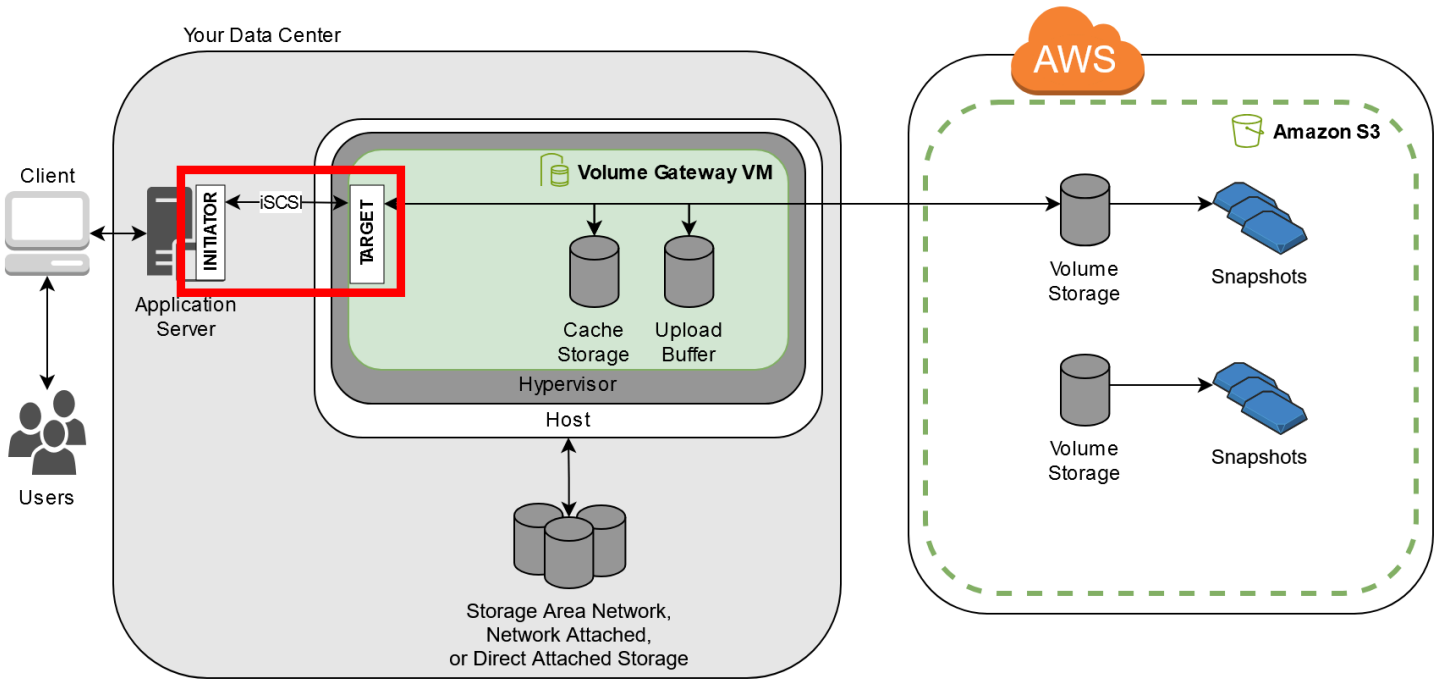
Setiap jenis gateway dapat terhubung ke perangkat iSCSI, dan Anda dapat menyesuaikan koneksi tersebut, seperti yang dijelaskan berikut.

Menghubungkan ke volume Anda dari klien Windows

Volume Gateway memperlihatkan volume yang telah Anda buat untuk gateway sebagai target iSCSI. Untuk informasi selengkapnya, lihat Menghubungkan volume Anda ke klien Anda.

> **Note**
>
> Untuk terhubung ke target volume Anda, gateway Anda harus memiliki buffer unggahan yang dikonfigurasi. Jika buffer upload tidak dikonfigurasi untuk gateway Anda, maka status volume Anda ditampilkan sebagai UPLOAD BUFFER TIDAK DIKONFIGURASI. Untuk mengonfigurasi buffer unggahan untuk gateway dalam pengaturan volume tersimpan, lihatUntuk mengonfigurasi buffer unggahan tambahan atau penyimpanan cache untuk gateway Anda. Untuk mengonfigurasi buffer unggahan untuk gateway dalam pengaturan volume cache, lihat. Untuk mengonfigurasi buffer unggahan tambahan atau penyimpanan cache untuk gateway Anda

Diagram berikut menyoroti target iSCSI dalam gambar yang lebih besar dari arsitektur Storage Gateway. Untuk informasi selengkapnya, lihat Cara kerja Volume Gateway.



Anda dapat terhubung ke volume Anda dari klien Windows atau Red Hat Linux. Anda dapat secara opsional mengkonfigurasi CHAP untuk salah satu jenis klien.

Gateway Anda mengekspos volume Anda sebagai target iSCSI dengan nama yang Anda tentukan, ditambah dengan. `iqn.1997-05.com.amazon:` Misalnya, jika Anda menentukan nama target`myvolume`, maka target iSCSI yang Anda gunakan untuk menyambung ke volume adalah. `iqn.1997-05.com.amazon:myvolume` Untuk informasi selengkapnya tentang cara

mengonfigurasi aplikasi Anda untuk memasang volume melalui iSCSI, lihat. Menghubungkan ke volume Anda dari klien Windows

Untuk	Lihat
Connect ke volume Anda dari Windows.	Menghubungkan ke Klien Microsoft Windows
Connect ke volume Anda dari Red Hat Linux.	Menghubungkan ke Klien Linux Red Hat Enterprise
Konfigurasikan otentikasi CHAP untuk Windows dan Red Hat Linux.	Mengkonfigurasi Otentikasi CHAP untuk Target iSCSI Anda

Untuk menghubungkan klien Windows Anda ke volume penyimpanan

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 Properti Inisiator iSCSI, pilih tab Discovery, lalu pilih Discover Portal.
4. Di kotak dialog Discover Target Portal, masukkan alamat IP target iSCSI 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 di EC2 instans Amazon, Anda dapat menemukan IP publik atau alamat DNS di tab Deskripsi di konsol Amazon EC2 .

   Alamat IP sekarang muncul di daftar portal Target pada tab Discovery.

   > **Warning**
   >
   > Untuk gateway yang digunakan pada EC2 instans Amazon, mengakses gateway melalui koneksi internet publik tidak didukung. Alamat IP Elastis dari EC2 instans Amazon tidak dapat digunakan sebagai alamat target.

5. Hubungkan portal target baru ke target volume penyimpanan di gateway:

   a. Pilih tabTarget.

      Portal target baru ditampilkan dengan status tidak aktif. Nama target yang ditampilkan harus sama dengan nama yang Anda tentukan untuk volume penyimpanan Anda di langkah 1.

   b. Pilih target, lalu pilih Connect.

      Jika nama target belum terisi, masukkan nama target seperti yang ditunjukkan pada langkah 1. Di kotak dialog Connect to Target, pilih Tambahkan koneksi ini ke daftar Target Favorit, lalu pilih OK.

   c. Di tab Target, pastikan bahwa Status target memiliki nilai Terhubung, menunjukkan target terhubung, lalu pilih OK.

Anda sekarang dapat menginisialisasi dan memformat volume penyimpanan ini untuk Windows sehingga Anda dapat mulai menyimpan data di dalamnya. Anda melakukan ini dengan menggunakan alat Manajemen Disk Windows.

> **Note**
>
> Meskipun tidak diperlukan untuk latihan ini, kami sangat menyarankan Anda menyesuaikan pengaturan iSCSI Anda untuk aplikasi dunia nyata seperti yang dibahas di. Menyesuaikan Pengaturan Windows iSCSI Anda

Menghubungkan volume 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 8 atau 9, gunakan perintah berikut.

      ```
      sudo service iscsid status
      ```

   b. Jika perintah status tidak mengembalikan status berjalan, mulai daemon menggunakan salah satu perintah berikut.

      Untuk RHEL 8 atau 9, gunakan perintah berikut. 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 *[GATEWAY_IP]* variabel dalam 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 yang benar *[GATEWAY_IP]* dan IQN dalam perintah connect.

> **Warning**
>
> Untuk gateway yang digunakan pada EC2 instans Amazon, mengakses gateway melalui koneksi internet publik tidak didukung. Alamat IP Elastis dari EC2 instans Amazon 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 dilampirkan 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

Saat menggunakan klien Windows, Anda menggunakan inisiator Microsoft iSCSI untuk terhubung ke volume gateway Anda. Untuk petunjuk tentang cara menghubungkan ke volume Anda, lihatMenghubungkan volume Anda ke klien Anda.

Untuk menyesuaikan pengaturan Windows iSCSI Anda

1. Tingkatkan waktu maksimum untuk permintaan yang diantrian.

   a. Mulai Editor Registri (`Regedit.exe`).

   b. Arahkan ke kunci pengenal unik global (GUID) untuk kelas perangkat yang berisi pengaturan pengontrol iSCSI, yang ditampilkan berikut.

   > **Warning**
   >
   > Pastikan Anda bekerja di CurrentControlSetsubkunci 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, ditampilkan sebagai berikut sebagai. *`[<Instance Number]`*

   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`.

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`**

MaxRequestHoldTimemenentukan 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.

2. Anda dapat meningkatkan jumlah maksimum data yang dapat dikirim dalam paket iSCSI dengan memodifikasi parameter berikut:

- FirstBurstLengthmengontrol 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.
- MaxBurstLengthmirip 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.
- MaxRecvDataSegmentLengthmengontrol 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:

a. Mulai Registry Editor (`Regedit.exe`), jika Anda belum melakukannya.

b. Arahkan ke subkunci Disk di subkunci Layanan dari CurrentControlSet, yang ditunjukkan berikut.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
```

c. Buka menu konteks (klik kanan) untuk nilai TimeOutValueDWORD (32-bit), pilih Ubah, lalu ubah nilainya menjadi. **`600`**

TimeOutValuemenentukan 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.

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. Tetapkan *[replacement_timeout_value]* nilainya ke**600**.

Tetapkan *[noop_out_interval_value]* nilainya ke**60**.

Tetapkan *[noop_out_timeout_value]* nilainya 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.

Tetapkan *[replacement_first_burst_length_value]* nilai ke **262144** atau default OS Linux, mana yang lebih tinggi.

Tetapkan *[replacement_max_burst_length_value]* nilai ke **1048576** atau default OS Linux, mana yang lebih tinggi.

Tetapkan *[replacement_segment_length_value]* nilai 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

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 *[timeout]* nilainya 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. Konfigurasikan CHAP di konsol Storage Gateway, seperti yang dibahas di Untuk mengkonfigurasi CHAP untuk target volume pada konsol Storage Gateway.
2. Dalam perangkat lunak inisiator klien Anda, selesaikan konfigurasi CHAP:
   - Untuk mengkonfigurasi CHAP bersama pada klien Windows, lihatUntuk mengkonfigurasi CHAP bersama pada klien Windows.
   - Untuk mengkonfigurasi CHAP bersama pada klien Red Hat Linux, lihatUntuk mengkonfigurasi CHAP bersama pada klien Red Hat Linux.

Untuk mengkonfigurasi CHAP untuk target volume pada konsol Storage Gateway

Dalam prosedur ini, Anda menentukan dua kunci rahasia yang digunakan untuk membaca dan menulis ke volume. Kunci yang sama ini digunakan dalam prosedur untuk mengkonfigurasi inisiator klien.

1. Pada konsol Storage Gateway, pilih Volume di panel navigasi.
2. Untuk Tindakan, pilih Konfigurasi Otentikasi CHAP.
3. 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 dilanjutkan dengan diikuti oleh nama target`iqn.1997-05.com.amazon:`. Berikut adalah contohnya.

      `iqn.1997-05.com.amazon:`*`your-volume-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.

4. Pilih tab Detail dan konfirmasikan bahwa 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. Konfigurasikan 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. Konfigurasikan target dengan rahasia inisiator untuk menyelesaikan konfigurasi CHAP bersama.

   a. Pilih tabTarget.

   b. Jika target yang ingin Anda konfigurasikan untuk CHAP saat ini terhubung, putuskan sambungan target dengan memilihnya dan memilih Putuskan sambungan.

   c. Pilih target yang ingin Anda konfigurasikan untuk CHAP, lalu pilih Connect.

   d. Di kotak dialog Connect to Target, pilih Advanced.

   e. Di kotak dialog Pengaturan Lanjut, konfigurasikan CHAP.

      i. Pilih Aktifkan CHAP log on.

      ii. Masukkan rahasia yang diperlukan untuk mengotentikasi 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 Menghubungkan ke Klien Linux Red Hat Enterprise .
2. Putuskan sambungan dan hapus konfigurasi yang ada untuk target yang akan Anda konfigurasikan 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*username*,, *passwordusername_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
username	Nama inisiator yang Anda temukan di langkah sebelumnya dalam prosedur ini. Nilai dimulai dengan iqn. Misalnya, **iqn.1994-05.com.redhat:8e89b27b5b8** adalah *username* nilai yang valid.
password	Kunci rahasia yang digunakan untuk mengotentikasi inisiator (klien yang Anda gunakan) ketika berkomunikasi dengan volume.
username_in	IQN dari volume target. Nilai dimulai dengan iqn dan diakhiri dengan nama target. Misalnya, **iqn.1997-05.com.amazon:myvolume** adalah *username_in* nilai yang valid.

Pengaturan Konfigurasi	Nilai
password_in	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 Menghubungkan ke Klien Linux Red Hat Enterprise yang .

Menggunakan AWS Direct Connect dengan Storage Gateway

AWS Direct Connect menautkan 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 gateway. 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 konfigurasikan router lokal Anda sesuai dengan itu. Bahkan dengan Direct Connect, titik akhir VPC harus dibuat dengan file. 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.

Mendapatkan alamat IP untuk alat 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 EC2 gateway Amazon, Anda juga bisa mendapatkan alamat IP EC2 instans Amazon Anda dari Amazon EC2 Management Console. Untuk mengetahui cara mendapatkan alamat IP gateway Anda, lihat salah satu dari berikut ini:

- VMware tuan rumah: 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
- EC2 tuan rumah: Mendapatkan Alamat IP dari EC2 Host Amazon

Ketika Anda menemukan alamat IP, perhatikan itu. Kemudian kembali ke konsol Storage Gateway dan ketik alamat IP ke konsol.

Mendapatkan Alamat IP dari EC2 Host Amazon

Untuk mendapatkan alamat IP EC2 instans Amazon gateway Anda digunakan, masuk ke konsol lokal EC2 instans. Kemudian dapatkan alamat IP dari bagian atas halaman konsol. Untuk petunjuk, silakan lihat Masuk ke Konsol Lokal Amazon EC2 Gateway Anda.

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 EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans, lalu pilih EC2 instance 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 EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans, lalu pilih EC2 instance 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 EC2 instance.

Memahami Sumber Daya dan Sumber Daya Storage Gateway IDs

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 subsumber daya ini memiliki Nama Sumber Daya Amazon (ARNs) unik yang terkait dengannya seperti yang ditunjukkan pada tabel berikut.

Jenis Sumber Daya	Format ARN
Gerbang ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`*` :gateway/` *`gateway-id`*
Volume ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`*` :gateway/` *`gateway-id`*` /volume/`*`volume-id`*
Target ARN (target iSCSI)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`*` :gateway/` *`gateway-id`*` /target/`*`iSCSItarget`*

Storage Gateway juga mendukung penggunaan EC2 instance dan volume dan snapshot EBS. Sumber daya ini adalah EC2 sumber daya Amazon yang digunakan di Storage Gateway.

Bekerja dengan Sumber Daya IDs

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 pengenal sumber daya untuk volume.

Untuk kaset virtual, Anda dapat menambahkan awalan hingga empat karakter ke ID barcode untuk membantu Anda mengatur kaset Anda.

Sumber daya Storage Gateway IDs berada dalam huruf besar. Namun, saat Anda menggunakan sumber daya ini IDs dengan Amazon EC2 API, Amazon EC2 mengharapkan sumber daya IDs dalam huruf kecil. Anda harus mengubah ID sumber daya Anda menjadi huruf kecil untuk menggunakannya dengan API. EC2 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, EC2 API 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 tag 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/rumah.
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/rumah.
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/rumah.
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 open-source untuk 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, unduh sources.tar VMware ESXi
- 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 volume
- Ukuran disk lokal yang direkomendasikan untuk gateway Anda

Kuota untuk volume

Tabel berikut mencantumkan kuota untuk volume.

Deskripsi	Volume cache	Volume yang disimpan
Ukuran maksimum volume	32 TiB	16 TiB

Deskripsi	Volume cache	Volume yang disimpan
Note Jika Anda membuat snapshot dari volume cache yang berukuran lebih dari 16 TiB, Anda dapat mengembal ikannya ke volume Storage Gateway tetapi tidak ke volume Amazon Elastic Block Store (Amazon EBS).		
Jumlah volume maksimum per gateway	32	32
Ukuran total semua volume untuk gateway	1.024 TiB	512 TiB

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 volume cache	150 GiB	64 TiB	150 GiB	2 TiB	—
Gerbang volume tersimpan	—	—	150 GiB	2 TiB	1 atau lebih untuk volume atau volume yang disimpan

> **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 SDKs saat mengembangkan aplikasi dengan AWS Storage Gateway. AWS SDKs 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

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 ActivateGatewayoperasi.

```
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`	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): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` Dalam sintaks sebelumnya, Anda menentukan, tahun, bulan YourAccesKey, dan hari (yyyymmdd), wilayah, dan. CalculatedSignature Format header otorisasi ditentukan oleh persyaratan proses Penandatanganan AWS V4. Rincian penandatanganan dibahas dalam topikMenandatangani Permintaan.
`Content-Type`	Gunakan `application/x-amz-json-1.1` sebagai tipe konten untuk semua permintaan ke Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Header	Deskripsi
`Host`	Gunakan header host untuk menentukan titik akhir Storage Gateway tempat Anda mengirim permintaan. Misalnya, `storagegateway.us-east-2.amazonaws.com` 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 `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Anda harus memberikan cap waktu baik di `Date` header HTTP atau AWS `x-amz-date` header. (Beberapa pustaka klien HTTP tidak mengizinkan Anda mengatur `Date` header.) Saat `x-amz-date` header hadir, Storage Gateway mengabaikan `Date` header apa pun selama otentikasi permintaan. Formatnya harus ISO86 01 Dasar `x-amz-date` dalam format YYYYYMMDD'T'HHMMSS'Z '. Jika kedua `Date` dan `x-amz-date` header digunakan, format header Tanggal tidak harus ISO86 01. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	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. `x-amz-target: StorageGateway_ APIversion .operationName` Nilai operationName (misalnya ActivateGateway "“) dapat ditemukan dari daftar API,. Referensi API untuk Storage Gateway

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 kredensyal 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 kredensyal untuk membuat serangkaian Kode Otentikasi Pesan berbasis Hash (). HMACs

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 apa pun APIs).

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.

UntukTugas 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, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, 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 diRespons 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
`IncompleteSignatureException`	Tanda tangan yang ditentukan tidak lengkap.	400 Permintaan Buruk
`InternalFailure`	Pemrosesan permintaan gagal karena beberapa kesalahan, pengecualian, atau kegagalan yang tidak diketahui.	500 Kesalahan Server Internal
`InternalServerError`	Salah satu pesan kode kesalahan operasiKode Kesalahan Operasi.	500 Kesalahan Server Internal
`InvalidAction`	Tindakan atau operasi yang diminta tidak valid.	400 Permintaan Buruk
`InvalidClientTokenId`	Sertifikat X.509 atau ID Kunci AWS Akses yang disediakan tidak ada dalam catatan kami.	403 Dilarang
`InvalidGatewayRequestException`	Salah satu pesan kode kesalahan operasi diKode Kesalahan Operasi.	400 Permintaan Buruk

Pengecualian	Pesan	Kode Status HTTP
`InvalidSignatureException`	Tanda tangan permintaan yang kami hitung tidak sesuai dengan tanda tangan yang Anda berikan. Periksa Kunci AWS Akses dan metode penandatanganan.	400 Permintaan Buruk
`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`	Tingkat terlampaui.	400 Permintaan Buruk
`TooManyRequests`	Terlalu banyak permintaan.	429 Terlalu Banyak Permintaan

Pengecualian	Pesan	Kode Status HTTP
`UnknownOperationException`	Operasi yang tidak diketahui ditentukan. Operasi yang valid tercantum dalamOperasi 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 APIs 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
`ActivationKeyExpired`	Kunci aktivasi yang ditentukan telah kedaluwarsa.	ActivateGateway
`ActivationKeyInvalid`	Kunci aktivasi yang ditentukan tidak valid.	ActivateGateway
`ActivationKeyNotFound`	Kunci aktivasi yang ditentukan tidak ditemukan.	ActivateGateway
`BandwidthThrottleScheduleNotFound`	Throttle bandwidth yang ditentukan tidak ditemukan.	DeleteBandwidthRateLimit

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`CannotExportSnapshot`	Snapshot yang ditentukan tidak dapat diekspor.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	Inisiator yang ditentukan tidak ditemukan.	DeleteChapCredentials
`DiskAlreadyAllocated`	Disk yang ditentukan sudah dialokasikan.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`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

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`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 DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

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 DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

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 DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	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 DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

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 ketinggalan zaman.	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 DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes 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 DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 dariPengecualian.

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

pesan

Salah satu pesan kode kesalahan operasi.

Tipe: String

Contoh Respon Kesalahan

Badan JSON berikut dikembalikan jika Anda menggunakan DescribeStoredi SCSIVolumes 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 Volume 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
Pemberitahuan perubahan ketersediaan untuk FSx File Gateway	Amazon FSx File Gateway tidak lagi tersedia untuk pelanggan baru. Pelanggan FSx File Gateway yang ada dapat terus menggunakan layanan ini secara normal. Untuk kemampuan yang mirip dengan FSx File Gateway, kunjungi posting blog ini.	Oktober 28, 2024
Pemberitahuan perubahan ketersediaan untuk FSx File Gateway	AWS Storage Gateway FSx File Gateway tidak akan lagi tersedia untuk pelanggan baru mulai 10/28/24. Untuk menggunakan layanan ini, Anda harus mendaftar sebelum tanggal tersebut. Pelanggan FSx File Gateway yang ada dapat terus menggunakan layanan ini secara normal. Untuk kemampuan yang mirip	September 26, 2024

	dengan FSx File Gateway, kunjungi posting blog ini.	
Menambahkan opsi untuk mengaktifkan atau menonaktifkan pembaruan pemeliharaan	Storage Gateway menerima pembaruan pemeliharaan rutin yang dapat mencakup peningkatan sistem operasi dan perangkat lunak, perbaikan untuk mengatasi stabilitas, kinerja, dan keamanan, dan akses ke fitur-fitur baru. Sekarang Anda dapat mengonfigurasi pengaturan untuk mengaktifkan atau menonaktifkan pembaruan ini untuk setiap gateway individu dalam penerapan Anda. Untuk informasi selengkapnya, lihat Mengelola pembaruan gateway menggunakan AWS Storage Gateway konsol.	Juni 6, 2024
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 .	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 disarankan juga telah diperbarui untuk `HealthNotifications` dan`AvailabilityNotifications` . Untuk informasi selengkapnya lihat .	2 Oktober 2023
Panduan Pengguna Pita dan Volume Gateway Terpisah	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.	Maret 23, 2022
Prosedur pembuatan gateway yang diperbarui	Prosedur untuk membuat semua jenis gateway menggunakan konsol Storage Gateway telah diperbarui. Untuk informasi selengkapnya, lihat Membuat Gateway Anda.	18 Januari 2022

Antarmuka Tapes baru	Halaman ikhtisar Tape di AWS Storage Gateway konsol telah diperbarui dengan fitur pencarian dan pemfilter an baru. Semua prosedur yang relevan dalam panduan ini telah diperbarui untuk menggambarkan fungsiona litas 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 untuk Storage 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 .	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 Wilayah Kanada (Tengah). 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 .	29 Mei 2020

Dukungan untuk titik akhir Federal Information Processing 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 mempertah ankan jumlah minimum kaset yang tersedia yang Anda konfigurasikan dan kemudian membuat kaset baru ini tersedia untuk diimpor oleh aplikasi cadangan, memungkin kan pekerjaan pencadang an 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 VMware untuk membantu melindungi beban kerja penyimpanan terhadap kegagalan perangkat keras, hypervisor, atau jaringan. Untuk informasi selengkapnya, lihat Menggunakan Ketersediaan Tinggi VMware vSphere dengan 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 penyimpan an 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 penyimpan an 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 ACLs	Untuk File Gateways, Anda sekarang dapat menggunakan daftar kontrol akses Microsoft Windows (ACLs) untuk mengontrol akses ke berbagi file Server Message Block (SMB). Untuk informasi selengkapnya, lihat Menggunakan Microsoft Windows ACLs 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 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 selengkap nya, lihat Menguji Pengatura n Anda dengan Menggunakan Microsoft System Center Data Protection Manager.	18 Juli 2018
Dukungan untuk protokol Server Message Block (SMB)	File Gateways menambahk an 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.	12 Juni 2018
Support NovaStor DataCenter untuk/Jaringan	Tape Gateways sekarang mendukung NovaStor DataCenter/Network. You can now use 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 Wilayah AWS yang mendukung Storage Gateway.	3 April 2018
Support untuk pemberitahuan cache refresh, pembayaran pemohon, dan kalengan ACLs untuk bucket Amazon S3.	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. File Gateways sekarang memungkinkan pemohon atau pembaca alih-alih pemilik bucket untuk membayar biaya akses. File Gateways sekarang memungkinkan Anda untuk memberikan kontrol penuh kepada pemilik bucket S3 yang memetakan ke berbagi file NFS. Untuk informasi selengkapnya, lihat Membuat berbagi file.	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 Wilayah AWS yang mendukung Storage Gateway.	18 Desember 2017
Support untuk notifikasi unggahan file dan tebakan tipe MIME	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 NotifyWhenUploadeddi Referensi API Storage Gateway. File Gateways sekarang memungkinkan menebak jenis MIME untuk objek yang diunggah berdasark an ekstensi file. Untuk informasi selengkapnya, lihat Membuat berbagi file.	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
Kompatibi litas dengan Commvault 11	Tape Gateways sekarang kompatibel dengan Commvault 11. Anda sekarang dapat menggunak an 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

Perubahan	Deskripsi	Tanggal Diubah
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
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 Wilayah AWS yang mendukung Storage Gateway.	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 RefreshCachedi Referensi API.	28 Maret 2017
Support untuk kloning 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
Support 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 komunitas AMI. Untuk informasi tentang cara membuat Gateway File dan menerapkannya pada EC2 instance, lihat Membuat dan mengaktifkan Gateway File Amazon S3 atau Membuat dan mengaktifkan FSx Amazon File Gateway. Untuk informasi tentang cara meluncurkan AMI Gateway File, lihat Menerapkan Gateway File S3 di EC2 host Amazon atau Menyebarkan Gateway FSx File 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 Wilayah AWS yang mendukung Storage Gateway.	13 Desember 2016
Wilayah Baru	Storage Gateway sekarang tersedia di Wilayah Kanada (Tengah). Untuk detail informasi, lihat Wilayah AWS yang mendukung Storage Gateway.	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 menggunak an 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 mencadang kan 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 Wilayah AWS yang mendukung Storage Gateway.	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 menyediak an 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 & Replicati on 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
Volume dan snapshot yang lebih panjang IDs	Storage Gateway memperkenalkan lebih lama IDs 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 dan Sumber Daya Storage Gateway IDs.	25 April 2016

Perubahan	Deskripsi	Tanggal Diubah
Wilayah Baru Support untuk penyimpanan hingga ukuran 512 TiB untuk volume yang disimpan Pembaruan dan penyempurnaan gateway lainnya ke konsol lokal Storage Gateway	Tape Gateway sekarang tersedia di Wilayah Asia Pasifik (Seoul). Untuk informasi selengkapnya, lihat Wilayah AWS yang mendukung Storage Gateway. Untuk volume tersimpan, Anda sekarang dapat membuat hingga 32 volume penyimpanan hingga 16 TiB dalam ukuran masing-masing, untuk penyimpan an maksimum 512 TiB. Untuk informasi selengkapnya, lihat Arsitektur volume tersimpan danAWS Storage Gateway kuota. Ukuran total semua kaset di perpustakaan pita virtual ditingkatkan menjadi 1 PiB. Untuk informasi selengkap nya, lihat AWS Storage Gateway kuota. Sekarang Anda dapat mengatur kata sandi untuk konsol lokal VM Anda di Storage Gateway Console. Untuk informasi, lihat Mengatur Kata Sandi Konsol Lokal dari Konsol Storage Gateway.	21 Maret 2016
Kompatibilitas dengan untuk Dell EMC 8.x NetWorker	Tape Gateway sekarang kompatibel dengan Dell EMC 8.x NetWorker . Anda sekarang dapat menggunak an 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.	29 Februari 2016

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. Untuk informasi selengkapnya, silakan lihat 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 Volume Gateway Anda.	

Perubahan	Deskripsi	Tanggal Diubah
Support untuk penyimpanan hingga 1.024 TiB dalam ukuran untuk volume cache Support untuk tipe adaptor jaringan VMXNET3 (10 GbE) di hypervisor VMware ESXi Peningkatan kinerja Berbagai penyempurnaan dan pembaruan ke konsol lokal Storage Gateway	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 danAWS Storage Gateway kuota. Jika gateway Anda di-host di VMware ESXi hyperviso r, Anda dapat mengkonfigurasi ulang gateway untuk menggunakan jenis adaptor. VMXNET3 Untuk informasi selengkapnya, lihat Mengkonfigurasi adapter jaringan untuk gateway Anda. Tingkat upload maksimum untuk Storage Gateway telah meningkat menjadi 120 MB per detik, dan tingkat unduhan maksimum telah meningkat menjadi 20 MB per detik. 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.	16 September 2015
Dukungan untuk penandaan	Storage Gateway sekarang mendukung penandaan sumber daya. Anda sekarang dapat menambahk an tag ke gateway, volume, dan kaset virtual untuk membuatnya lebih mudah dikelola. Untuk informasi selengkapnya, lihat Menandai Sumber Daya Storage Gateway.	September 2, 2015

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	Storage Gateway sekarang mendukung inisiator Red Hat Enterprise Linux 6 iSCSI. Untuk informasi selengkapnya, lihat Persyaratan untuk mengatur Volume Gateway.	
	Rilis ini mencakup peningkatan dan pembaruan Storage Gateway berikut: • 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. • Storage Gateway sekarang menyediakan API yang dapat Anda gunakan untuk membuat daftar inisiator iSCSI yang terhubung ke volume penyimpanan Anda. Untuk informasi selengkapnya, lihat ListVolumeInitiatorsdi referensi API.	

Perubahan	Deskripsi	Tanggal Diubah
Support untuk Microsoft Hyper-V hypervisor versi 2012 dan 2012 R2	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.	30 April 2015
Kompatibilitas dengan Symantec Backup Exec 15	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.	April 6, 2015
Dukungan otentikasi CHAP untuk volume penyimpanan	Storage Gateway sekarang mendukung konfigura si otentikasi CHAP untuk volume penyimpanan. Untuk informasi selengkapnya, lihat Mengkonfigurasi otentikasi CHAP untuk volume Anda.	2 April 2015
Support untuk VMware ESXi Hypervisor versi 5.1 dan 5.5	Storage Gateway sekarang mendukung VMware ESXi Hypervisor versi 5.1 dan 5.5. Ini sebagai tambahan untuk dukungan untuk VMware ESXi Hypervisor versi 4.1 dan 5.0. Untuk informasi selengkapnya, lihat Hypervisor dan persyaratan host yang didukung.	Maret 30, 2015
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

Perubahan	Deskripsi	Tanggal Diubah
Integrasi dengan AWS CloudTrail untuk menangkap panggilan API	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. Rilis ini mencakup peningkatan dan pembaruan Storage Gateway berikut: • 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	Tape Gateway sekarang kompatibel dengan perangkat lunak cadangan berikut: • Eksekutif Cadangan Symantec 2014 • Manajer Perlindungan Data Microsoft System Center 2012 R2 • Veeam Backup & Replikasi V7 • Veeam Backup & Replikasi V8 Anda sekarang dapat menggunakan empat produk perangkat lunak cadangan ini dengan pustaka pita virtual Storage Gateway (VTL) untuk mencadang kan 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. Storage Gateway sekarang menyediakan medium changer tambahan yang bekerja dengan perangkat lunak cadangan baru. Rilis ini mencakup berbagai AWS Storage Gateway perbaikan dan pembaruan.	November 3, 2014
Wilayah Eropa (Frankfurt)	Storage Gateway sekarang tersedia di Wilayah Eropa (Frankfurt). Untuk detail informasi, lihat Wilayah AWS yang mendukung Storage Gateway.	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
Support untuk Windows Server Failover Clustering Support untuk VMware inisiator ESX Support untuk melakukan tugas konfigurasi di konsol lokal Storage Gateway	• 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 AndaVMs. • 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 EC2 instance, lihat atau. Melakukan Tugas di Konsol EC2 Lokal Amazon Melakukan Tugas di Konsol EC2 Lokal Amazon	Januari 31, 2014

Perubahan	Deskripsi	Tanggal Diubah
Support untuk virtual tape library (VTL) dan pengenalan API versi 2013-06-30	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-v irtual 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. • 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	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	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 instance gateway di Amazon EC2 menggunakan Storage Gateway AMI yang tersedia di AWS Marketplace. Untuk mulai menerapkan gateway menggunakan Storage Gateway AMI, lihatMenerapkan EC2 instans Amazon yang disesuaikan untuk Volume Gateway.	Januari 15, 2013

Perubahan	Deskripsi	Tanggal Diubah
Support untuk volume cache dan pengenalan API Versi 2012-06-30	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 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. Dalam rilis ini, Storage Gateway juga memperkenalkan versi API baru yang, selain mendukung operasi saat ini, menyediakan operasi baru untuk mendukung volume cache. Untuk informasi selengkapnya tentang dua solusi Storage Gateway, lihatCara kerja Volume Gateway. Anda juga dapat mencoba pengaturan pengujian. Untuk petunjuk, lihat Membuat Gateway Tape.	Oktober 29, 2012

Perubahan	Deskripsi	Tanggal Diubah
Dukungan API dan IAM	Dalam rilis ini, Storage Gateway memperkenalkan dukungan API serta dukungan untuk AWS Identity and Access Management(IAM). • Dukungan API- Anda sekarang dapat mengkonfi gurasi 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, lihatIdentity 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	Anda sekarang dapat menentukan IP statis untuk gateway lokal Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi Jaringan Gateway Anda.	Maret 5, 2012
Panduan baru	Ini adalah rilis pertama Panduan AWS Storage Gateway Pengguna.	24 Januari 2012

Catatan rilis untuk perangkat lunak alat Volume Gateway

Catatan rilis ini menjelaskan fitur, peningkatan, dan perbaikan baru dan yang diperbarui yang disertakan dengan setiap versi alat Volume 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 DescribeGatewayInformationAPI 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 , termasuk cara mengubah pemeliharaan otomatis default dan jadwal pembaruan untuk gateway, lihat Mengelola Pembaruan Gateway Menggunakan Konsol Gateway AWS Penyimpanan.

Gateway berbasis Amazon Linux 2023 (AL2023)

Tabel berikut mencantumkan catatan rilis untuk gateway berdasarkan AL2 023.

> **Note**
>
> Gateway versi 2.xx tidak dapat diperbarui ke 3.xx.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-07-16	3.0.0	• Rilis awal sistem operasi baru

Gateway berbasis Amazon Linux 2 (AL2)

Tabel berikut mencantumkan catatan rilis untuk gateway berdasarkan. AL2

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-07-31	2.12.12	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2025-07-01	2.12.11	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2025-06-02	2.12.10	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2025-05-01	2.12.9	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
		untuk gateway baru dan yang sudah ada
2025-05-01	2.12.8	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2025-04-01	2.12.7	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2025-03-04	2.12.6	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2025-02-04	2.12.5	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada • Mengatasi masalah di mana gateway bisa macet dalam status shutdown setelah pembaruan perangkat lunak

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-01-07	2.12.3	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2024-12-06	2.12.2	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2024-11-06	2.12.1	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2024-10-03	2.12.0	• Mengatasi masalah di mana inisiator iSCSI tidak akan secara otomatis terhubung kembali dengan volume setelah gateway restart atau pembaruan perangkat lunak gateway • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2024-08-30	2.11.0	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2024-07-29	2.10.0	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada • Perbaikan dan penyempurnaan bug lain-lain
2024-06-17	2.9.2	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja untuk gateway baru dan yang sudah ada
2024-05-28	2.9.0	• Mengurangi waktu restart gateway selama pembaruan perangkat lunak • Mengurangi jumlah data yang ditransfer untuk memperkirakan bandwidth jaringan
2024-05-08	2.8.3	• Mengatasi masalah konektivitas cloud saat menggunakan SOCKS5 proxy

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2024-04-10	2.8.1	• Mengatasi masalah penggunaan memori yang diperkenalkan di 2.8.0 • Pembaruan patch keamanan • Proses pembaruan perangkat lunak yang ditingkatkan • Mengatasi komponen Network Time Protocol (NTP) yang hilang untuk gateway baru
2024-03-06	2.8.0	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja untuk gateway baru • Pembaruan patch keamanan
2023-12-19	2.7.0	• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja untuk gateway baru
2023-12-14	2.6.6	• Rilis pemeliharaan

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