Panduan Pengguna Gateway File Amazon S3

AWS Storage Gateway

Versi API 2013-06-30

AWS Storage Gateway: Panduan Pengguna Gateway File Amazon S3

Table of Contents

Apa itu Gateway File Amazon S3

Amazon S3 File Gateway — Amazon S3 File Gateway mendukung antarmuka file ke Amazon Simple Storage Service (Amazon S3) dan menggabungkan layanan dan alat perangkat lunak virtual. Dengan kombinasi ini, Anda dapat menyimpan dan mengambil objek di Amazon S3 menggunakan protokol file standar industri seperti Network File System (NFS) dan Server Message Block (SMB). Anda menerapkan gateway ke lingkungan lokal Anda sebagai mesin virtual (VM) yang berjalan di VMware ESXi, Hyper-V Microsoft, atau Kernel-based Linux Virtual Machine (KVM), atau sebagai perangkat keras yang Anda pesan dari pengecer pilihan Anda. Anda juga dapat menerapkan Storage Gateway VM di VMware Cloud AWS, atau sebagai AMI di Amazon EC2. Gateway ini menyediakan akses ke objek di S3 sebagai file atau titik pemasangan pembagian file. Dengan S3 File Gateway, Anda dapat melakukan hal berikut:

- Anda dapat menyimpan dan mengambil file secara langsung menggunakan protokol NFS versi 3 atau 4.1.
- Anda dapat menyimpan dan mengambil file secara langsung menggunakan versi sistem file SMB, protokol 2 dan 3.
- Anda dapat mengakses data Anda secara langsung di Amazon S3 dari aplikasi atau AWS layanan Cloud apa pun.
- Anda dapat mengelola data S3 menggunakan kebijakan siklus hidup, replikasi lintas wilayah, dan pembuatan versi. Anda dapat menganggap S3 File Gateway sebagai mount sistem file di Amazon S3.

Gateway File S3 menyederhanakan penyimpanan file di Amazon S3, terintegrasi ke aplikasi yang ada melalui protokol sistem file standar industri, dan menyediakan alternatif hemat biaya untuk penyimpanan lokal. Ini juga menyediakan akses latensi rendah ke data melalui caching lokal transparan. File Gateway S3 mengelola transfer data ke dan dari AWS, buffer aplikasi dari kemacetan jaringan, mengoptimalkan dan mengalirkan data secara paralel, dan mengelola konsumsi bandwidth.

S3 File Gateway terintegrasi dengan AWS layanan lain, misalnya:

- Manajemen akses umum menggunakan AWS Identity and Access Management (IAM)
- Enkripsi menggunakan AWS Key Management Service (AWS KMS)
- Pemantauan menggunakan Amazon CloudWatch (CloudWatch)

- Audit menggunakan AWS CloudTrail (CloudTrail)
- Operasi menggunakan Konsol Manajemen AWS dan AWS Command Line Interface (AWS CLI)
- Manajemen penagihan dan biaya

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

- memberikan instruksi tentang cara membuat dan menggunakan S3 File Gateway. Ini menunjukkan kepada Anda cara membuat berbagi file, memetakan drive Anda ke bucket Amazon S3, dan mengunggah file dan folder ke Amazon S3.

- menjelaskan cara melakukan tugas manajemen untuk semua jenis dan sumber daya gateway.

Dalam panduan ini, Anda terutama dapat menemukan cara bekerja dengan operasi gateway dengan menggunakan Konsol Manajemen AWS. Jika Anda ingin menjalankan operasi ini secara terprogram, lihat Referensi API AWS Storage Gateway.

Cara kerja Gateway File Amazon S3

Untuk menggunakan Gateway File S3, Anda mulai dengan mengunduh gambar VM untuk gateway. Anda kemudian mengaktifkan gateway dari Konsol Manajemen AWS atau melalui Storage Gateway API. Anda juga dapat membuat Gateway File S3 menggunakan gambar Amazon EC2.

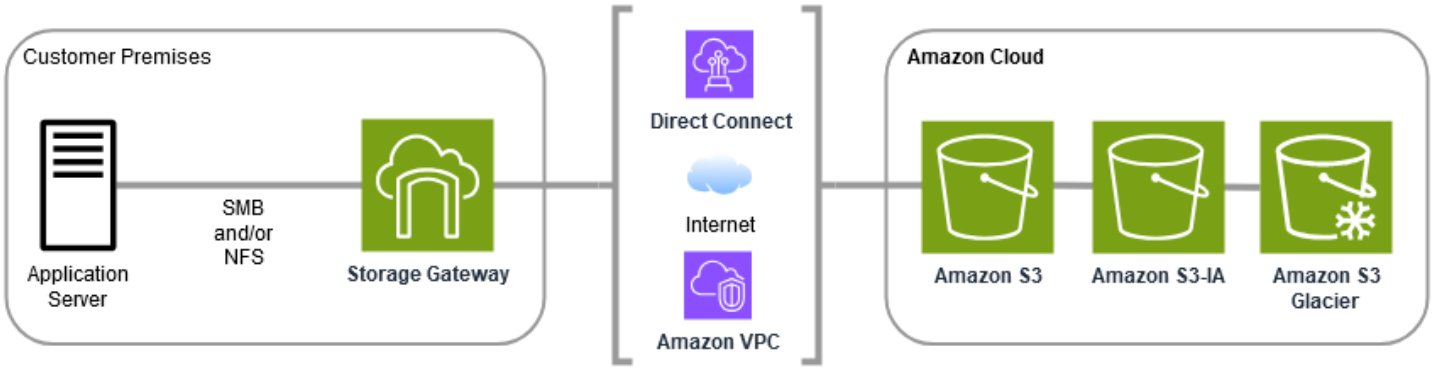
Setelah Gateway File S3 diaktifkan, Anda membuat dan mengonfigurasi berbagi file dan mengaitkan berbagi itu dengan bucket Amazon Simple Storage Service (Amazon S3). Melakukan hal ini membuat share dapat diakses oleh klien menggunakan protokol Network File System (NFS) atau Server Message Block (SMB). File yang ditulis ke berbagi file menjadi objek di Amazon S3, dengan jalur sebagai kuncinya. Ada pemetaan satu-ke-satu antara file dan objek, dan gateway secara asinkron memperbarui objek di Amazon S3 saat Anda mengubah file. Objek yang ada di bucket Amazon S3 muncul sebagai file dalam sistem file, dan kuncinya menjadi jalur. Objek dienkripsi dengan Amazon S3 — kunci enkripsi sisi server (). SSE-S3 Semua transfer data dilakukan melalui HTTPS.

Saat mengirim permintaan unggahan data HTTPS ke Amazon S3, File Gateway mengisi Content-MD5 header dengan checksum MD5 dari data yang diunggah. Penggunaan header ini menyebabkan

Amazon S3 mengembalikan kegagalan jika terjadi ketidakcocokan antara checksum MD5 yang dihitung oleh Amazon S3 dan nilai yang diterima dari File Gateway. Jika kegagalan tersebut dikembalikan, File Gateway mengirim ulang permintaan.

Layanan ini mengoptimalkan transfer data antara gateway dan AWS menggunakan unggahan paralel multibagian atau unduhan rentang byte, untuk menggunakan bandwidth yang tersedia dengan lebih baik. Cache lokal dipertahankan untuk menyediakan akses latensi rendah ke data yang baru diakses dan mengurangi biaya keluar data. CloudWatch metrik memberikan wawasan tentang penggunaan sumber daya pada VM dan transfer data ke dan dari. AWS CloudTrail melacak semua panggilan API.

Dengan penyimpanan S3 File Gateway, Anda dapat melakukan tugas-tugas seperti menelan beban kerja cloud ke Amazon S3, melakukan pencadangan dan pengarsipan, tiering, dan migrasi data penyimpanan ke Cloud. AWS Diagram berikut memberikan gambaran umum tentang penyebaran penyimpanan file untuk Storage Gateway.



S3 File Gateway mengonversi file ke objek S3 saat mengunggah file ke Amazon S3. Interaksi antara operasi file yang dilakukan terhadap berbagi file pada S3 File Gateway dan objek S3 memerlukan operasi tertentu untuk dipertimbangkan dengan cermat saat mengonversi antara file dan objek.

Operasi file umum mengubah metadata file, yang menghasilkan penghapusan objek S3 saat ini dan pembuatan objek S3 baru. Tabel berikut menunjukkan contoh operasi file dan dampak pada objek S3.

Operasi file	Dampak objek S3	Implikasi kelas penyimpanan
Ganti nama file	Mengganti objek S3 yang ada dan membuat objek S3 baru untuk setiap file	Biaya penghapusan awal dan biaya pengambilan mungkin berlaku

Operasi file	Dampak objek S3	Implikasi kelas penyimpanan
Ganti nama folder	Mengganti semua objek S3 yang ada dan membuat objek S3 baru untuk setiap folder dan file dalam struktur folder	Biaya penghapusan awal dan biaya pengambilan mungkin berlaku
Ubah file/folder izin	Mengganti objek S3 yang ada dan membuat objek S3 baru untuk setiap file atau folder	Biaya penghapusan awal dan biaya pengambilan mungkin berlaku
Ubah file/folder kepemilikan	Mengganti objek S3 yang ada dan membuat objek S3 baru untuk setiap file atau folder	Biaya penghapusan awal dan biaya pengambilan mungkin berlaku
Tambahkan ke file	Mengganti objek S3 yang ada dan membuat objek S3 baru untuk setiap file	Biaya penghapusan awal dan biaya pengambilan mungkin berlaku

Saat file ditulis ke Gateway File S3 oleh klien NFS atau SMB, File Gateway mengunggah data file ke Amazon S3 diikuti oleh metadatanya, (kepemilikan, cap waktu, dll.). Mengunggah data file membuat objek S3, dan mengunggah metadata untuk file memperbarui metadata untuk objek S3. Proses ini menciptakan versi lain dari objek, menghasilkan dua versi objek. Jika S3 Versioning diaktifkan, kedua versi akan disimpan.

Saat file dimodifikasi di Gateway File S3 oleh klien NFS atau SMB setelah diunggah ke Amazon S3, Gateway File S3 mengunggah data baru atau yang dimodifikasi alih-alih mengunggah seluruh file. Modifikasi file menghasilkan versi baru dari objek S3 yang sedang dibuat.

Ketika S3 File Gateway mengunggah file yang lebih besar, mungkin perlu mengunggah potongan file yang lebih kecil sebelum klien selesai menulis ke S3 File Gateway. Beberapa alasan untuk ini termasuk membebaskan ruang cache atau tingkat penulisan yang tinggi ke berbagi file. Ini dapat menghasilkan beberapa versi objek di bucket S3.

Anda harus memantau bucket S3 untuk menentukan berapa banyak versi objek yang ada sebelum menyiapkan kebijakan siklus hidup untuk memindahkan objek ke kelas penyimpanan yang berbeda. Anda harus mengonfigurasi kedaluwarsa siklus hidup untuk versi sebelumnya untuk meminimalkan jumlah versi yang Anda miliki untuk objek di bucket S3 Anda. Penggunaan Same-Region replikasi

(SRR) atau Cross-Region replikasi (CRR) antara bucket S3 akan meningkatkan penyimpanan yang digunakan.

Memulai denganAWS Storage Gateway

Bagian ini memberikan instruksi untuk memulaiAWS. Anda memerlukan AWS akun sebelum Anda dapat mulai menggunakanAWS 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 AWSWilayah yang didukung dan persyaratan penyiapan File Gateway sebelum Anda bekerja dengan Storage Gateway.

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

Topik

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

Mendaftar untukAkun AWS

Untuk memulaiAWS, Anda membutuhkanAkun AWS. Untuk informasi tentang membuatAkun AWS, lihat Memulai dengan Akun AWS di Panduan AWS Account Management Referensi.

MengaksesAWS Storage Gateway

Anda dapat menggunakan AWS Storage Gatewaykonsol untuk melakukan berbagai tugas konfigurasi dan pemeliharaan gateway, termasuk mengaktifkan atau menghapus peralatan perangkat keras Storage Gateway dari penerapan Anda, membuat, mengelola, dan menghapus berbagai

jenis gateway, membuat , mengelola, dan menghapus yang , 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 memilih 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 AWSCLI.

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

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

Wilayah AWSyang 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, sepertiAWS 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 instans Amazon EC2 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.

- Storage Gateway — Untuk AWS Wilayah yang didukung dan daftar titik akhir AWS layanan yang dapat Anda gunakan dengan Storage Gateway, lihat AWS Storage Gatewaytitik akhir dan kuota di. Referensi Umum AWS
- Storage Gateway Hardware Appliance — Untuk Wilayah yang didukung yang dapat Anda gunakan dengan AWS Storage Gatewayperangkat keras, lihat Wilayah Perangkat Keras di Referensi Umum AWS.

Persyaratan pengaturan File Gateway

Kecuali dinyatakan lain, persyaratan berikut ini umum untuk semua jenis File Gateway di AWS Storage Gateway. Pengaturan Anda harus memenuhi persyaratan di bagian ini. Tinjau persyaratan yang berlaku untuk penyiapan gateway sebelum menerapkan gateway.

Topik

Prasyarat

Sebelum Anda mengatur Gateway (S3 File Gateway), Anda harus memenuhi prasyarat berikut:

- Konfigurasikan Microsoft Active Directory (AD) dan buat akun layanan Active Directory dengan izin yang diperlukan. Untuk informasi selengkapnya, lihat Persyaratan izin akun layanan Direktori Aktif Persyaratan .
- Pastikan bahwa ada bandwidth jaringan yang cukup antara gateway dan AWS. Minimal 100 Mbps diperlukan untuk berhasil mengunduh, mengaktifkan, dan memperbarui gateway.
- Konfigurasikan sambungan yang ingin Anda gunakan untuk lalu lintas jaringan antara AWS dan lingkungan lokal tempat Anda menggunakan gateway. Anda dapat terhubung menggunakan internet publik, jaringan pribadi, VPN, atau Direct Connect. Jika Anda ingin gateway Anda berkomunikasi AWS melalui koneksi pribadi ke Amazon Virtual Private Cloud, siapkan VPC Amazon sebelum mengatur gateway Anda.
- Pastikan gateway Anda dapat menyelesaikan nama Active Directory Domain Controller Anda. Anda dapat menggunakan DHCP di domain Active Directory untuk menangani resolusi, atau menentukan server DNS secara manual dari menu pengaturan Konfigurasi Jaringan di konsol lokal gateway.

Persyaratan perangkat keras dan penyimpanan

Bagian berikut memberikan informasi tentang konfigurasi perangkat keras dan penyimpanan minimum yang diperlukan untuk gateway Anda, dan jumlah minimum ruang disk yang akan dialokasikan untuk penyimpanan yang diperlukan.

Untuk informasi tentang praktik terbaik untuk kinerja File Gateway, lihatPanduan kinerja dasar untuk S3 File Gateway Gateway.

Persyaratan perangkat keras untuk VM lokal

Saat menerapkan gateway lokal, pastikan perangkat keras dasar tempat Anda menggunakan mesin virtual gateway (VM) dapat mendedikasikan sumber daya minimum berikut:

- Empat prosesor virtual ditugaskan ke VM
- 16 GiB RAM yang dicadangkan untuk File Gateways
- 80 GiB ruang disk untuk instalasi gambar VM dan data sistem

Untuk informasi selengkapnya, lihat Memaksimalkan throughput Gateway File S3. Untuk informasi tentang bagaimana perangkat keras Anda memengaruhi kinerja VM gateway, lihatKuota untuk berbagi file.

Persyaratan untuk jenis instans Amazon EC2

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

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

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

Direkomendasikan untuk tipe File Gateway

- General-purpose keluarga instance — tipe instans m5, m6, atau m7. Pilih ukuran instans xlarge atau lebih tinggi untuk memenuhi persyaratan prosesor dan RAM Storage Gateway.
- Compute-optimized keluarga instance — c5, c6, atau c7 jenis instans. Pilih ukuran instans 2xlarge atau lebih tinggi untuk memenuhi persyaratan prosesor dan RAM Storage Gateway.
- Memory-optimized keluarga instance — tipe instans r5, r6, atau r7. Pilih ukuran instans xlarge atau lebih tinggi untuk memenuhi persyaratan prosesor dan RAM Storage Gateway.
- Storage-optimized keluarga instance — tipe instans i3, i4 atau i7. Pilih ukuran instans xlarge atau lebih tinggi untuk memenuhi persyaratan prosesor dan RAM Storage Gateway.

> **Note**
>
> Saat meluncurkan gateway di Amazon EC2 dan jenis instans yang Anda pilih mendukung penyimpanan sementara, disk akan dicantumkan secara otomatis. Untuk informasi selengkapnya tentang penyimpanan instans Amazon EC2, lihat Penyimpanan instans di Panduan Pengguna Amazon EC2.
>
> Penulisan aplikasi disimpan dalam cache secara sinkron, dan kemudian diunggah secara asinkron ke penyimpanan tahan lama di Amazon S3. Jika penyimpanan sementara hilang karena instance berhenti sebelum unggahan selesai, data yang masih berada di cache dan belum ditulis ke Amazon Simple Storage Service (Amazon S3) dapat hilang. Sebelum Anda menghentikan instance yang menghosting gateway, pastikan `CachePercentDirty` CloudWatch metriknya`0`. Untuk informasi tentang penyimpanan sementara, lihat. Menggunakan penyimpanan singkat dengan gateway EC2 Untuk informasi tentang metrik pemantauan untuk Storage Gateway Anda, lihatMemantau Gateway File Gateway S3 Anda.
>
> Jika Anda memiliki lebih dari 5 juta objek di bucket S3 Anda dan Anda menggunakan volume EBS gp2, volume EBS root minimum 350 GiB diperlukan untuk kinerja gateway Anda yang dapat diterima selama start up. Newly-created Instans Gateway File Amazon EC2 menggunakan volume root gp3 secara default, yang tidak memiliki persyaratan ini. Untuk informasi tentang cara meningkatkan ukuran volume, lihat Memodifikasi volume EBS menggunakan volume elastis (konsol).

Persyaratan penyimpanan

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

Jenis gateway	Cache (minimum)	Cache (maksimum)			
Gateway File:	150 GiB	64 TiB			

> **Note**
>
> Anda dapat mengkonfigurasi satu atau lebih drive lokal untuk cache Anda, hingga kapasitas maksimum.
> Saat menambahkan cache 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.

Untuk informasi tentang kuota gateway, lihatKuota untuk berbagi file.

Persyaratan jaringan dan firewall

Gateway Anda memerlukan akses ke internet, jaringan lokal, server Domain Name Service (DNS), firewall, router, dan sebagainya.

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.

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 gateway di Amazon EC2 atau menggunakan jenis penerapan lain (termasuk lokal) dengan kebijakan keamanan jaringan yang AWS membatasi rentang alamat IP. Dalam kasus ini, gateway Anda mungkin mengalami masalah konektivitas layanan saat nilai rentang AWS IP berubah. Nilai rentang alamat AWS IP yang perlu Anda gunakan ada di subset layanan Amazon untuk AWS Wilayah

tempat Anda mengaktifkan gateway Anda. Untuk nilai rentang IP saat ini, lihat rentang alamat AWS IP di Referensi Umum AWS.

Topik

- Persyaratan port
- Persyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance
- Mengizinkan AWS Storage Gateway akses melalui firewall dan router
- Mengonfigurasi grup keamanan untuk instans gateway Amazon EC2 Anda

Persyaratan port

S3 File Gateway memerlukan port tertentu untuk diizinkan melalui keamanan jaringan Anda untuk penyebaran dan operasi yang berhasil. Beberapa port diperlukan untuk semua gateway, sementara yang lain hanya diperlukan untuk konfigurasi tertentu, seperti saat menghubungkan ke klien NFS atau SMB, titik akhir VPC, atau Microsoft Active Directory.

Untuk S3 File Gateway, Anda hanya perlu menggunakan Microsoft Active Directory ketika Anda ingin mengizinkan pengguna domain mengakses berbagi file Server Message Block (SMB). Anda dapat bergabung dengan File Gateway Anda ke domain Microsoft Windows yang valid (dapat diselesaikan oleh DNS).

Anda juga dapat menggunakan Directory Service untuk membuat AWS Managed Microsoft ADdi Amazon Web Services Cloud. Untuk sebagian besar AWS Managed Microsoft AD penerapan, Anda perlu mengonfigurasi layanan Dynamic Host Configuration Protocol (DHCP) untuk VPC Anda. Untuk informasi tentang membuat set opsi DHCP, lihat Membuat opsi DHCP yang diatur dalam Panduan AWS Directory Service Administrasi.

Tabel berikut mencantumkan port yang diperlukan dan menjelaskan persyaratan bersyarat di kolom Catatan.

Persyaratan port untuk persyaratan Port Gateway File S3 File 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 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 diperluka

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
								n ke port 80 tergantung pada konfigurasi jaringan Anda. Jika Anda mengaktifkan gateway dari Storage Gateway Management Console, host tempat Anda terhubung ke konsol harus memiliki akses ke port gateway 80 Anda.

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	✓	✓	✓	Kontrol manajemen
Amazon CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	Untuk aktivasi
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	Kontrol 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 Pesawat 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	✓	✓	✓*	Kontrol manajemen * Diperlukan hanya saat menggunakan titik akhir VPC

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Klien berbagi file	Klien SMB	Storage Gateway VM	TCP atau UDP SMBv3	445	✓	✓	✓*	Layanan sesi transfer data berbagi file. Menggantikan port 137-139 untuk Microsoft Windows NT dan yang lebih baru. *Diperlukan untuk SMB saja.
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	UDP NetBIOS	137	✓	✓	✓*	Nama layanan *Diperlukan hanya untuk SMBv1.

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	UDP NetBIOS	138	✓	✓	✓*	Layanan datagram *Diperlukan hanya untuk SMBv1.
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	LDAP TCP & UDP	389	✓	✓	✓*	Koneksi klien Directory System Agent (DSA) *Diperlukan untuk SMB saja.
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	TCP & UDP Kerberos	88	✓	✓	✓*	Kerberos *Diperlukan untuk SMB saja.

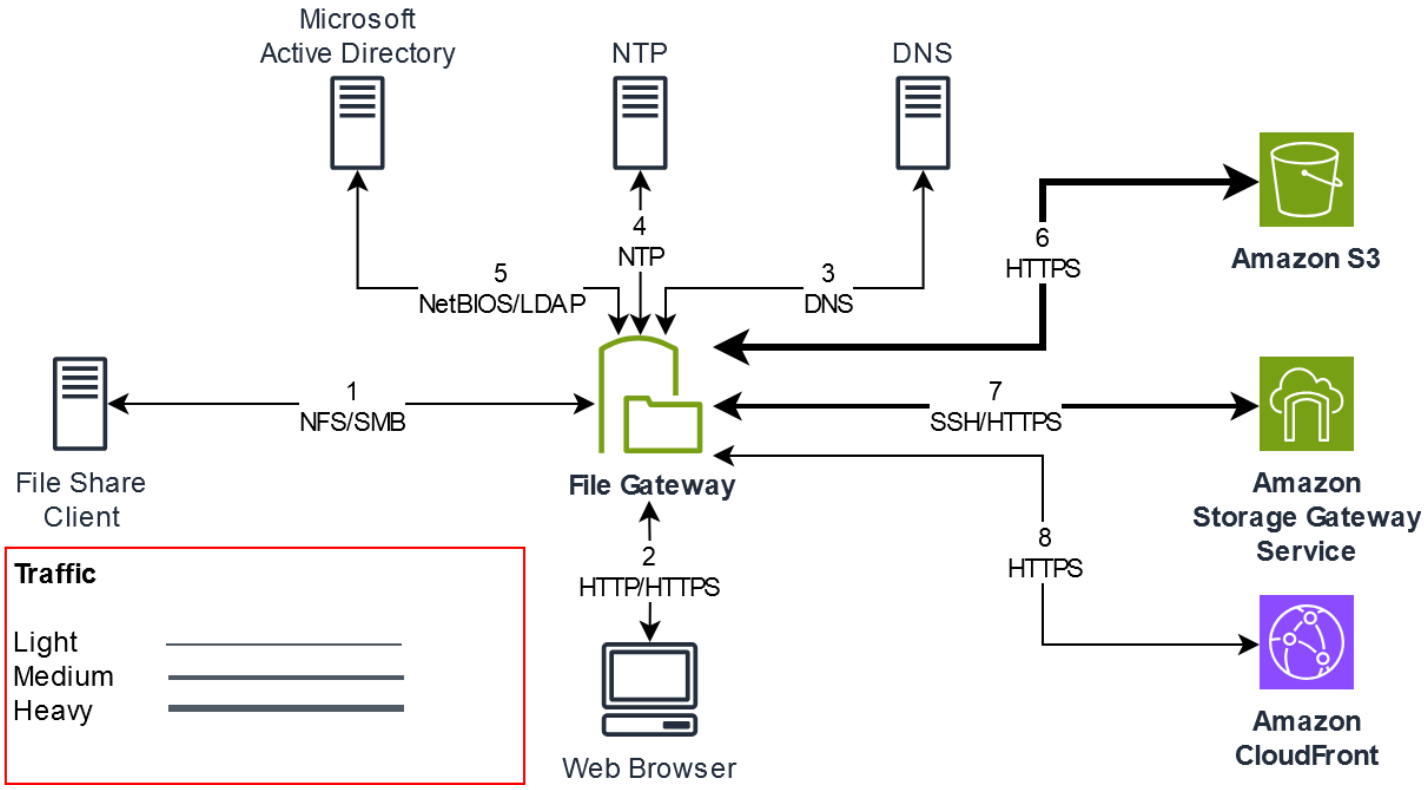
Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	Pemetaar Environme nt/End Titik Komputas Terdistri busi TCP () DCE/ EMAP	135	✓	✓	✓*	RPC *Diperluk an untuk SMB saja.
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	Pemetaar Environme nt/End Titik Komputas Terdistri busi TCP () DCE/ EMAP	49152-65 35	✓	✓	✓*	RPC Atau, jika Pengontro l Domain AD Anda menggunak an port RPC khusus, buka port tersebut. *Diperluk an untuk SMB saja.

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Klien berbagi file	Klien NFS	Storage Gateway VM	Data TCP atau UDP NFSv3	111	✓	✓	✓*	Transfer data berbagi file (hanya untuk NFS v3) * Diperlukan hanya untuk NFS.
Klien berbagi file	Klien NFS	Storage Gateway VM	TCP atau UDP NFS	2049	✓	✓	✓*	Transfer data berbagi file * Diperlukan untuk NFS v3 & v4 saja.

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Klien berbagi file	Klien NFS	Storage Gateway VM	TCP atau UDP NFSv3	20048	✓	✓	✓*	Transfer data berbagi file *Diperlukan hanya untuk NFSv3
Klien berbagi file	Klien SMB	Storage Gateway VM	TCP atau UDP SMBv2	139	✓	✓	✓*	Layanan sesi transfer data berbagi file *Diperlukan hanya untuk SMB

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Amazon S3	Storage Gateway VM	Titik akhir layanan Amazon S3	TCP HTTPS	443	✓	✓	✓	Untuk komunikasi dari Storage Gateway VM ke endpoint AWS layanan. Untuk informasi tentang titik akhir layanan, lihat Mengizinkan akses AWS Storage Gateway melalui firewall dan router.

Ilustrasi berikut menunjukkan arus lalu lintas jaringan untuk penerapan S3 File Gateway dasar.



Persyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance

Setiap Storage Gateway Hardware Appliance memerlukan layanan jaringan berikut:

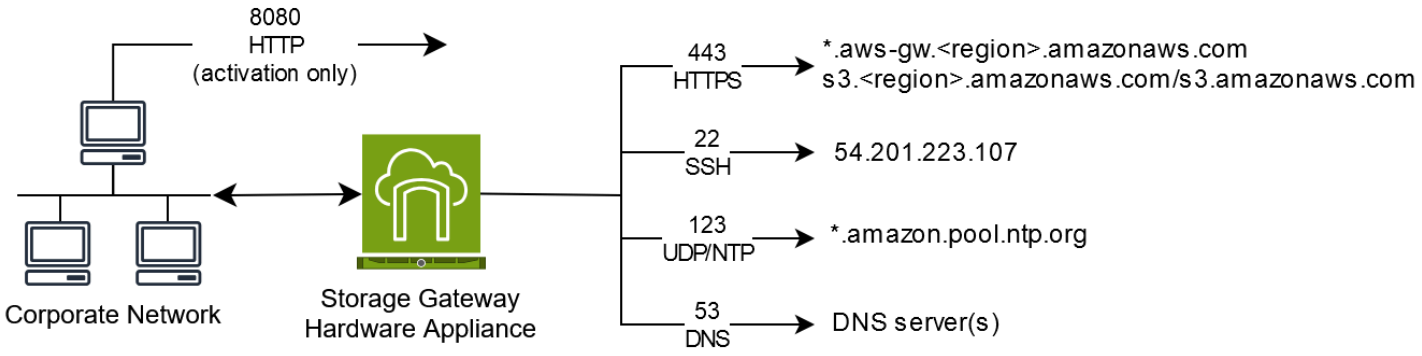
- Akses Internet — koneksi jaringan yang selalu aktif ke internet melalui antarmuka jaringan apa pun di server.
- Layanan DNS — Layanan DNS untuk komunikasi antara perangkat keras dan server DNS.
- Sinkronisasi waktu - layanan waktu Amazon NTP yang dikonfigurasi secara otomatis harus dapat dijangkau.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

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

1. iDRAC
2. `em1`

3. em2
4. em3
5. em4

Anda dapat menggunakan port IDRac untuk manajemen server jarak jauh.



Alat perangkat keras membutuhkan port berikut untuk beroperasi.

Protokol	Port	Arahan	Sumber	Destinasi	Penggunaan
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

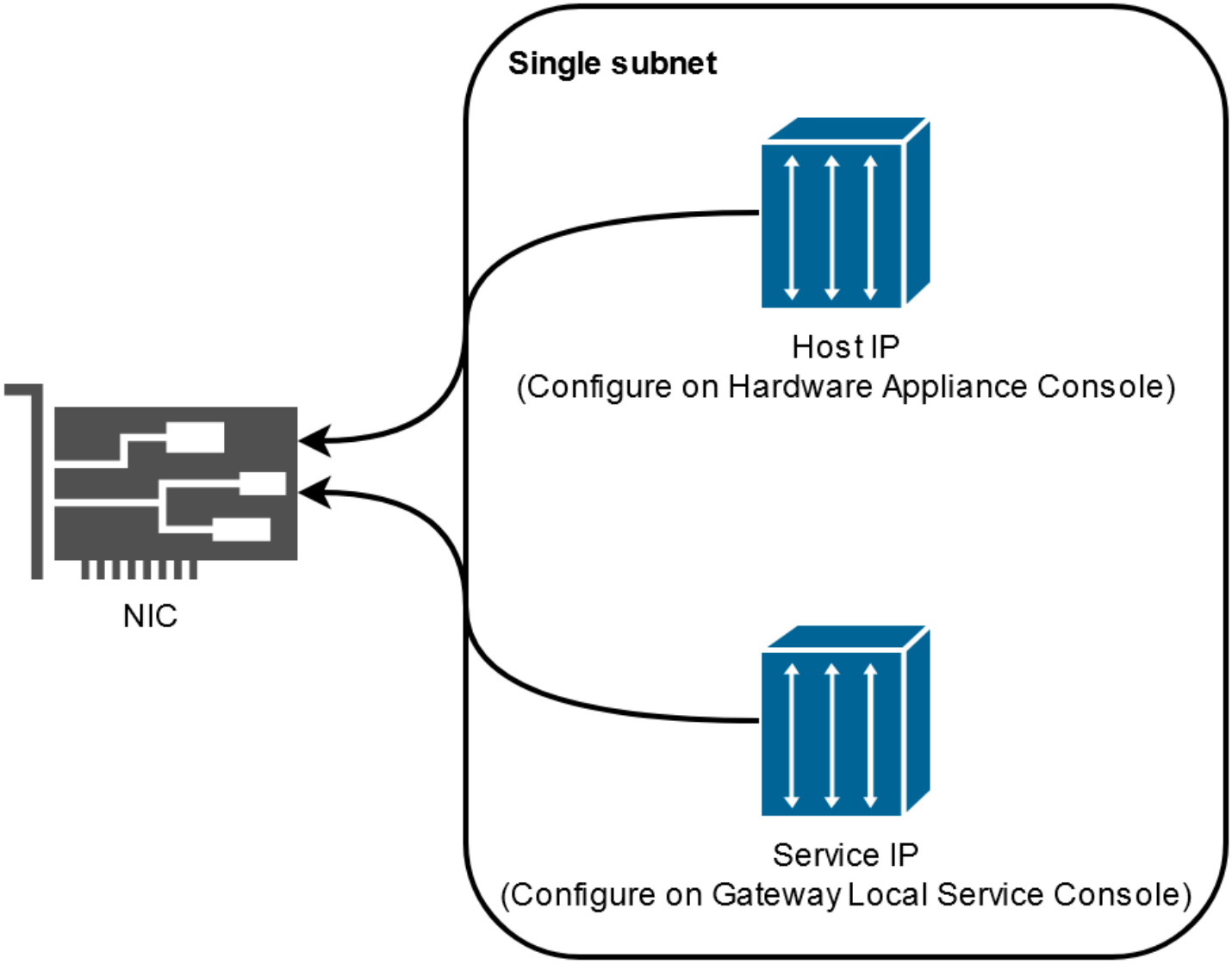
Protokol	Port	Arahan	Sumber	Destinasi	Penggunaan
HTTP	8080	Ke dalam	AWS	Alat perangkat keras	Aktivasi (hanya sebentar)

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, lihatMemasang 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 AWS Peralatan Perangkat Keras Storage Gateway]

Mengizinkan AWS Storage Gateway akses melalui firewall dan router

Gateway Anda memerlukan akses ke titik akhir layanan Storage Gateway berikut untuk berkomunikasi AWS. Selama pengaturan gateway, pilih jenis titik akhir untuk gateway Anda berdasarkan lingkungan jaringan Anda. 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**
>
> Ganti *region* contoh endpoint berikut dengan Wilayah AWS string yang benar untuk gateway Anda, sepertius-west-2.
> Ganti *amzn-s3-demo-bucket* dengan nama sebenarnya dari bucket Amazon S3 dalam penerapan Anda. Anda juga dapat menggunakan tanda bintang (*) sebagai pengganti *amzn-s3-demo-bucket* untuk membuat entri wildcard dalam aturan firewall Anda, yang akan memungkinkan daftar titik akhir layanan untuk semua nama bucket.
> Jika gateway Anda digunakan Wilayah AWS di Amerika Serikat atau Kanada dan memerlukan koneksi titik akhir yang sesuai dengan Standar Pemrosesan Informasi Federal (FIPS), ganti dengan. *s3* s3-fips

Jenis titik akhir

Titik akhir standar

Titik akhir ini mendukung lalu lintas IPv4 antara alat gateway Anda dan. AWS

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

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

Titik akhir layanan berikut diperlukan oleh semua gateway untuk operasi jalur kontrol (anon-cp,client-cp,proxy-app) dan jalur data (dp-1).

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

Titik akhir layanan gateway berikut diperlukan untuk melakukan panggilan API.

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

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

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

Dual-stack titik akhir

Titik akhir ini mendukung lalu lintas IPv4 dan IPv6 antara perangkat gateway Anda dan. AWS

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

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

Titik akhir layanan dual-stack berikut diperlukan oleh semua gateway untuk operasi jalur kontrol (aktivasi, controlplane, proxy) dan jalur data (dataplane).

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

Titik akhir layanan dual-stack gateway berikut diperlukan untuk melakukan panggilan API.

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

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

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

Titik akhir layanan Amazon S3

Amazon S3 File Gateway memerlukan tiga jenis titik akhir berikut untuk terhubung ke layanan Amazon S3:

Titik akhir layanan Amazon S3

> **Note**
>
> Untuk titik akhir ini saja, jangan ganti `s3` dengan `s3-fips` untuk FIPS-compliant penerapan.

```
s3.amazonaws.com
```

Titik akhir regional Amazon S3

```
s3.region.amazonaws.com (Standard)
s3.dualstack.region.amazonaws.com (Dual-stack)
```

Contoh berikut menunjukkan titik akhir regional Amazon S3 di Wilayah Timur AS (Ohio) (). `us-east-2`

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

Contoh berikut menunjukkan titik akhir regional Amazon FIPS-compliant S3 standar dan dual-stack di Wilayah AS Barat (California Utara) (). `us-west-1`

```
s3-fips.us-west-1.amazonaws.com
s3-fips.dualstack.us-west-1.amazonaws.com
```

Contoh berikut menunjukkan titik akhir regional Amazon S3 standar dan dual-stack yang digunakan oleh Wilayah: AWS GovCloud (US)

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

```
s3.dualstack.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Dual-stack))
```

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

Titik akhir bucket Amazon S3

```
bucket-name.s3.region.amazonaws.com (Standard)
bucket-name.s3.dualstack.region.amazonaws.com (Dual-stack)
```

Contoh berikut menunjukkan titik akhir bucket Amazon S3 standar dan dual-stack untuk bucket yang *amzn-s3-demo-bucket* diberi nama di Wilayah AS Timur (Ohio) (). `us-east-2`

```
amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com (Standard)
amzn-s3-demo-bucket.s3.dualstack.us-east-2.amazonaws.com (Dual-stack)
```

Contoh berikut menunjukkan titik akhir bucket Amazon FIPS-compliant S3 standar dan dual-stack untuk bucket yang *amzn-s3-demo-bucket1* diberi nama di AWS GovCloud (US-East) Region (). `us-gov-east-1`

```
amzn-s3-demo-bucket1.s3-fips.us-gov-east-1.amazonaws.com (FIPS)
amzn-s3-demo-bucket1.s3-fips.dualstack.us-gov-east-1.amazonaws.com (FIPS dual-stack)
```

Selain Storage Gateway dan endpoint layanan Amazon S3, VM Storage Gateway juga memerlukan akses jaringan ke server NTP berikut:

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

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

Untuk informasi selengkapnya tentang titik akhir yang didukung Wilayah AWS dan layanan, lihat Storage Gateway di. Referensi Umum AWS

Mengonfigurasi grup keamanan untuk instans gateway Amazon EC2 Anda

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

- Kelompok keamanan tidak boleh mengizinkan koneksi masuk dari internet luar. Seharusnya hanya mengizinkan instance dalam grup keamanan gateway untuk berkomunikasi dengan gateway.

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

Untuk informasi tentang port yang akan dibuka untuk gateway Anda, lihatPersyaratan port.

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**
>
> Mode boot UEFI dengan boot aman dinonaktifkan (loader_secure=no) diperlukan untuk File Gateway 2.x, Volume Gateway 3.x, dan Tape Gateway 3.x. File xml. disediakan dengan setiap unduhan qcow sebagai konfigurasi pengaturan cepat.

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 (2019, 2022, atau 2025) - Untuk pengaturan ini, Anda memerlukan Microsoft Hyper-V Manager di komputer klien Microsoft Windows untuk terhubung ke host.
- Linux Kernel-based Virtual Machine (KVM) — Teknologi virtualisasi open-source gratis. 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, RHEL 8.6 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. Lihat file aws-storage-gateway.xml yang disediakan untuk konfigurasi boot yang disarankan. Mode boot UEFI dengan boot aman dinonaktifkan (loader_secure=no) diperlukan untuk File Gateway 2.x, Volume Gateway 3.x, dan Tape Gateway 3.x.
- Nutanix AHV (Acropolis Hypervisor) dimulai dengan versi 10.0.1.1 — Platform KVM-based virtualisasi yang terintegrasi ke dalam solusi Nutanix hyper-converged infrastructure (HCI).
- Instans Amazon EC2 — Storage Gateway menyediakan Amazon Machine Image (AMI) yang berisi image VM gateway. Untuk informasi tentang cara menerapkan gateway di Amazon EC2, lihat. Menerapkan host Amazon EC2 default untuk S3 File Gateway
- Storage Gateway Hardware Appliance — Storage Gateway menyediakan perangkat keras fisik sebagai opsi penyebaran lokal untuk lokasi dengan infrastruktur mesin virtual terbatas.

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

Klien NFS dan SMB yang didukung untuk File Gateway

File Gateway mendukung klien berikut:

Versi Sistem Operasi	Versi Kernel	Protokol yang Didukung
Amazon Linux 2023	6.1 LTS	NFSv4.1, NFSv3
Amazon Linux 2	5.10 LTS	NFSv4.1, NFSv3
RHEL 9	5.14	NFSv4.1, NFSv3
RHEL 8.10	4.18	NFSv4.1, NFSv3
SUSE 15	6.4	NFSv4.1, NFSv3
Ubuntu 24.04 LTS	6,8 LTS	NFSv4.1, NFSv3
Ubuntu 22.04 LTS	5.15 LTS	NFSv4.1, NFSv3
Microsoft Windows Server 2025		SMBv2, SMBv3, NFSv3
Server Microsoft Windows 2022		SMBv2, SMBv3, NFSv3
Microsoft Windows 11		SMBv2, SMBv3, NFSv3
Microsoft Windows 10		SMBv2, SMBv3, NFSv3

> **Note**
>
> Enkripsi Blok Pesan Server (SMB) membutuhkan klien yang mendukung dialek SMB v3.

Operasi sistem file yang didukung untuk File Gateway

Klien NFS atau SMB Anda dapat menulis, membaca, menghapus, dan memotong file. Ketika klien mengirim penulisan ke AWS Storage Gateway, ia menulis ke cache lokal secara sinkron. Kemudian ia menulis ke Amazon S3 secara asinkron melalui transfer yang dioptimalkan. Pembacaan pertama kali disajikan melalui cache lokal. Jika data tidak tersedia, data diambil melalui S3 sebagai cache baca-melalui.

Menulis dan membaca dioptimalkan karena hanya bagian yang diubah atau diminta yang ditransfer melalui gateway Anda. Menghapus menghapus objek dari Amazon S3. Direktori dikelola sebagai objek folder di S3, menggunakan sintaks yang sama seperti di konsol Amazon S3.

Operasi HTTP sepertiGET,, PUTUPDATE, dan DELETE dapat memodifikasi file dalam berbagi file. Operasi ini sesuai dengan fungsi atomic create, read, update, and delete (CRUD).

Mengelola disk lokal untuk gateway Anda

Mesin virtual (VM) gateway menggunakan disk lokal yang Anda alokasikan secara on-premise untuk buffering dan penyimpanan. File Gateway yang Anda buat di instans Amazon EC2 akan menggunakan volume Amazon EBS sebagai disk lokal. Jumlah dan ukuran disk yang ingin Anda alokasikan untuk gateway Anda terserah Anda. Gateway menggunakan penyimpanan cache yang Anda alokasikan 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 . File Gateways membutuhkan setidaknya satu disk 150 GiB untuk digunakan sebagai cache. Setelah konfigurasi awal dan penerapan gateway Anda, Anda dapat menambahkan lebih banyak disk untuk penyimpanan cache saat tuntutan beban kerja Anda meningkat. Bagian ini berisi topik-topik berikut, yang menjelaskan konsep dan prosedur yang terkait dengan pengelolaan disk lokal.

Topik

- Menentukan jumlah penyimpanan disk lokal- Pelajari cara menentukan jumlah dan ukuran disk cache lokal yang akan dialokasikan untuk File Gateway Anda.
- Mengkonfigurasi penyimpanan cache tambahan- Pelajari cara meningkatkan kapasitas penyimpanan cache File Gateway Anda saat aplikasi Anda perlu diubah.
- Menggunakan penyimpanan singkat dengan gateway EC2- Pelajari cara mencegah kehilangan data saat menggunakan penyimpanan disk sementara dengan File Gateway.

Menentukan jumlah penyimpanan disk lokal

Saat menerapkan Gateway File S3 FSx File , pertimbangkan berapa banyak disk cache yang akan dialokasikan. S3 File Gateway Gateway menggunakan algoritma yang paling jarang digunakan untuk secara otomatis mengusir data dari cache. Cache pada Gateway File S3 Gateway dibagi antara semua berbagi file di gateway itu. Jika Anda memiliki beberapa saham aktif, penting untuk dicatat

bahwa pemanfaatan berat pada satu saham dapat memengaruhi jumlah sumber daya cache yang dapat diakses oleh pembagian lain, yang mungkin memengaruhi kinerja.

Saat menentukan berapa banyak disk cache yang Anda butuhkan untuk beban kerja tertentu, penting untuk dicatat bahwa Anda selalu dapat menambahkan disk cache ke gateway Anda (hingga kuota saat ini di S3 File Gateway FSx), tetapi Anda tidak dapat mengurangi cache untuk gateway tertentu. Anda dapat melakukan analisis dasar pada dataset untuk menentukan jumlah disk cache yang tepat, tetapi tidak ada cara untuk menentukan dengan tepat berapa banyak data yang 'panas', dan perlu disimpan secara lokal, versus 'dingin' dan dapat berjenjang ke cloud. Beban kerja berubah seiring waktu, dan S3 File Gateway FSx memberikan fleksibilitas dan elastisitas terkait dengan jumlah sumber daya yang dapat dikonsumsi. Jumlah cache selalu dapat ditingkatkan, jadi mulai dari yang kecil dan meningkat sesuai kebutuhan seringkali merupakan pendekatan yang paling hemat biaya.

Anda dapat menggunakan perkiraan awal 150 GiB untuk menyediakan disk untuk penyimpanan cache selama pengaturan gateway. 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. Kinerja dan optimasi

> **Note**
>
> 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), 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. Penyimpanan data yang didukung oleh hanya satu disk fisik yang mendasarinya dapat menyebabkan kinerja yang buruk dalam beberapa situasi ketika digunakan untuk mendukung kedua penyimpanan cache. Ini juga berlaku jika cadangan adalah konfigurasi RAID yang kurang berkinerja seperti RAID1.

Mengkonfigurasi penyimpanan cache tambahan

Karena aplikasi Anda perlu berubah, Anda dapat meningkatkan kapasitas penyimpanan cache gateway. 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 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.

Untuk mengonfigurasi penyimpanan cache tambahan untuk gateway Anda

1. Menyediakan satu atau beberapa disk baru di hypervisor host gateway atau instans Amazon EC2 Anda. Untuk informasi tentang cara menyediakan disk pada hypervisor, lihat dokumentasi hypervisor Anda. Untuk informasi tentang penyediaan volume Amazon EBS untuk instans Amazon EC2, lihat volume Amazon EBS di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux. Pada langkah-langkah berikut, Anda akan mengkonfigurasi disk ini sebagai penyimpanan cache.
2. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.
3. Di panel navigasi, pilih Gateway.
4. Cari gateway Anda dan pilih dari daftar.
5. Dari menu Tindakan, pilih Konfigurasi penyimpanan cache.
6. Di bagian Konfigurasi penyimpanan cache, identifikasi disk yang Anda sediakan. Jika Anda tidak melihat disk Anda, pilih ikon penyegaran untuk menyegarkan daftar. Untuk setiap disk, pilih Cache dari menu drop-down yang dialokasikan ke.

   > **Note**
   >
   > Cache adalah satu-satunya pilihan yang tersedia untuk mengalokasikan disk pada File Gateway.

7. Pilih Simpan perubahan untuk menyimpan pengaturan konfigurasi Anda.

Menggunakan penyimpanan singkat dengan gateway EC2

Bagian ini menjelaskan langkah-langkah yang perlu Anda ambil untuk mencegah kehilangan data ketika Anda memilih disk sementara sebagai penyimpanan untuk cache gateway Anda.

Disk ephemeral menyediakan penyimpanan tingkat blok sementara untuk instans Amazon EC2 Anda. Disk ephemeral ideal untuk penyimpanan sementara data yang sering berubah, seperti data dalam penyimpanan cache gateway. Saat meluncurkan gateway dengan Amazon EC2 Amazon Machine Image dan jenis instans yang Anda pilih mendukung penyimpanan sementara, disk fana akan dicantumkan secara otomatis. Anda dapat memilih salah satu disk untuk menyimpan data cache gateway Anda. Untuk informasi selengkapnya, lihat penyimpanan instans Amazon EC2 di Panduan Pengguna Amazon EC2.

Anda dapat mencegah kehilangan data tersebut dengan mengikuti langkah-langkah sebelum memulai ulang atau menghentikan instans EC2 yang menghosting gateway Anda.

> **Important**
>
> Jika Anda berhenti dan memulai gateway Amazon EC2 yang menggunakan penyimpanan sementara, gateway akan offline secara permanen. Ini terjadi karena disk penyimpanan fisik diganti. Tidak ada solusi untuk masalah ini. Satu-satunya resolusi adalah menghapus gateway dan mengaktifkan yang baru pada instans EC2 baru.

Langkah-langkah dalam prosedur berikut ini khusus untuk File Gateways.

Untuk mencegah kehilangan data di File Gateways yang menggunakan disk sementara

1. Hentikan semua proses yang menulis ke Amazon S3.
2. Berlangganan untuk menerima pemberitahuan dari CloudWatch Acara. Untuk informasi, lihat Mendapatkan pemberitahuan tentang operasi file.
3. Panggil NotifyWhenUploaded API untuk mendapatkan pemberitahuan ketika data yang ditulis, hingga penyimpanan sementara hilang, telah disimpan dengan tahan lama di Amazon S3.
4. Tunggu API selesai dan Anda menerima id notifikasi.

   Anda menerima CloudWatch acara dengan id notifikasi yang sama.
5. Verifikasi bahwa `CachePercentDirty` metrik untuk berbagi file Anda adalah 0. Ini menegaskan bahwa semua data Anda telah ditulis ke Amazon S3. Untuk informasi tentang metrik berbagi file, lihatMemahami metrik berbagi file.
6. Anda sekarang dapat memulai ulang atau menghentikan File Gateway tanpa risiko kehilangan data apa pun.

Menggunakan AWS Peralatan Perangkat Keras Storage Gateway

> **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.

AWS 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 menyebarkan jenis gateway ini pada alat perangkat keras sama dengan pada platform virtual.

Untuk daftar yang didukung Wilayah AWS di mana AWS Storage Gateway Hardware Appliance tersedia untuk aktivasi dan penggunaan, lihat AWS 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 AWS Storage Gateway Hardware Appliance.

Topik

- Memasang alat perangkat keras Anda secara fisik
- Mengakses konsol alat perangkat keras
- Mengkonfigurasi parameter jaringan alat perangkat keras
- Mengaktifkan Anda AWS Peralatan Perangkat Keras Storage Gateway
- Membuat gateway pada perangkat keras Anda
- Mengkonfigurasi alamat IP gateway pada alat perangkat keras
- Menghapus perangkat lunak gateway dari alat perangkat keras Anda
- Menghapus Anda AWS Peralatan Perangkat Keras Storage Gateway

Menyiapkan Anda AWS Peralatan Perangkat Keras Storage Gateway

> **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. Rack-mount alat, dan colokkan listrik dan koneksi 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 Anda AWS Peralatan Perangkat Keras Storage Gateway.
4. Buat gateway pada alat perangkat keras Anda. Untuk informasi selengkapnya, lihat Membuat gateway Anda.

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

Meningkatkan penyimpanan cache yang dapat digunakan

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

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

1. Setel ulang alat perangkat keras ke pengaturan pabriknya. Hubungi AWS Support untuk petunjuk tentang cara melakukan ini.
2. Tambahkan lima SSD 1,92 TB ke alat.

Opsi kartu antarmuka jaringan

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

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

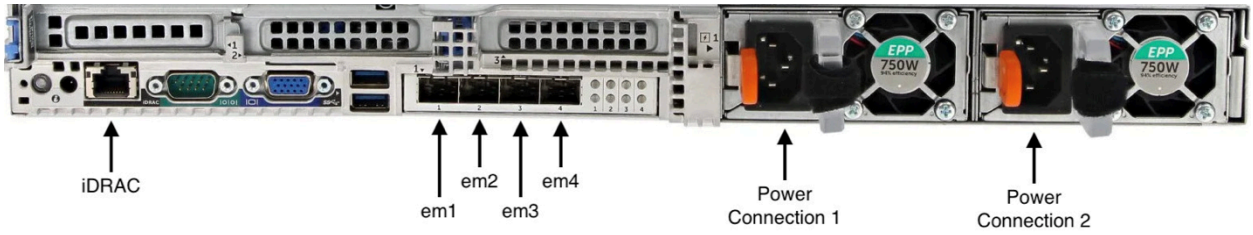
- Kabel daya: satu diperlukan, dua direkomendasikan.
- Kabel jaringan yang didukung (tergantung pada Kartu Antarmuka Jaringan (NIC) yang disertakan dalam alat perangkat keras). Twinax Copper DAC, modul optik SFP+(kompatibel dengan Intel) atau transceiver SFP ke tembaga. Base-T
- Keyboard dan monitor,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

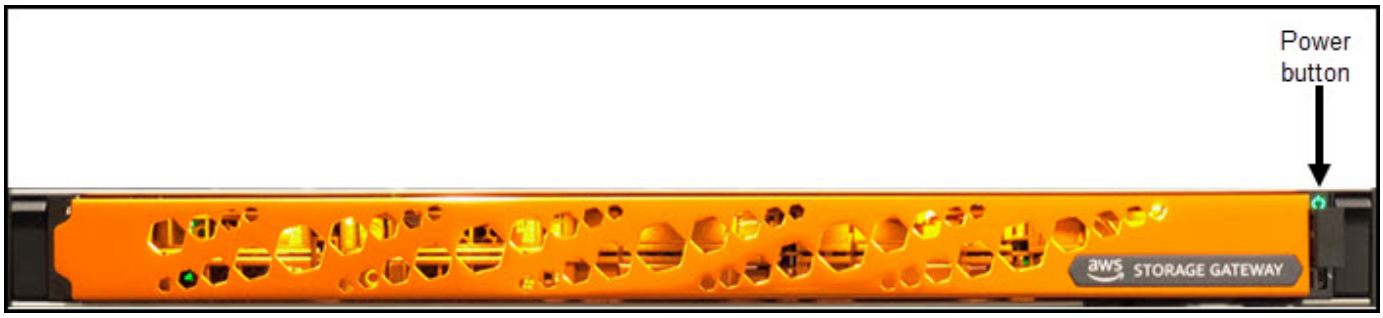


alat perangkat keras satu belakang dengan label konektor jaringan dan daya.

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 menyetel 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 alamat IPv4 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 mengkonfigurasi alamat IPv4 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 Anda AWS Peralatan Perangkat Keras Storage Gateway

Mengaktifkan Anda AWS Peralatan Perangkat Keras Storage Gateway

> **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 Anda AWS Peralatan Perangkat Keras Storage Gateway

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 Mengonfigurasi parameter jaringan parameter jaringan.
5. Untuk Nama, masukkan nama untuk perangkat keras Anda. Nama dapat mencapai 255 karakter dan tidak dapat menyertakan karakter garis miring.
6. Untuk zona waktu perangkat keras, masukkan zona waktu lokal 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 Gateway File S3, FSx File Gateway, Tape Gateway, atau Volume Gateway pada AWS Storage Gateway Hardware Appliance apa pun dalam penerapan Anda.

Untuk membuat gateway pada perangkat keras Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.

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 Storage Gateway di konsol 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 Aktivasi AWS Alat - Konfigurasi mencakup opsi menu berikut:

   - HTTP/SOCKS Konfigurasi Proxy
   - 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 pengaturan dan konfigurasi untuk gateway Anda di konsol Storage Gateway. Untuk petunjuk, lihat Mengonfigurasikan Gateway File Amazon S3.

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/home.
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 Anda AWS Peralatan Perangkat Keras Storage Gateway

> **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 AWS Storage Gateway Hardware Appliance yang telah diaktifkan, Anda dapat menghapus perangkat sepenuhnya dari AWS akun Anda.

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

Untuk menghapus alat perangkat keras Anda

1. Jika Anda telah menginstal gateway pada alat perangkat keras, Anda harus terlebih dahulu menghapus gateway sebelum Anda dapat menghapus alat. Untuk petunjuk tentang cara menghapus gateway dari perangkat keras Anda, 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 Gateway File Amazon S3
- Membuat dan mengaktifkan Amazon FSx File Gateway
- Membuat dan mengaktifkan Tape Gateway
- Membuat dan mengaktifkan Volume Gateway

Ikhtisar - Aktivasi Gateway

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

Menyiapkan gateway

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

Connect ke AWS

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

Tinjau dan aktifkan

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

Ikhtisar - Konfigurasi Gateway

Setelah 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 dan mengaktifkan Gateway File Amazon S3

Di bagian ini, Anda dapat menemukan petunjuk tentang cara membuat, menyebarkan, dan mengaktifkan File Gateway di AWS Storage Gateway.

Topik

- Menyiapkan Gateway File Amazon S3
- Hubungkan Gateway File Amazon S3 Anda ke AWS

- Tinjau pengaturan dan aktifkan Gateway File Amazon S3 Anda
- Mengonfigurasikan Gateway File Amazon S3

Menyiapkan Gateway File Amazon S3

Untuk mengatur Gateway File S3 baru

1. Buka Konsol Manajemen AWS 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 Mengatur gateway.
3. Di bagian Pengaturan Gateway, lakukan hal berikut:

   a. Untuk nama Gateway, masukkan nama untuk gateway Anda. Setelah gateway Anda dibuat, Anda dapat mencari nama ini untuk menemukan gateway Anda di halaman daftar di AWS Storage Gateway konsol.

   b. Untuk zona waktu Gateway, pilih zona waktu lokal untuk bagian dunia tempat Anda ingin menggunakan gateway Anda.
4. Di bagian opsi Gateway, untuk jenis Gateway, pilih Amazon S3 File Gateway.
5. Di bagian Opsi platform, lakukan hal berikut:

   a. Untuk platform Host, pilih platform tempat Anda ingin menggunakan gateway Anda. Kemudian 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, terapkan, dan konfigurasikan mesin virtual gateway menggunakan VMware ESXi.
      - Microsoft Hyper-V — Unduh, gunakan, dan konfigurasikan mesin virtual gateway menggunakan Microsoft Hyper-V.
      - Linux KVM — Download, deploy, dan konfigurasi gateway virtual machine menggunakan Linux Kernel-based Virtual Machine (KVM). Lihat aws-storage-gateway file.xl yang disediakan untuk konfigurasi boot yang disarankan. Mode boot UEFI dengan boot aman dinonaktifkan (loader_secure=no) diperlukan untuk File Gateway 2.x, Volume Gateway 3.x, dan Tape Gateway 3.x.
      - Nutanix AHV — Download, deploy, dan konfigurasi gateway virtual machine menggunakan Linux Kernel-based Virtual Machine (KVM). Gambar yang sama berfungsi untuk lingkungan hypervisor Linux KVM dan Nutanix AHV.

- Amazon EC2 — Konfigurasikan dan luncurkan instans Amazon EC2 untuk meng-host gateway Anda.
- 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. Sekarang gateway Anda sudah diatur, Anda harus memilih bagaimana Anda ingin terhubung dan berkomunikasi dengannya AWS. Pilih Berikutnya untuk melanjutkan.

Hubungkan Gateway File Amazon S3 Anda ke AWS

Untuk menghubungkan S3 File Gateway baru ke AWS

1. Jika Anda belum melakukannya, selesaikan prosedur yang dijelaskan di Siapkan Gateway File Amazon S3. Setelah selesai, pilih Berikutnya untuk membuka AWS halaman Connect to di AWS Storage Gateway konsol.
2. Di bagian Opsi koneksi Gateway, untuk opsi Koneksi, pilih cara mengidentifikasi gateway Anda AWS. Anda dapat memilih dari opsi berikut:

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

     Anda dapat memperoleh alamat IP gateway dengan masuk ke konsol lokal gateway dari klien hypervisor Anda, atau dengan menyalinnya dari halaman detail instans Amazon EC2 Anda. Untuk informasi selengkapnya, lihat Mendapatkan alamat IP gateway.
   - Kunci aktivasi — Berikan kunci aktivasi untuk gateway Anda di bidang yang sesuai. Anda dapat membuat kunci aktivasi menggunakan konsol lokal gateway. Jika alamat IP gateway Anda tidak tersedia, pilih opsi ini.

3. Di bagian opsi Endpoint, lakukan hal berikut:

   a. 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 AWS Storage Gateway titik akhir dan kuota di. Referensi Umum AWS

- VPC Hosted — Gateway Anda berkomunikasi dengan AWS melalui koneksi pribadi dengan virtual private cloud (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 daftar tarik-turun. Anda juga dapat memberikan nama atau alamat IP VPC endpoint Domain Name System (DNS).

  > **Note**
  >
  > Untuk menentukan titik akhir VPC yang dimiliki Akun AWS selain yang saat ini Anda gunakan untuk membuat gateway, Anda harus memberikan nama DNS atau alamat IP-nya.

b. Untuk versi IP, pilih versi protokol dan titik akhir yang akan digunakan gateway Anda untuk berkomunikasi AWS.

> **Note**
>
> Alamat IP gateway Anda harus sesuai dengan versi IP yang Anda tentukan di sini. Dual-stack endpoint menerima IPv4 dan IPv6 koneksi, tetapi mereka hanya berkomunikasi dengan gateway Anda menggunakan versi IP yang Anda pilih.

4. Sekarang setelah Anda memilih bagaimana Anda ingin gateway Anda terhubung AWS, Anda harus mengaktifkan gateway. Pilih Berikutnya untuk melanjutkan.

Tinjau pengaturan dan aktifkan Gateway File Amazon S3 Anda

Untuk meninjau pengaturan dan mengaktifkan S3 File Gateway baru

1. Jika Anda belum melakukannya, lengkapi prosedur yang dijelaskan dalam topik berikut:

   - Menyiapkan Gateway File Amazon S3
   - Hubungkan Gateway File Amazon S3 Anda ke AWS

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

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

4. Sekarang setelah Anda mengaktifkan gateway Anda, Anda harus melakukan konfigurasi pertama kali untuk mengalokasikan disk penyimpanan lokal dan mengonfigurasi logging. Pilih Berikutnya untuk melanjutkan.

Mengonfigurasikan Gateway File Amazon S3

Untuk melakukan konfigurasi pertama kali pada S3 File Gateway baru

1. Jika Anda belum melakukannya, lengkapi prosedur yang dijelaskan dalam topik berikut:

   - Menyiapkan Gateway File Amazon S3
   - Hubungkan Gateway File Amazon S3 Anda ke AWS
   - Tinjau pengaturan dan aktifkan Gateway File Amazon S3 Anda

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

2. Di bagian Konfigurasi penyimpanan, gunakan daftar dropdown untuk mengalokasikan setidaknya satu disk lokal dengan setidaknya 150 gibibytes (GiB) kapasitas ke Cache. 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 daftar dropdown 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 Anda 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.
   - Tidak ada 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 di halaman daftar di konsol. AWS Storage Gateway Ulangi langkah ini untuk menambahkan tag sebanyak yang Anda butuhkan.

6. (Opsional) Di bagian Verifikasi Ketersediaan VMware Tinggi konfigurasi, jika gateway Anda diterapkan pada VMware host yang merupakan bagian dari klaster Ketersediaan VMware Tinggi (HA), pilih Verifikasi VMware HA untuk menguji apakah konfigurasi HA berfungsi dengan baik.

   > **Note**
   >
   > Bagian ini hanya muncul untuk gateway yang berjalan di platform VMware host.

Langkah ini tidak diperlukan untuk menyelesaikan proses konfigurasi gateway. Anda dapat menguji konfigurasi HA gateway Anda kapan saja. Verifikasi membutuhkan waktu beberapa menit, dan reboot mesin virtual Storage Gateway (VM).

7. Pilih Konfigurasi untuk menyelesaikan pembuatan gateway Anda.

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

Sekarang setelah Anda membuat gateway, Anda harus membuat file share agar dapat digunakan. Untuk petunjuk, lihat Membuat berbagi file.

Mengaktifkan gateway 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 mengonfigurasinya untuk 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 buat titik akhir VPC untuk Storage Gateway dan mengaktifkan gateway. Untuk informasi selengkapnya, lihat Menyambungkan Gateway File Amazon S3 untuk AWS Menyambungkan Gateway FSx Anda. AWS

Untuk mengonfigurasi Gateway File S3 Anda untuk mentransfer data melalui VPC, Anda harus membuat titik akhir VPC terpisah untuk Amazon S3, lalu tentukan titik akhir VPC ini saat Anda membuat berbagi file untuk gateway.

> **Note**
>
> Anda harus mengaktifkan gateway Anda di wilayah yang sama di mana Anda membuat titik akhir VPC untuk Storage Gateway, dan penyimpanan Amazon S3 yang Anda konfigurasikan

untuk berbagi file harus berada di wilayah yang sama tempat Anda membuat titik akhir VPC untuk Amazon S3.

Buat titik akhir 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 membuat titik akhir VPC untuk Storage Gateway

1. Masuk ke Konsol Manajemen AWS 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 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 akan terlihat mirip

dengan contoh berikut: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Sekarang setelah Anda memiliki titik akhir VPC, Anda dapat membuat dan mengaktifkan gateway Anda. Untuk informasi selengkapnya, lihat Membuat dan mengaktifkan Amazon S3 File Gateway Gateway.

Untuk informasi tentang mendapatkan kunci aktivasi, lihat Mendapatkan kunci aktivasi untuk gateway Anda .

> **Important**
>
> Untuk mengonfigurasi Gateway File S3 Anda untuk mentransfer data melalui VPC, Anda harus membuat titik akhir VPC terpisah untuk Amazon S3, lalu tentukan titik akhir VPC ini saat Anda membuat berbagi file untuk gateway.
> Untuk melakukannya, ikuti langkah yang sama seperti yang ditunjukkan di atas, tetapi pilih `com.amazonaws.region.s3` untuk Nama Layanan, lalu pilih tabel rute yang Anda inginkan terkait dengan titik akhir S3, bukan grup. subnet/security Untuk petunjuk, lihat Membuat titik akhir gateway.

Membuat berbagi file

Di bagian ini, Anda dapat menemukan petunjuk tentang cara membuat file share yang dapat diakses menggunakan Network File System (NFS) atau protokol Server Message Block (SMB).

Saat Anda membuat berbagi NFS, siapa pun yang memiliki akses ke server NFS dapat mengakses berbagi file NFS secara default. Anda dapat membatasi akses ke klien berdasarkan alamat IP.

Saat Anda membuat berbagi file SMB, Anda dapat menggunakan salah satu dari tiga mode otentikasi:

- Berbagi file dengan akses Microsoft Active Directory (AD). Setiap pengguna Microsoft AD yang diautentikasi mendapatkan akses ke jenis berbagi file ini.
- Berbagi file SMB dengan akses terbatas. Hanya pengguna dan grup domain tertentu yang Anda tentukan yang diizinkan mengakses (melalui daftar izinkan). Pengguna dan grup juga dapat ditolak aksesnya (melalui daftar penolakan).
- Berbagi file SMB dengan akses tamu. Setiap pengguna yang dapat memberikan kata sandi tamu memiliki akses ke berbagi file ini.

> **Note**
>
> Berbagi file yang diekspor melalui gateway untuk berbagi file NFS mendukung izin POSIX. Untuk berbagi file SMB, Anda dapat menggunakan daftar kontrol akses (ACL) untuk mengelola izin pada file dan folder dalam berbagi file Anda. Untuk informasi selengkapnya, lihat Menggunakan Windows ACL untuk membatasi akses berbagi file SMB.

File Gateway dapat meng-host satu atau beberapa file share dari berbagai jenis. Anda dapat memiliki beberapa berbagi file NFS dan SMB di File Gateway.

> **Important**
>
> Untuk membuat file share, File Gateway mengharuskan Anda untuk mengaktifkan AWS Security Token Service (AWS STS). Jika AWS STS tidak diaktifkan di Wilayah AWS tempat Anda membuat File Gateway, aktifkan. Untuk informasi tentang cara mengaktifkanAWS STS, lihat Mengaktifkan dan menonaktifkan AWS Security Token Service di AWS Wilayah di Panduan Pengguna. AWS Identity and Access Management

Topik

Menghindari biaya yang tidak terduga saat mengunggah data gateway

Ketika file ditulis ke File Gateway oleh klien NFS, File Gateway mengunggah data file ke Amazon S3 diikuti oleh metadata-nya. Mengunggah data file membuat objek S3, dan mengunggah metadata untuk file memperbarui metadata untuk objek S3. Proses ini menciptakan versi tambahan dari objek. Jika versi S3 diaktifkan, kedua versi disimpan.

Jika Anda mengubah metadata file yang disimpan di File Gateway Anda, objek S3 baru akan dibuat dan menggantikan objek S3 yang ada. Perilaku ini berbeda dengan mengedit file dalam sistem file, di mana mengedit file tidak menghasilkan file baru yang dibuat. Uji semua operasi file yang Anda rencanakan untuk digunakan dengan AWS Storage Gateway sehingga Anda memahami bagaimana setiap operasi file berinteraksi dengan penyimpanan Amazon S3.

Pertimbangkan dengan cermat penggunaan versi dan Cross-Region replikasi S3 (CRR) di Amazon S3 saat Anda mengunggah data dari Gateway File Anda. Mengunggah file dari File Gateway Anda ke Amazon S3 saat versi S3 diaktifkan biasanya menghasilkan lebih dari satu versi objek S3.

Alur kerja tertentu yang melibatkan file besar dan pola penulisan file seperti unggahan file yang dilakukan dalam beberapa langkah dapat meningkatkan jumlah versi objek S3 yang disimpan. Jika cache File Gateway perlu mengosongkan ruang karena tingkat penulisan file yang tinggi, beberapa versi objek S3 mungkin dibuat. Skenario ini meningkatkan penyimpanan S3 jika Versi S3 dihidupkan dan meningkatkan biaya transfer yang terkait dengan CRR. Uji semua operasi file yang Anda rencanakan untuk digunakan dengan Storage Gateway sehingga Anda memahami bagaimana setiap operasi file berinteraksi dengan penyimpanan Amazon S3.

Menggunakan utilitas Rsync dengan File Gateway Anda menghasilkan pembuatan file sementara dalam cache dan pembuatan objek S3 sementara di Amazon S3. Situasi ini menghasilkan biaya penghapusan awal di kelas penyimpanan S3 Standard-Infrequent Access (S3 Standard-IA).

Enkripsi objek yang disimpan oleh File Gateway di Amazon S3

S3 File Gateway mendukung metode enkripsi sisi server berikut untuk data yang disimpan di Amazon S3:

- SSE-S3— Secara default, semua objek baru yang diunggah ke bucket Amazon S3 menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3. Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- SSE-KMS— Anda dapat mengonfigurasi berbagi file Anda untuk menggunakan enkripsi sisi server dengan AWS Key Management Service (AWS KMS) kunci terkelola. AWS KMSadalah layanan yang menggabungkan perangkat keras dan perangkat lunak yang aman dan sangat tersedia untuk menyediakan sistem manajemen kunci yang diskalakan untuk cloud. Untuk informasi selengkapnya, lihat Apa itu Layanan Manajemen AWS Kunci? di Panduan AWS Key Management Service Pengembang.
- DSSE-KMS— enkripsi Dual-layer sisi server dengan AWS KMS kunci menerapkan dua lapisan enkripsi ke objek saat diunggah ke Amazon S3. Ini membantu memenuhi standar kepatuhan untuk enkripsi multilayer. Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dua lapis dengan kunci AWS KMS di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

> **Note**
>
> Ada biaya tambahan untuk menggunakan DSSE-KMS dan AWS KMS kunci. Untuk informasi selengkapnya, lihat harga AWS KMS.

Anda dapat menentukan metode enkripsi saat membuat berbagi file baru dengan menggunakan konsol Storage Gateway atau Storage Gateway API. Untuk prosedur konsol, lihat Buat berbagi file NFS dengan konfigurasi khusus ataуBuat berbagi file SMB dengan konfigurasi khusus. Untuk informasi tentang perintah API terkait, lihat CreateNFSFileShareatau CreateSMBFileSharedi Referensi API AWS Storage Gateway.

Anda juga dapat memperbarui pengaturan enkripsi untuk berbagi file yang ada menggunakan konsol Storage Gateway, atau Storage Gateway API. Untuk prosedur konsol, lihatUbah metode enkripsi sisi server untuk berbagi file yang ada. Untuk informasi tentang perintah API terkait, lihat UpdateNFSFileShareatau UpdateSMBFileSharedi Referensi API AWS Storage Gateway.

> **Note**
>
> Setelah Anda memperbarui metode enkripsi, gateway menggunakan metode baru untuk semua objek baru yang dibuatnya di Amazon S3 dan untuk objek tersimpan yang diperbarui atau dimodifikasi di masa mendatang. Objek Amazon S3 yang ada hanya akan menerima metode enkripsi baru jika diperbarui atau dimodifikasi oleh gateway.

> **Important**
>
> Pastikan file share Anda menggunakan jenis enkripsi yang sama dengan bucket Amazon S3 tempat menyimpan data Anda.
> Jika Anda mengonfigurasi File Gateway untuk digunakan SSE-KMS atau DSSE-KMS untuk enkripsi, Anda harus menambahkan`kms:Encrypt`,,`kms:Decrypt`,`kms:ReEncrypt*`,`kms:GenerateDataKey`, dan `kms:DescribeKey` izin secara manual ke peran IAM yang terkait dengan berbagi file. Untuk informasi selengkapnya, lihat Menggunakan Identity-Based Kebijakan (Kebijakan IAM) untuk Storage Gateway.

Buat berbagi file NFS

Protokol Network File System (NFS) adalah protokol berbagi file stateful untuk sistem berbasis Unix. Ketika klien berkemampuan NFS dan server NFS berkomunikasi, klien meminta file atau direktori dari server menggunakan panggilan prosedur jarak jauh (RPC). Server memverifikasi bahwa file atau direktori tersedia dan klien memiliki izin akses yang diperlukan. Server kemudian memasang file atau direktori dari jarak jauh pada klien dan berbagi akses melalui koneksi virtual. Untuk operasi klien, NFS menggunakan file server jarak jauh mirip dengan mengakses file lokal.

> **Note**
>
> Protokol NFS mendukung maksimal 16 grup per pengguna. Pengguna mungkin mengalami masalah saat memasang berbagi file NFS jika mereka termasuk dalam lebih dari 16 grup. Untuk menghindari masalah yang meningkat, pastikan bahwa pengguna adalah anggota dari 16 grup atau lebih sedikit saat mengakses berbagi file NFS.

Topik berikut menjelaskan berbagai metode untuk membuat berbagi file NFS untuk File Gateway Anda:

Daftar Isi

Buat berbagi file NFS menggunakan konfigurasi default

Bagian ini menjelaskan cara membuat file share Network File System (NFS) baru menggunakan pengaturan default yang telah dikonfigurasi sebelumnya. Gunakan metode ini untuk penerapan dasar, penggunaan pribadi, pengujian, atau sebagai cara untuk menyebarkan beberapa berbagi file dengan cepat yang akan Anda edit dan sesuaikan nanti. Untuk daftar pengaturan default untuk berbagi file yang Anda buat menggunakan prosedur ini, lihat Pengaturan konfigurasi default untuk berbagi file NFS. Jika Anda memerlukan kontrol yang lebih terperinci atau ingin menggunakan pengaturan lanjutan untuk berbagi file, lihat Membuat berbagi file NFS menggunakan konfigurasi kustom.

> **Note**
>
> Jika Anda perlu menghubungkan berbagi file Anda ke Amazon S3 melalui Virtual Private Cloud (VPC), Anda harus mengikuti prosedur konfigurasi khusus. Anda tidak dapat mengedit pengaturan VPC untuk berbagi file setelah Anda membuatnya.

> **Important**
>
> Menggunakan Versi S3, Replikasi Lintas Wilayah, atau utilitas Rsync saat mengunggah data dari File Gateway dapat memiliki implikasi biaya yang signifikan. Untuk informasi selengkapnya, lihat Menghindari biaya yang tidak terduga saat mengunggah data dari File Gateway.

Untuk membuat berbagi file NFS menggunakan konfigurasi default:

1. Buka konsol AWS Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah/ dan pilih Berbagi file dari panel navigasi kiri.
2. Pilih Buat berbagi file.
3. Untuk Gateway, pilih Gateway File Amazon S3 Anda dari daftar.
4. Untuk protokol berbagi file, pilih NFS.
5. Untuk bucket S3, lakukan salah satu hal berikut:

   - Pilih bucket Amazon S3 yang ada di akun Anda dari daftar tarik-turun.
   - Pilih Bucket di akun lain dari daftar dropdown, lalu masukkan nama bucket di Cross-account bucket name.
   - Pilih Buat bucket S3 baru, lalu pilih Wilayah AWS tempat endpoint Amazon S3 untuk bucket baru Anda berada, dan masukkan nama bucket S3 yang unik. Pilih Buat ember S3 setelah selesai.

     Untuk informasi tentang membuat bucket baru, lihat Bagaimana cara membuat bucket S3? di Panduan Pengguna Amazon S3.

   > **Note**
   >
   > S3 File Gateway tidak mendukung bucket Amazon S3 dengan period `.` () dalam nama bucket.
   > Pastikan nama bucket Anda sesuai dengan aturan penamaan bucket di Amazon S3. Untuk informasi selengkapnya, lihat Aturan untuk penamaan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

6. Tinjau pengaturan di bawah Konfigurasi default, lalu pilih Buat berbagi file untuk membuat berbagi file NFS baru Anda menggunakan konfigurasi default.

Setelah berbagi file NFS dibuat, Anda dapat melihat pengaturan konfigurasinya di konsol AWS Storage Gateway di tab Rincian berbagi file. Untuk informasi tentang pemasangan berbagi file Anda, lihat Memasang berbagi file NFS Anda di klien Anda.

Pengaturan konfigurasi default untuk berbagi file NFS

Pengaturan berikut berlaku untuk semua berbagi file NFS baru yang Anda buat menggunakan konfigurasi default. Setelah Anda membuat berbagi file, Anda dapat memilihnya dari halaman berbagi File di konsol AWS Storage Gateway untuk melihat detail tentang konfigurasinya.

> **Important**
>
> Konfigurasi berbagi file NFS default menyediakan kontrol file penuh dan izin akses ke pemilik bucket S3 yang dipetakan ke berbagi file, bahkan jika bucket dimiliki oleh akun lain. AWS Untuk informasi selengkapnya tentang menggunakan file share untuk mengakses objek dalam bucket yang dimiliki oleh akun lain, lihatMenggunakan berbagi file untuk akses lintas akun.

Pengaturan	Nilai default	Catatan
Lokasi Amazon S3	Berbagi file terhubung langsung ke bucket Amazon S3 dan memiliki nama yang sama dengan bucket. Gateway Anda menggunakan bucket ini untuk menyimpan dan mengambil file.	Nama tidak termasuk awalan.
AWS PrivateLink untuk S3	Berbagi file tidak terhubung ke Amazon S3 melalui titik akhir antarmuka di cloud pribadi virtual (VPC) Anda.	
Pemberitahuan unggahan file	Mati	
Kelas penyimpanan untuk objek baru	Standar Amazon S3	Ini memungkinkan Anda menyimpan data objek yang sering diakses secara berlebihan di beberapa Availability Zone yang terpisah secara geografis. Untuk

Pengaturan	Nilai default	Catatan
		informasi selengkapnya tentang kelas Amazon S3 Standard penyimpanan, lihat Kelas penyimpanan untuk objek yang sering diakses di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
Enkripsi	Enkripsi sisi server dengan kunci terkelola S3 (SSE-S3)	Semua objek Amazon S3 yang diunggah, diperbarui, atau dimodifikasi oleh Gateway File S3 Anda dienkripsi secara default dengan enkripsi sisi server menggunakan kunci terkelola Amazon S3.

Pengaturan	Nilai default	Catatan
Metadata objek	Tebak tipe MIME	Hal ini memungkinkan Storage Gateway untuk menebak jenis Multipurpose Internet Mail Extension (MIME) untuk objek yang diunggah berdasarkan ekstensi file. Opsi ini mengharuskan Access Control Lists (ACLs) diaktifkan untuk bucket Amazon S3 yang terkait dengan berbagi file Anda. Jika ACLs ada dimatikan, berbagi file tidak dapat mengakses bucket Amazon S3, dan tetap dalam status Tidak Tersedia tanpa batas.
Aktifkan pembayaran pemohon	Mati	Untuk informasi selengkap nya, lihat Pemohon Membayar bucket.
Log audit	Mati	Logging ke Amazon CloudWatch grup dimatikan secara default.

Pengaturan	Nilai default	Catatan
Akses ke bucket S3 Anda	Buat peran IAM baru	Opsi default memungkinkan File Gateway untuk membuat peran dan akses IAM baru kebijakan atas nama Anda. Semua klien NFS diizinkan mengakses. Untuk informasi tentang dukungan Klien NFS, lihatKlien NFS dan SMB yang didukung untuk File Gateway.
Opsi pemasangan	• Tingkat labu - Labu akar • Ekspor sebagai - Baca-tulis	Nilai default tingkat Squash berarti bahwa akses untuk remote superuser (root) dipetakan ke User Identifie r (UID) (65534) dan Group Identifier (GID) (65534).
Default metadata file	• Izin direktori - 0777 • Izin file - 0666 • Pengidentifikasi Pengguna (UID) - 65534 • Pengidentifikasi Grup (GID) - 65534	

Buat berbagi file NFS dengan konfigurasi khusus

Gunakan prosedur berikut untuk membuat berbagi file Network File System (NFS) dengan konfigurasi kustom. Untuk membuat berbagi file NFS menggunakan pengaturan konfigurasi default, lihat Membuat berbagi file NFS menggunakan konfigurasi default.

> **Important**
>
> Menggunakan Versi S3, Replikasi Lintas Wilayah, atau utilitas Rsync saat mengunggah data dari File Gateway dapat memiliki implikasi biaya yang signifikan. Untuk informasi selengkapnya, lihat Menghindari biaya yang tidak terduga saat mengunggah data dari File Gateway.

Untuk membuat berbagi file NFS dengan pengaturan yang disesuaikan

1. Buka konsol AWS Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah/ dan pilih Berbagi file dari panel navigasi kiri.
2. Pilih Buat berbagi file.
3. Pilih Sesuaikan konfigurasi. Anda dapat mengabaikan bidang lain di halaman ini untuk saat ini. Anda akan diminta untuk mengonfigurasi pengaturan gateway, protokol, dan penyimpanan di langkah selanjutnya.
4. Untuk Gateway, pilih Amazon S3 File Gateway untuk berbagi file baru Anda dari daftar dropdown.
5. Untuk grup CloudWatch log, pilih salah satu dari berikut ini dari daftar dropdown:

   - Untuk menonaktifkan logging untuk berbagi file ini, pilih Nonaktifkan logging.
   - Untuk secara otomatis membuat grup log baru untuk berbagi file ini, pilih Dibuat oleh Storage Gateway.
   - Untuk mengirim pemberitahuan kesehatan dan sumber daya untuk berbagi file ini ke grup log yang ada, pilih grup yang diinginkan dari daftar.

   Untuk informasi selengkapnya tentang log audit, lihat Memahami log audit Gateway File S3.
6. (Opsional) Di bawah Tag - Opsional, pilih Tambahkan tag baru, lalu masukkan Kunci dan Nilai untuk berbagi file Anda.

   Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengkategorikan sumber daya Storage Gateway Anda. Menambahkan tag dapat membuat pemfilteran dan pencarian berbagi file Anda lebih mudah. Anda dapat mengulangi langkah ini untuk menambahkan hingga 50 tag.

   Pilih Berikutnya setelah selesai.

7. Untuk bucket S3, lakukan salah satu hal berikut untuk menentukan di mana file share Anda akan menyimpan dan mengambil file:

   - Untuk menghubungkan berbagi file secara langsung ke bucket S3 yang ada di akun Amazon Web Services Anda, pilih nama bucket dari daftar tarik-turun.
   - Untuk menghubungkan berbagi file ke bucket S3 yang ada yang dimiliki oleh akun Amazon Web Services selain akun yang Anda gunakan untuk membuat berbagi file, pilih Bucket di akun lain dari daftar tarik-turun, lalu masukkan nama bucket Cross-account.
   - Untuk menghubungkan berbagi file ke bucket S3 baru, pilih Buat bucket S3 baru, lalu pilih Wilayah tempat titik akhir Amazon S3 untuk bucket baru Anda berada, dan masukkan nama bucket S3 yang unik. Pilih Buat ember S3 setelah selesai. Untuk informasi selengkapnya tentang membuat bucket baru, lihat Bagaimana cara membuat bucket S3? di Panduan Pengguna Amazon S3.
   - Untuk menghubungkan berbagi file ke bucket S3 menggunakan nama titik akses, pilih nama jalur akses Amazon S3 dari daftar tarik-turun, lalu masukkan nama titik akses. Jika Anda perlu membuat titik akses baru, Anda dapat memilih Buat titik akses S3. Untuk petunjuk lebih lanjut, lihat Membuat titik akses di Panduan Pengguna Amazon S3. Untuk informasi selengkapnya tentang titik akses, lihat Mengelola akses data dengan jalur akses Amazon S3 dan Mendelegasikan kontrol akses ke titik akses di Panduan Pengguna Amazon S3.
   - Untuk menghubungkan berbagi file ke bucket S3 menggunakan alias titik akses, pilih alias titik akses Amazon S3 dari daftar tarik-turun, lalu masukkan alias Access point. Jika Anda perlu membuat titik akses baru, Anda dapat memilih Buat titik akses S3. Untuk petunjuk lebih lanjut, lihat Membuat titik akses di Panduan Pengguna Amazon S3. Untuk informasi selengkapnya tentang alias titik akses, lihat Menggunakan alias gaya ember untuk titik akses Anda di Panduan Pengguna Amazon S3.

   > **Note**
   >
   > Setiap berbagi file hanya dapat terhubung ke satu bucket S3, tetapi beberapa berbagi file dapat terhubung ke bucket yang sama. Jika Anda menghubungkan lebih dari satu file share ke bucket yang sama, Anda harus mengonfigurasi setiap file share untuk menggunakan awalan bucket S3 yang unik dan tidak tumpang tindih untuk mencegah konflik. read/write
   >
   > S3 File Gateway tidak mendukung bucket Amazon S3 dengan period `.` () dalam nama bucket.

Pastikan nama bucket Anda sesuai dengan aturan penamaan bucket di Amazon S3. Untuk informasi selengkapnya, lihat Aturan untuk penamaan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

8. (Opsional) Untuk awalan bucket S3, masukkan awalan untuk berbagi file agar diterapkan ke objek yang dibuat di Amazon S3. Awalan adalah cara untuk mengatur data Anda di S3, mirip dengan direktori dalam struktur file tradisional. Untuk informasi selengkapnya, lihat Mengatur objek menggunakan awalan di Panduan Pengguna Amazon S3.

   Note

   - Jika Anda menghubungkan lebih dari satu file share ke bucket yang sama, Anda harus mengonfigurasi setiap file share untuk menggunakan awalan unik yang tidak tumpang tindih untuk mencegah konflik. read/write
   - Prefiks harus diakhiri dengan garis miring ke depan (/).
   - Setelah berbagi file dibuat, awalan tidak dapat diubah atau dihapus.

9. Untuk Wilayah, pilih Wilayah AWS tempat titik akhir S3 untuk bucket Anda berada dari daftar tarik-turun. Bidang ini hanya muncul jika Anda menentukan titik akses atau bucket di akun lain untuk bucket S3.
10. Untuk kelas Storage untuk objek baru, pilih kelas penyimpanan dari daftar dropdown. Untuk informasi selengkapnya tentang kelas penyimpanan, lihat Menggunakan kelas penyimpanan dengan File Gateway.
11. Untuk Peran IAM, lakukan salah satu hal berikut untuk mengonfigurasi peran IAM untuk berbagi file Anda:

    - Untuk secara otomatis membuat peran IAM baru dengan izin yang diperlukan agar berbagi file Anda berfungsi dengan baik, pilih Dibuat oleh Storage Gateway dari daftar tarik-turun.
    - Untuk menggunakan peran IAM yang ada, pilih nama peran dari daftar tarik-turun.
    - Untuk membuat peran IAM baru, pilih Buat peran. Untuk petunjuk lebih lanjut, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan di AWS Identity and Access Management Panduan Pengguna.

    Untuk informasi selengkapnya tentang cara peran IAM mengontrol akses antara berbagi file dan bucket S3, lihat Memberikan akses ke bucket Amazon S3.

12. Untuk tautan Pribadi, lakukan hal berikut hanya jika Anda perlu mengonfigurasi berbagi file Anda untuk berkomunikasi dengan AWS menggunakan titik akhir pribadi di Virtual Private Cloud (VPC). Jika tidak, lewati langkah ini. Untuk informasi lebih lanjut, lihat Apa itu AWS PrivateLink? dalam AWS PrivateLink Guide.

    a. Pilih Gunakan titik akhir VPC.

    b. Untuk Identifikasi titik akhir VPC dengan, lakukan salah satu hal berikut:

    - Pilih ID titik akhir VPC, lalu pilih titik akhir yang ingin Anda gunakan dari daftar dropdown titik akhir VPC.
    - Pilih nama DNS, lalu masukkan nama DNS untuk titik akhir yang ingin Anda gunakan.

13. Untuk Enkripsi, pilih jenis enkripsi sisi server yang akan digunakan oleh file share untuk data yang disimpan di Amazon S3:

- Untuk menggunakan enkripsi sisi server yang dikelola dengan Amazon S3 (SSE-S3), pilih S3-Managed Keys (SSE-S3).

  Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

- Untuk menggunakan enkripsi sisi server yang dikelola dengan AWS Key Management Service (SSE-KMS), pilih KMS-Managed Keys (SSE-KMS). Untuk kunci KMS Primer, pilih kunci AWS KMS yang ada, atau pilih Buat kunci KMS baru untuk membuat kunci KMS baru di konsol Key Management Service (). AWS AWS KMS

  Untuk informasi selengkapnya AWS KMS, lihat Apa itu Layanan Manajemen AWS Kunci? di Panduan AWS Key Management Service Pengembang.

- Untuk menggunakan enkripsi sisi server dual-layer yang dikelola dengan AWS Key Management Service (DSSE-KMS), pilih Enkripsi sisi server dual-layer dengan kunci (DSSE-KMS). AWS Key Management Service Untuk kunci KMS Primer, pilih kunci AWS KMS yang ada, atau pilih Buat kunci KMS baru untuk membuat kunci KMS baru di konsol Key Management Service (). AWS AWS KMS

  Untuk informasi selengkapnya tentang DSSE-KMS, lihat Menggunakan enkripsi sisi server dua lapis dengan AWS KMS kunci di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

> **Note**
>
> Ada biaya tambahan untuk menggunakan DSSE-KMS dan kunci. AWS KMS Untuk informasi selengkapnya, lihat harga AWS KMS.
> Untuk menentukan AWS KMS kunci dengan alias yang tidak terdaftar atau menggunakan AWS KMS kunci dari AWS akun yang berbeda, Anda harus menggunakan. AWS Command Line Interface Tombol KMS asimetris tidak didukung. Untuk informasi selengkapnya, lihat Membuat NFSFile Bagikan di Referensi API AWS Storage Gateway.

> **Important**
>
> Pastikan file share Anda menggunakan jenis enkripsi yang sama dengan bucket Amazon S3 tempat menyimpan data Anda.

14. Untuk tipe Guess MIME, pilih Guess media MIME type untuk memungkinkan Storage Gateway menebak jenis media untuk objek yang diunggah berdasarkan ekstensi file mereka.
15. Untuk nama berbagi file, masukkan nama untuk berbagi file Anda.

> **Note**
>
> Nama berbagi file NFS yang valid hanya dapat berisi karakter berikut: a `-z`, A `0` -Z,,9, `-.`, dan_.

16. Untuk peristiwa Upload, pilih Log peristiwa saat file berhasil diunggah oleh gateway jika Anda ingin gateway merekam peristiwa CloudWatch log saat berhasil mengunggah file ke Amazon S3. Penundaan notifikasi mengontrol penundaan minimum antara operasi penulisan klien terbaru dan pembuatan notifikasi `ObjectUploaded` log. Karena klien dapat membuat banyak penulisan kecil ke file dalam waktu singkat, kami sarankan untuk mengatur parameter ini selama mungkin untuk menghindari menghasilkan beberapa notifikasi untuk file yang sama secara berurutan. Untuk informasi selengkapnya, lihat Mendapatkan notifikasi unggahan file.

> **Note**
>
> Pengaturan ini tidak berpengaruh pada waktu pengunggahan objek ke S3, hanya pada waktu pemberitahuan.

Pengaturan ini tidak dimaksudkan untuk menentukan waktu yang tepat di mana pemberitahuan akan dikirim. Dalam beberapa kasus, gateway mungkin memerlukan lebih dari waktu tunda yang ditentukan untuk menghasilkan dan mengirim pemberitahuan.

Pilih Berikutnya setelah selesai.

17.

18. Untuk protokol berbagi file, pilih NFS.
19. Untuk akses Klien, lakukan salah satu hal berikut untuk menentukan klien NFS mana yang dapat mengakses berbagi file Anda:

    - Untuk menerima semua koneksi klien yang masuk, pilih Semua klien NFS.
    - Untuk menerima koneksi klien yang masuk hanya dari alamat IP tertentu, pilih Klien NFS Spesifik, lalu pilih Tambahkan klien. Untuk klien yang Diizinkan, tentukan alamat IP atau blok CIDR yang valid untuk menerima koneksi. Jika Anda perlu menentukan alamat IP tambahan, pilih Tambahkan klien lain.

    > **Note**
    >
    > Kami merekomendasikan untuk mengonfigurasi pembatasan akses ke berbagi file Anda menggunakan opsi klien NFS Spesifik. Jika tidak, klien mana pun di jaringan Anda dapat memasang ke berbagi file.

20. Untuk tipe Access, pilih salah satu dari berikut ini:

    - Untuk memungkinkan klien membaca dan menulis file pada berbagi file, pilih Baca/Tulis.
    - Untuk memungkinkan klien membaca file tetapi tidak menulis ke berbagi file, pilih Read-only.

    > **Note**
    >
    > Untuk berbagi file yang dipasang pada klien Microsoft Windows, jika Anda memilih Read-only, Anda mungkin melihat pesan tentang kesalahan tak terduga yang mencegah Anda membuat folder. Anda dapat mengabaikan pesan ini.

21. Untuk tingkat Akses, pilih salah satu dari berikut ini:

- Root squash (default): Akses untuk superuser jarak jauh (root) dipetakan ke UID (65534) dan GID (65534).
- Semua squash: Semua akses pengguna dipetakan ke User ID (UID) (65534) dan Group ID (GID) (65534).
- Tanpa root squash: Superuser jarak jauh (root) menerima akses sebagai root.

22. (Opsional) Untuk penyegaran cache otomatis dari S3, pilih Setel interval penyegaran cache, lalu atur waktu dalam Menit atau Hari untuk menyegarkan cache berbagi file menggunakan Time To Live (TTL). TTL adalah lamanya waktu sejak penyegaran terakhir. Setelah interval TTL berlalu, mengakses direktori menyebabkan File Gateway menyegarkan konten direktori itu dari bucket Amazon S3.

    > **Note**
    >
    > Menyetel nilai ini lebih pendek dari 30 menit dapat berdampak negatif pada kinerja gateway dalam situasi di mana sejumlah besar objek Amazon S3 sering dibuat atau dihapus.

23. Untuk default metadata File, pilih Ubah metadata default untuk objek S3 yang tidak dibuat atau dimodifikasi oleh gateway jika Anda ingin gateway menerapkan metadata file (termasuk izin Unix) ke objek yang sudah ada sebelumnya yang ditemukan di bucket S3 Anda. Tentukan Izin direktori, Izin file, ID Pengguna, dan ID Grup yang ingin Anda terapkan di bidang yang sesuai.
24. Untuk kepemilikan dan izin File, pilih Berikan pemilik bucket S3 kepemilikan penuh atas file yang dibuat oleh gateway, termasuk izin baca, tulis, edit, dan hapus jika Anda ingin AWS akun yang memiliki bucket S3 memiliki kontrol penuh atas semua objek yang ditulis ke bucket oleh berbagi file Anda.

    Pilih Berikutnya setelah selesai.
25. Tinjau konfigurasi berbagi file. Pilih Edit untuk mengubah pengaturan untuk bagian mana pun yang ingin Anda ubah. Setelah selesai, pilih Buat.

Setelah berbagi file NFS dibuat, Anda dapat melihat pengaturan konfigurasinya di konsol AWS Storage Gateway di tab Rincian berbagi file. Untuk petunjuk untuk me-mount berbagi file Anda, lihat Memasang berbagi file NFS Anda di klien Anda.

Buat berbagi file SMB

Protokol Server Message Block (SMB) terintegrasi secara mendalam ke dalam rangkaian produk Microsoft Windows, dan tetap menjadi protokol berbagi file default untuk sistem operasi Windows. Proses komunikasi client-server mirip dengan NFS pada tingkat tinggi, tetapi ada perbedaan dalam beberapa detail dan mekanisme operasional. Misalnya, di SMB, sistem file tidak dipasang pada klien SMB lokal. Sebaliknya, berbagi jaringan yang dihosting di server SMB diakses melalui jalur jaringan.

Topik di bagian ini menjelaskan berbagai metode untuk membuat berbagi file SMB untuk File Gateway Anda.

Daftar Isi

Buat berbagi file SMB menggunakan konfigurasi default

Bagian ini menjelaskan cara membuat file share Server Message Block (SMB) baru menggunakan pengaturan default yang telah dikonfigurasi sebelumnya. Gunakan metode ini untuk penerapan dasar, penggunaan pribadi, pengujian, atau sebagai cara untuk menyebarkan beberapa berbagi file dengan cepat yang akan Anda edit dan sesuaikan nanti. Untuk daftar pengaturan default untuk berbagi file yang Anda buat menggunakan prosedur ini, lihat Pengaturan konfigurasi default untuk berbagi file SMB. Jika Anda memerlukan kontrol yang lebih terperinci atau ingin menggunakan pengaturan lanjutan untuk berbagi file, lihat Membuat berbagi file SMB dengan konfigurasi khusus.

> **Note**
>
> Jika Anda perlu menghubungkan berbagi file Anda ke Amazon S3 melalui Virtual Private Cloud (VPC), Anda harus mengikuti prosedur konfigurasi khusus. Anda tidak dapat mengedit pengaturan VPC untuk berbagi file setelah Anda membuatnya.

> **Important**
>
> Menggunakan Versi S3, Replikasi Lintas Wilayah, atau utilitas Rsync saat mengunggah data dari File Gateway dapat memiliki implikasi biaya yang signifikan. Untuk informasi

selengkapnya, lihat Menghindari biaya yang tidak terduga saat mengunggah data dari File Gateway.

Prasyarat

Sebelum Anda membuat file share, lakukan hal berikut:

- Konfigurasikan pengaturan keamanan SMB untuk File Gateway Anda. Untuk petunjuk, lihat Menyetel tingkat keamanan untuk gateway Anda.
- Konfigurasikan Microsoft Active Directory atau akses tamu untuk otentikasi. Untuk petunjuk, lihat Menggunakan Active Directory untuk mengautentikasi pengguna atau Menyediakan akses tamu ke berbagi file Anda.
- Pastikan port yang diperlukan terbuka di grup keamanan Anda. Untuk informasi selengkapnya, lihat Persyaratan Port.

Untuk membuat berbagi file SMB menggunakan konfigurasi default:

1. Buka konsol AWS Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah/ dan pilih Berbagi file dari panel navigasi kiri.
2. Pilih Buat berbagi file.
3. Untuk Gateway, pilih Amazon S3 File Gateway dari daftar dropdown.
4. Untuk protokol berbagi file, pilih SMB.
5. Untuk bucket S3, lakukan salah satu hal berikut:
   - Pilih bucket Amazon S3 yang ada di akun Anda dari daftar tarik-turun.
   - Pilih Bucket di akun lain dari daftar dropdown, lalu masukkan nama bucket di Cross-account bucket name.
   - Pilih Buat bucket S3 baru, lalu pilih Wilayah AWS tempat endpoint Amazon S3 untuk bucket baru Anda berada, dan masukkan nama bucket S3 yang unik. Pilih Buat ember S3 setelah selesai.

     Untuk informasi tentang membuat bucket baru, lihat Bagaimana cara membuat bucket S3? di Panduan Pengguna Amazon S3.

> **Note**
>
> S3 File Gateway tidak mendukung bucket Amazon S3 dengan period `.` () dalam nama bucket.
> Pastikan nama bucket Anda sesuai dengan aturan penamaan bucket di Amazon S3. Untuk informasi selengkapnya, lihat Aturan untuk penamaan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

6. Otentikasi pengguna, pilih metode otentikasi yang ingin Anda gunakan dari daftar dropdown:

   - Untuk menggunakan Microsoft Active Directory perusahaan Anda atau AWS Managed Microsoft AD untuk mengautentikasi akses pengguna ke berbagi file SMB Anda, pilih Active Directory. Gateway Anda harus bergabung dengan domain untuk menggunakan metode ini. Untuk informasi selengkapnya, lihat Menggunakan Active Directory untuk mengautentikasi pengguna.

     > **Note**
     >
     > Untuk menggunakan AWS Managed Microsoft AD gateway Amazon EC2, Anda harus membuat instans Amazon EC2 di VPC yang sama dengan, menambahkan `_workspaceMembers` grup keamanan ke instans Amazon EC2, dan bergabung dengan domain AD menggunakan kredensi Admin dari. AWS Managed Microsoft AD AWS Managed Microsoft AD
     > Untuk informasi selengkapnya AWS Managed Microsoft AD, lihat Panduan AWS Directory Service Administrasi.
     > Untuk informasi selengkapnya tentang Amazon EC2, lihat Dokumentasi Amazon Elastic Compute Cloud.

     Jika status Gabung menunjukkan bahwa gateway Anda sudah bergabung ke domain Active Directory, lanjutkan ke langkah berikutnya. Jika tidak, lakukan tindakan berikut:

     1. Pilih Konfigurasikan
     2. Untuk Domain, masukkan nama domain Active Directory yang Anda inginkan untuk bergabung dengan gateway Anda.

3. Masukkan Nama Pengguna dan Kata Sandi yang akan digunakan gateway untuk bergabung dengan domain.
4. (Opsional) Untuk unit Organisasi (OU), masukkan OU yang ditunjuk yang digunakan Direktori Aktif Anda untuk objek komputer baru.
5. (Opsional) Untuk pengontrol Domain (DC), masukkan nama DC di mana gateway Anda akan terhubung ke Active Directory. Anda dapat membiarkan bidang ini kosong untuk memungkinkan DNS memilih DC secara otomatis.
6. Pilih Gabung Direktori Aktif.

> **Note**
>
> Bergabung dengan domain akan membuat akun Active Directory di container default (yang bukan unit organisasi) menggunakan ID Gateway sebagai nama akun (misalnya, SGW-1234ADE). Tidak mungkin untuk menyesuaikan nama akun ini.
> Jika lingkungan Active Directory Anda mengharuskan Anda melakukan pra-tahap akun untuk memfasilitasi proses penggabungan domain, Anda harus membuat akun ini sebelumnya.
> Jika lingkungan Active Directory Anda memiliki OU yang ditunjuk untuk objek komputer baru, Anda harus menentukan OU tersebut saat bergabung dengan domain.

- Untuk memberikan akses yang dilindungi kata sandi kepada siapa saja yang memberikan kata sandi tamu yang Anda konfigurasikan, pilih Akses tamu. File Gateway Anda tidak perlu menjadi bagian dari domain Microsoft Active Directory untuk menggunakan metode ini. Pilih Konfigurasi untuk menentukan kata sandi Tamu Anda, lalu pilih Simpan.

7. Tinjau pengaturan di bawah Konfigurasi default, lalu pilih Buat berbagi file untuk membuat berbagi file SMB baru Anda menggunakan konfigurasi default.

Setelah berbagi file SMB dibuat, Anda dapat melihat pengaturan konfigurasinya di konsol AWS Storage Gateway di tab Rincian berbagi file. Untuk informasi tentang pemasangan berbagi file Anda, lihat Memasang berbagi file SMB Anda di klien Anda.

Pengaturan konfigurasi default untuk berbagi file SMB

Pengaturan berikut berlaku untuk semua berbagi file SMB baru yang Anda buat menggunakan konfigurasi default. Setelah Anda membuat berbagi file, Anda dapat memilihnya dari halaman berbagi File di konsol AWS Storage Gateway untuk melihat detail tentang konfigurasinya.

> **Important**
>
> Konfigurasi berbagi file SMB default menyediakan kontrol file penuh dan izin akses kepada pemilik bucket S3 yang dipetakan ke berbagi file, meskipun bucket dimiliki oleh akun Amazon Web Services yang berbeda. Untuk informasi selengkapnya tentang menggunakan berbagi file untuk mengakses objek dalam bucket yang dimiliki oleh akun lain, lihat Menggunakan berbagi file untuk akses lintas akun.

Pengaturan	Nilai default	Catatan
Lokasi Amazon S3	Berbagi file terhubung langsung ke bucket Amazon S3 dan memiliki nama yang sama dengan bucket. Gateway Anda menggunakan bucket ini untuk menyimpan dan mengambil file.	Nama tidak termasuk awalan.
AWS PrivateLink untuk S3	Berbagi file tidak terhubung ke Amazon S3 melalui titik akhir antarmuka di cloud pribadi virtual (VPC) Anda.	
Pemberitahuan unggahan file	Mati	
Kelas penyimpanan untuk objek baru	Amazon S3 Standard	Ini memungkinkan Anda menyimpan data objek yang sering diakses secara berlebihan di beberapa Availability Zone yang terpisah secara geografis. Untuk informasi selengkapnya tentang kelas Amazon S3 Standard penyimpanan, lihat Kelas penyimpanan untuk objek yang sering diakses di

Pengaturan	Nilai default	Catatan
		Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
Enkripsi	Enkripsi sisi server dengan kunci terkelola S3 (SSE-S3)	Semua objek Amazon S3 yang diunggah, diperbarui, atau dimodifikasi oleh Gateway File S3 Anda dienkripsi secara default dengan enkripsi sisi server menggunakan kunci terkelola Amazon S3.
Metadata objek	Tebak tipe MIME	Hal ini memungkinkan Storage Gateway untuk menebak jenis Multipurpose Internet Mail Extension (MIME) untuk objek yang diunggah berdasarkan ekstensi file. Opsi ini mengharuskan Access Control Lists (ACLs) diaktifkan untuk bucket Amazon S3 yang terkait dengan berbagi file Anda. Jika ACLs ada dimatikan, berbagi file tidak dapat mengakses bucket Amazon S3, dan tetap dalam status Tidak Tersedia tanpa batas.

Pengaturan	Nilai default	Catatan
Pencacahan berbasis akses	Tidak diaktifkan	File dan folder pada berbagi file terlihat oleh semua pengguna selama pencacahan direktori. Pencacahan berbasis akses adalah sistem yang menyaring pencacahan file dan folder pada berbagi file SMB berdasarkan akses berbagi daftar kontrol (ACLs).
Aktifkan pembayaran pemohon	Mati	Untuk informasi selengkapnya, lihat Pemohon Membayar bucket.
Penguncian oportunistik	Pada	Ini memungkinkan berbagi file menggunakan penguncian oportunistik untuk mengoptimalkan strategi buffering file. Dalam kebanyakan kasus, mengaktifkan penguncian oportunistik meningkat kinerja, terutama yang berkaitan dengan konteks Windows menu.
Log audit	Mati	Logging ke Amazon CloudWatch grup dimatikan secara default.
Sensitivitas kasus paksa	Mati	Ini memungkinkan klien untuk mengontrol sensitivitas kasus.

Pengaturan	Nilai default	Catatan
Akses ke bucket S3 Anda	Buat peran IAM baru	Opsi default memungkinkan File Gateway untuk membuat peran dan akses IAM baru kebijakan atas nama Anda.

Buat berbagi file SMB dengan konfigurasi khusus

Gunakan prosedur berikut untuk membuat file share Server Message Block (SMB) dengan konfigurasi kustom. Untuk membuat berbagi file SMB menggunakan pengaturan konfigurasi default, lihat Membuat berbagi file SMB menggunakan konfigurasi default.

> **Important**
>
> Menggunakan Versi S3, Replikasi Lintas Wilayah, atau utilitas Rsync saat mengunggah data dari File Gateway dapat memiliki implikasi biaya yang signifikan. Untuk informasi selengkapnya, lihat Menghindari biaya yang tidak terduga saat mengunggah data dari File Gateway.

Prasyarat

Sebelum Anda membuat file share Anda, lakukan hal berikut:

- Konfigurasikan pengaturan keamanan SMB untuk File Gateway Anda. Untuk petunjuk, lihat Menyetel tingkat keamanan untuk gateway Anda.
- Konfigurasikan Microsoft Active Directory atau akses tamu untuk otentikasi. Untuk petunjuk, lihat Menggunakan Active Directory untuk mengautentikasi pengguna atau Menyediakan akses tamu ke berbagi file Anda.
- Pastikan port yang diperlukan terbuka di grup keamanan Anda. Untuk informasi selengkapnya, lihat Persyaratan Port.

Untuk membuat berbagi file SMB dengan pengaturan yang disesuaikan

1. Buka konsol AWS Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah/ dan pilih Berbagi file dari panel navigasi kiri.
2. Pilih Buat berbagi file.
3. Pilih Sesuaikan konfigurasi. Anda dapat mengabaikan bidang lain di halaman ini untuk saat ini. Anda akan diminta untuk mengonfigurasi pengaturan gateway, protokol, dan penyimpanan di langkah selanjutnya.
4. Untuk Gateway, pilih Amazon S3 File Gateway dari daftar dropdown.
5. Untuk grup CloudWatch log, pilih salah satu dari berikut ini dari daftar dropdown:

   - Untuk menonaktifkan pencatatan untuk berbagi file ini, pilih Nonaktifkan logging.
   - Untuk secara otomatis membuat grup log baru untuk berbagi file ini, pilih Dibuat oleh Storage Gateway.
   - Untuk mengirim pemberitahuan kesehatan dan sumber daya untuk berbagi file ini ke grup log yang ada, pilih grup yang diinginkan dari daftar.

   Untuk informasi selengkapnya tentang log audit, lihat Memahami log audit Gateway File S3.
6. (Opsional) Di bawah Tag - Opsional, pilih Tambahkan tag baru, lalu masukkan Kunci dan Nilai untuk berbagi file Anda. Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengkategorikan sumber daya Storage Gateway Anda. Menambahkan tag dapat membuat pemfilteran dan pencarian berbagi file Anda lebih mudah. Anda dapat mengulangi langkah ini untuk menambahkan hingga 50 tag.

   Pilih Berikutnya setelah selesai.
7. Untuk bucket S3, lakukan salah satu hal berikut untuk menentukan tempat menyimpan dan mengambil file:

   - Untuk menghubungkan berbagi file secara langsung ke bucket S3 yang ada di akun Amazon Web Services Anda, pilih nama bucket dari daftar tarik-turun.
   - Untuk menghubungkan berbagi file ke bucket S3 yang ada yang dimiliki oleh akun Amazon Web Services selain yang Anda gunakan untuk membuat berbagi file, pilih Bucket di akun lain dari daftar tarik-turun, lalu masukkan nama bucket Cross-account.
   - Untuk menghubungkan berbagi file ke bucket S3 baru, pilih Buat bucket S3 baru, lalu pilih Wilayah tempat titik akhir Amazon S3 untuk bucket baru Anda berada, dan masukkan nama

bucket S3 yang unik. Pilih Buat ember S3 setelah selesai. Untuk informasi selengkapnya tentang membuat bucket baru, lihat Bagaimana cara membuat bucket S3? di Panduan Pengguna Amazon S3.

- Untuk menghubungkan berbagi file ke bucket S3 menggunakan nama titik akses, pilih nama jalur akses Amazon S3 dari daftar tarik-turun, lalu masukkan nama titik akses. Jika Anda perlu membuat titik akses baru, Anda dapat memilih Buat titik akses S3. Untuk petunjuk lebih lanjut, lihat Membuat titik akses di Panduan Pengguna Amazon S3. Untuk informasi selengkapnya tentang titik akses, lihat Mengelola akses data dengan jalur akses Amazon S3 dan Mendelegasikan kontrol akses ke titik akses di Panduan Pengguna Amazon S3.
- Untuk menghubungkan berbagi file ke bucket S3 menggunakan alias titik akses, pilih alias titik akses Amazon S3 dari daftar tarik-turun, lalu masukkan alias Access point. Jika Anda perlu membuat titik akses baru, Anda dapat memilih Buat titik akses S3. Untuk petunjuk lebih lanjut, lihat Membuat titik akses di Panduan Pengguna Amazon S3. Untuk informasi selengkapnya tentang alias titik akses, lihat Menggunakan alias gaya ember untuk titik akses Anda di Panduan Pengguna Amazon S3.

> **Note**
>
> Setiap berbagi file hanya dapat terhubung ke satu bucket S3, tetapi beberapa berbagi file dapat terhubung ke bucket yang sama. Jika Anda menghubungkan lebih dari satu file share ke bucket yang sama, Anda harus mengonfigurasi setiap file share untuk menggunakan awalan bucket S3 yang unik dan tidak tumpang tindih untuk mencegah konflik. read/write
> S3 File Gateway tidak mendukung bucket Amazon S3 dengan period `.` () dalam nama bucket.
> Pastikan nama bucket Anda sesuai dengan aturan penamaan bucket di Amazon S3. Untuk informasi selengkapnya, lihat Aturan untuk penamaan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

8. (Opsional) Untuk awalan bucket S3, masukkan awalan untuk berbagi file agar diterapkan ke objek yang dibuat di Amazon S3. Awalan adalah cara untuk mengatur data Anda di S3, mirip dengan direktori dalam struktur file tradisional. Untuk informasi selengkapnya, lihat Mengatur objek menggunakan awalan di Panduan Pengguna Amazon S3.

> **Note**
>
> - Jika Anda menghubungkan lebih dari satu file share ke bucket yang sama, Anda harus mengonfigurasi setiap file share untuk menggunakan awalan unik yang tidak tumpang tindih untuk mencegah konflik. read/write
> - Prefiks harus diakhiri dengan garis miring ke depan (/).
> - Setelah berbagi file dibuat, awalan tidak dapat diubah atau dihapus.

9. Untuk Wilayah, pilih Wilayah AWS tempat titik akhir S3 untuk bucket Anda berada dari daftar tarik-turun. Bidang ini hanya muncul jika Anda menentukan titik akses atau bucket di akun lain untuk bucket S3.
10. Untuk kelas Storage untuk objek baru, pilih kelas penyimpanan dari daftar dropdown. Untuk informasi selengkapnya tentang kelas penyimpanan, lihat Menggunakan kelas penyimpanan dengan File Gateway.
11. Untuk Peran IAM, lakukan salah satu hal berikut untuk mengonfigurasi peran IAM untuk berbagi file Anda:

    - Untuk secara otomatis membuat peran IAM baru dengan izin yang diperlukan agar berbagi file Anda berfungsi dengan baik, pilih Dibuat oleh Storage Gateway dari daftar tarik-turun.
    - Untuk menggunakan peran IAM yang ada, pilih nama peran dari daftar tarik-turun.
    - Untuk membuat peran IAM baru, pilih Buat peran. Untuk petunjuk lebih lanjut, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan di AWS Identity and Access Management Panduan Pengguna.

    Untuk informasi selengkapnya tentang cara peran IAM mengontrol akses antara berbagi file dan bucket S3, lihat Memberikan akses ke Amazon S3Bucket.
12. Untuk tautan Pribadi, lakukan hal berikut hanya jika Anda perlu mengonfigurasi berbagi file Anda untuk berkomunikasi dengan AWS menggunakan titik akhir pribadi di Virtual Private Cloud (VPC). Jika tidak, lewati langkah ini. Untuk informasi lebih lanjut, lihat Apa itu AWS PrivateLink? dalam AWS PrivateLink Guide.

    a. Pilih Gunakan titik akhir VPC.

    b. Untuk Identifikasi titik akhir VPC dengan, lakukan salah satu hal berikut:

- Pilih ID titik akhir VPC, lalu pilih titik akhir yang ingin Anda gunakan dari daftar dropdown titik akhir VPC.
- Pilih nama DNS, lalu masukkan nama DNS untuk titik akhir yang ingin Anda gunakan.

13. Untuk Enkripsi, pilih jenis kunci enkripsi yang akan digunakan untuk mengenkripsi objek yang disimpan File Gateway Anda di Amazon S3:

    - Untuk menggunakan enkripsi sisi server yang dikelola dengan Amazon S3 (SSE-S3), pilih S3-Managed Keys (SSE-S3).

      Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
    - Untuk menggunakan enkripsi sisi server yang dikelola dengan AWS Key Management Service (SSE-KMS), pilih KMS-Managed Keys (SSE-KMS). Untuk kunci KMS Primer, pilih kunci AWS KMS yang ada, atau pilih Buat kunci KMS baru untuk membuat kunci KMS baru di konsol Key Management Service (). AWS AWS KMS

      Untuk informasi selengkapnya AWS KMS, lihat Apa itu Layanan Manajemen AWS Kunci? di Panduan AWS Key Management Service Pengembang.
    - Untuk menggunakan enkripsi sisi server dual-layer yang dikelola dengan AWS Key Management Service (DSSE-KMS), pilih Enkripsi sisi server dual-layer dengan kunci (DSSE-KMS). AWS Key Management Service Untuk kunci KMS Primer, pilih kunci AWS KMS yang ada, atau pilih Buat kunci KMS baru untuk membuat kunci KMS baru di konsol Key Management Service (). AWS AWS KMS

      Untuk informasi selengkapnya tentang DSSE-KMS, lihat Menggunakan enkripsi sisi server dua lapis dengan AWS KMS kunci di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

      > **Note**
      >
      > Ada biaya tambahan untuk menggunakan DSSE-KMS dan kunci. AWS KMS Untuk informasi selengkapnya, lihat harga AWS KMS.
      > Untuk menentukan AWS KMS kunci dengan alias yang tidak terdaftar atau menggunakan AWS KMS kunci dari AWS akun yang berbeda, Anda harus menggunakan. AWS Command Line Interface Tombol KMS asimetris tidak didukung.

Untuk informasi selengkapnya, lihat Membuat SMBFile Bagikan di Referensi API AWS Storage Gateway.

> **Important**
>
> Pastikan file share Anda menggunakan jenis enkripsi yang sama dengan bucket Amazon S3 tempat menyimpan data Anda.

14. Untuk tipe Guess MIME, pilih tipe MIME media Guess untuk memungkinkan Storage Gateway menebak jenis Multipurpose Internet Mail Extension (MIME) untuk objek yang diunggah berdasarkan ekstensi filenya.
15. Untuk nama berbagi file, masukkan nama untuk berbagi file Anda.

> **Note**
>
> Nama berbagi file SMB yang valid tidak dapat berisi karakter berikut: `[,,],,#,;,<,>,:,",\,/,|, ? *+`, atau karakter kontrol ASCII. `1-31`

16. Untuk peristiwa Unggah, pilih Log peristiwa saat file berhasil diunggah oleh gateway jika Anda ingin gateway merekam peristiwa CloudWatch log saat berhasil mengunggah file ke Amazon S3. Penundaan notifikasi mengontrol penundaan antara operasi penulisan klien terbaru dan pembuatan notifikasi `ObjectUploaded` log. Karena klien dapat membuat banyak penulisan kecil ke file dalam waktu singkat, kami sarankan untuk mengatur parameter ini selama mungkin untuk menghindari menghasilkan beberapa notifikasi untuk file yang sama secara berurutan. Untuk informasi selengkapnya, lihat Mendapatkan notifikasi unggahan file.

> **Note**
>
> Pengaturan ini tidak berpengaruh pada waktu pengunggahan objek ke S3, hanya pada waktu pemberitahuan.
> Pengaturan ini tidak dimaksudkan untuk menentukan waktu yang tepat di mana pemberitahuan akan dikirim. Dalam beberapa kasus, gateway mungkin memerlukan lebih dari waktu tunda yang ditentukan untuk menghasilkan dan mengirim pemberitahuan.

Pilih Berikutnya setelah selesai.

17. Untuk protokol berbagi file, pilih SMB.
18. Untuk otentikasi Pengguna, pilih metode otentikasi yang ingin Anda gunakan dari daftar dropdown:

    - Untuk menggunakan Microsoft Active Directory perusahaan Anda atau AWS Managed Microsoft AD untuk mengautentikasi akses pengguna ke berbagi file SMB Anda, pilih Active Directory. Gateway Anda harus bergabung dengan domain untuk menggunakan metode ini. Untuk informasi selengkapnya, lihat Menggunakan Active Directory untuk mengautentikasi pengguna.

      > **Note**
      >
      > Untuk menggunakan AWS Managed Microsoft AD gateway Amazon EC2, Anda harus membuat instans Amazon EC2 di VPC yang sama dengan, menambahkan `_workspaceMembers` grup keamanan ke instans Amazon EC2, dan bergabung dengan domain AD menggunakan kredensi Admin dari. AWS Managed Microsoft AD AWS Managed Microsoft AD
      > Untuk informasi selengkapnya AWS Managed Microsoft AD, lihat Panduan AWS Directory Service Administrasi.
      > Untuk informasi selengkapnya tentang Amazon EC2, lihat Dokumentasi Amazon Elastic Compute Cloud.

      Jika status Gabung menunjukkan bahwa gateway Anda sudah bergabung ke domain Active Directory, lanjutkan ke langkah berikutnya. Jika tidak, lakukan tindakan berikut:

      1. Pilih Konfigurasikan
      2. Untuk Domain, masukkan nama domain Active Directory yang Anda ingin gateway Anda bergabung.
      3. Masukkan Nama Pengguna dan Kata Sandi yang akan digunakan gateway untuk bergabung dengan domain.
      4. (Opsional) Untuk unit Organisasi (OU), masukkan OU yang ditunjuk yang digunakan Direktori Aktif Anda untuk objek komputer baru.

5. (Opsional) Untuk pengontrol Domain (DC), masukkan nama DC di mana gateway Anda akan terhubung ke Active Directory. Anda dapat membiarkan bidang ini kosong untuk memungkinkan DNS memilih DC secara otomatis.
6. Pilih Gabung Direktori Aktif.

> **Note**
>
> Bergabung dengan domain akan membuat akun Active Directory di container default (yang bukan unit organisasi), menggunakan ID Gateway gateway sebagai nama akun (misalnya, SGW-1234ADE). Tidak mungkin untuk menyesuaikan nama akun ini.
> Jika lingkungan Active Directory Anda mengharuskan Anda melakukan pra-tahap akun untuk memfasilitasi proses penggabungan domain, Anda harus membuat akun ini sebelumnya.
> Jika lingkungan Active Directory Anda memiliki OU yang ditunjuk untuk objek komputer baru, Anda harus menentukan OU tersebut saat bergabung dengan domain.

- Untuk memberikan akses yang dilindungi kata sandi kepada siapa saja yang memberikan kata sandi tamu yang Anda konfigurasikan, pilih Akses tamu. File Gateway Anda tidak perlu menjadi bagian dari domain Microsoft Active Directory untuk menggunakan metode ini. Pilih Konfigurasi untuk menentukan kata sandi Tamu Anda, lalu pilih Simpan.

19. Untuk akses Pengguna, lakukan salah satu hal berikut untuk menentukan klien SMB mana yang dapat mengakses berbagi file Anda:

    - Untuk memberikan akses ke semua pengguna yang berhasil mengautentikasi melalui Active Directory, pilih Semua pengguna yang diautentikasi iklan.
    - Untuk mengizinkan atau menolak akses ke pengguna atau grup tertentu, pilih Pengguna atau grup yang diautentikasi iklan tertentu, lalu lakukan hal berikut:
        - Untuk pengguna dan grup yang Diizinkan, pilih Tambahkan pengguna yang diizinkan atau Tambahkan grup yang diizinkan dan masukkan pengguna atau grup Direktori Aktif yang ingin Anda izinkan akses berbagi file. Ulangi proses ini untuk memungkinkan sebanyak mungkin pengguna dan grup
        - Untuk pengguna dan grup Ditolak, pilih Tambah pengguna yang ditolak atau Tambahkan grup yang ditolak dan masukkan pengguna atau grup Direktori Aktif yang ingin Anda tolak akses berbagi file. Ulangi proses ini untuk menolak sebanyak mungkin pengguna dan grup yang diperlukan.

> **Note**
>
> Bagian akses berbagi file pengguna dan grup hanya muncul jika otentikasi pengguna diatur ke Active Directory.
> Saat menentukan pengguna atau grup, jangan sertakan domain. Nama domain tersirat oleh keanggotaan gateway di Direktori Aktif tertentu yang bergabung.

20. (Opsional) Untuk pengguna Admin, masukkan daftar pengguna dan grup Active Directory yang dipisahkan koma. Pengguna admin menerima hak istimewa untuk memperbarui daftar kontrol akses (ACLs) pada semua file dan folder dalam berbagi file. Grup harus diawali dengan `@` karakter, misalnya,`@group1`.
21. Untuk tipe Access, pilih salah satu dari berikut ini:
    - Untuk memungkinkan klien membaca dan menulis file pada berbagi file, pilih Baca/Tulis.
    - Untuk memungkinkan klien membaca file tetapi tidak menulis ke berbagi file, pilih Read-only.

    > **Note**
    >
    > Untuk berbagi file yang dipasang pada klien Microsoft Windows, jika Anda memilih Read-only, Anda mungkin melihat pesan tentang kesalahan tak terduga yang mencegah Anda membuat folder. Anda dapat mengabaikan pesan ini.

22. Untuk kontrol akses File dan direktori, pilih salah satu dari berikut ini:
    - Untuk mengatur izin berbutir halus pada file dan folder di berbagi file SMB Anda, pilih Daftar Kontrol Akses Windows. Untuk informasi selengkapnya, lihat Menggunakan Microsoft Windows ACLs untuk Mengontrol Akses ke Berbagi File SMB.
    - Untuk menggunakan izin POSIX untuk mengontrol akses ke file dan direktori yang disimpan melalui berbagi file SMB Anda, pilih izin POSIX.
23. Untuk enumerasi berbasis Access, lakukan salah satu hal berikut:
    - Untuk membuat file dan folder pada share hanya terlihat oleh pengguna yang memiliki akses baca, pilih Sembunyikan file dan direktori di mana pengguna tidak memiliki izin.
    - Untuk membuat file dan folder pada share terlihat oleh semua pengguna selama pencacahan direktori, jangan pilih kotak centang.

> **Note**
>
> Pencacahan berbasis akses adalah sistem yang memfilter enumerasi file dan folder pada berbagi file SMB berdasarkan daftar kontrol akses share (). ACLs

24. Untuk opsi akses File, pilih salah satu dari berikut ini:

    - Untuk mengoptimalkan strategi buffering file share menggunakan penguncian oportunistik, pilih Opportunistic lock. Dalam kebanyakan kasus, mengaktifkan penguncian oportunistik meningkatkan kinerja, terutama yang berkaitan dengan menu konteks Windows.
    - Untuk mengizinkan gateway - bukan klien SMB - untuk mengontrol sensitivitas huruf nama file, pilih Paksa sensitivitas kasus.
    - Untuk menonaktifkan kedua pengaturan, pilih Tidak.

    > **Note**
    >
    > Untuk menghindari konflik akses file, pengaturan ini saling eksklusif dan tidak dapat diaktifkan secara bersamaan.

25. (Opsional) Untuk penyegaran cache otomatis dari S3, pilih Setel interval penyegaran cache, lalu atur waktu dalam Menit atau Hari untuk menyegarkan cache berbagi file menggunakan Time To Live (TTL). TTL adalah lamanya waktu sejak penyegaran terakhir. Setelah interval TTL berlalu, mengakses direktori menyebabkan File Gateway menyegarkan konten direktori itu dari bucket Amazon S3.

    > **Note**
    >
    > Menyetel nilai ini lebih pendek dari 30 menit dapat berdampak negatif pada kinerja gateway dalam situasi di mana sejumlah besar objek Amazon S3 sering dibuat atau dihapus.

26. Untuk kepemilikan dan izin File, pilih Berikan pemilik bucket S3 kepemilikan penuh atas file yang dibuat oleh gateway, termasuk izin baca, tulis, edit, dan hapus jika Anda ingin AWS akun yang memiliki bucket S3 memiliki kontrol penuh atas semua objek yang ditulis ke bucket oleh berbagi file Anda.

Pilih Berikutnya setelah selesai.

27. Tinjau konfigurasi berbagi file. Pilih Edit untuk mengubah pengaturan untuk bagian mana pun yang ingin Anda ubah. Setelah selesai, pilih Buat.

Setelah berbagi file SMB dibuat, Anda dapat melihat pengaturan konfigurasinya di konsol AWS Storage Gateway di tab Rincian berbagi file. Untuk petunjuk untuk me-mount berbagi file Anda, lihat Memasang berbagi file SMB Anda di klien Anda.

Salin berbagi file

> **Note**
>
> Fitur copy file share hanya tersedia melalui konsol Storage Gateway. Tidak ada perintah AWS CLI atau tindakan API yang sesuai untuk fitur ini.

Anda dapat menggunakan konsol Storage Gateway untuk menyalin berbagi file NFS atau SMB yang ada ke gateway lain. Menyalin berbagi file akan membuat berbagi file baru di gateway tujuan yang mengarah ke bucket Amazon S3 yang sama dengan berbagi file sumber, sambil mempertahankan sebagian besar pengaturan konfigurasi share asli. Ini terutama dimaksudkan untuk membantu migrasi gateway, memungkinkan Anda memindahkan berbagi file ke gateway pengganti tanpa membuat ulang konfigurasinya secara manual. Setelah Anda memverifikasi bahwa berbagi file yang disalin berfungsi dengan benar di gateway baru, Anda harus menghapus berbagi file asli dari gateway sumber.

Pertimbangan-pertimbangan

Sebelum Anda menyalin file share, pertimbangkan hal berikut:

- Gateway tujuan harus dalam status Aktif.
- Gateway sumber dan tujuan harus berupa gateway Gateway File Amazon S3. Anda tidak dapat menyalin pembagian file di antara jenis gateway yang berbeda.
- Berbagi file yang disalin menunjuk ke bucket Amazon S3 yang sama dengan sumbernya. Kami tidak menyarankan untuk mempertahankan kedua pembagian file secara aktif untuk waktu yang lama. Menulis ke bucket Amazon S3 yang sama dari beberapa gateway secara bersamaan dapat

menyebabkan inkonsistensi data, konflik cache, dan perilaku tak terduga. Setelah mengonfirmasi bahwa berbagi file yang disalin berfungsi dengan benar, hapus berbagi file sumber.

- Operasi salinan mempertahankan protokol berbagi file (NFS atau SMB). Anda tidak dapat mengubah jenis protokol selama penyalinan.
- Jika berbagi file sumber menggunakan peran IAM untuk akses bucket Amazon S3, Anda dapat memilih untuk menggunakan peran yang sama untuk berbagi file yang disalin, memilih peran lain yang ada, atau meminta konsol membuat peran baru secara otomatis.
- Jika berbagi file sumber memiliki pemantauan grup CloudWatch log yang dikonfigurasi, Anda dapat memilih untuk menggunakan grup log yang sama, memilih grup log yang berbeda, atau meminta konsol membuat grup log baru secara otomatis.
- Jika Anda menyalin berbagi file SMB antara gateway yang digabungkan ke domain Active Directory yang berbeda, atau antara gateway menggunakan otentikasi Active Directory dan yang menggunakan akses tamu, tinjau setelan akses SMB Anda setelah salinan selesai untuk memastikan bahwa izin akses dikonfigurasi dengan benar.
- Jika gateway sumber dan tujuan memiliki konfigurasi VPC yang berbeda (misalnya, satu gateway diaktifkan dalam VPC dan yang lainnya tidak), berbagi file yang disalin menggunakan konfigurasi jaringan gateway tujuan.

> **Important**
>
> Saat menyalin berbagi file SMB, daftar kontrol akses tingkat root (ACL) tidak disalin ke berbagi file baru. Berbagi file yang disalin dibuat dengan ACL root default. Jika Anda telah mengonfigurasi ACL root kustom pada berbagi file sumber, Anda harus mengkonfigurasi ulang secara manual pada berbagi file yang disalin setelah salinan selesai.

Salin berbagi file ke gateway lain

Untuk menyalin berbagi file menggunakan konsol Storage Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.
2. Di panel navigasi, pilih Berbagi file.
3. Pilih file share yang ingin Anda salin.
4. Dari menu Tindakan, pilih Salin berbagi file ke gateway lain.
5. Untuk Gateway, pilih gateway tujuan tempat Anda ingin membuat salinan.

6. Untuk peran IAM, pilih salah satu opsi berikut:

   - Gunakan peran IAM yang sama — Menggunakan peran IAM yang sama dengan berbagi file sumber. Pilih opsi ini jika gateway tujuan harus menggunakan izin yang sama untuk mengakses bucket Amazon S3.
   - Pilih peran IAM yang ada — Pilih peran IAM yang berbeda dari daftar. Pastikan peran memberikan izin Amazon S3 yang diperlukan.
   - Auto-generate peran IAM baru — Konsol membuat peran IAM baru dengan izin yang diperlukan untuk bucket Amazon S3.

7. Untuk grup Log, pilih salah satu opsi berikut:

   - Gunakan grup log yang sama — Mengirim log kesehatan ke grup CloudWatch log yang sama dengan berbagi file sumber.
   - Pilih grup log yang ada — Pilih grup CloudWatch log yang berbeda dari daftar.
   - Auto-generate grup log baru — Konsol membuat grup CloudWatch log baru untuk berbagi file yang disalin.

8. Pilih Salin berbagi file.

Berbagi file baru muncul di daftar Berbagi file dengan status Creating. Setelah berbagi menjadi Tersedia, Anda dapat memasangnya di klien Anda menggunakan protokol yang sama dengan berbagi sumber.

Pengaturan dipertahankan selama penyalinan

Saat Anda menyalin berbagi file, pengaturan berikut akan dibawa dari berbagi file sumber ke salinan baru:

- Nama dan awalan bucket Amazon S3
- Kelas penyimpanan
- Pengaturan enkripsi objek (SSE-S3, SSE-KMS, atau DSSE-KMS)
- Protokol berbagi file (NFS atau SMB)
- Pengaturan penyegaran cache
- Pengaturan squash dan akses klien (berbagi file NFS)
- Pengaturan akses SMB termasuk metode otentikasi, visibilitas berbagi file, dan enumerasi berbasis akses (berbagi file SMB)

- Pengguna dan grup yang diizinkan dan ditolak (berbagi file SMB)

Pengaturan berikut tidak disalin dan menggunakan konfigurasi atau default gateway tujuan:

- Konfigurasi jaringan gateway (titik akhir VPC, titik akhir publik)
- Keanggotaan domain Active Directory (menggunakan konfigurasi AD gateway tujuan)
- Batas tingkat bandwidth (menggunakan batas gateway tujuan)
- Root-level ACL (berbagi file SMB - bagian yang disalin dibuat dengan ACL root default)

Memasang dan menggunakan berbagi file Anda

Topik di bagian ini memberikan petunjuk tentang cara memasang berbagi file di klien, menggunakan berbagi file, menguji Gateway File, dan membersihkan sumber daya yang tidak lagi diperlukan, seperti gateway, instans Amazon EC2, atau dan VMs lokal yang mungkin Anda buat untuk tujuan pengujian. Untuk informasi selengkapnya tentang klien Network File System (NFS) dan Service Message Block (SMB) yang didukung, lihat. Klien NFS dan SMB yang didukung untuk File Gateway

> **Note**
>
> Ini Konsol Manajemen AWS juga menyediakan contoh perintah yang dapat Anda gunakan untuk me-mount berbagi file Anda.

Topik

- Pasang berbagi file NFS Anda di klien Anda- Pelajari cara memasang berbagi file NFS Anda di drive di klien Anda dan memetakannya ke bucket Amazon S3 Anda.
- Pasang berbagi file SMB Anda di klien Anda- Pelajari cara memasang berbagi file SMB dan memetakan ke drive yang dapat diakses oleh klien Anda.
- Menggunakan berbagi file pada ember dengan objek yang sudah ada sebelumnya- Pelajari cara mengekspor berbagi file di bucket Amazon S3 dengan objek yang dibuat di luar File Gateway menggunakan NFS atau SMB.
- Uji Gateway File S3 Anda- Pelajari cara menguji gateway Anda dengan menyalin file dan folder ke drive yang dipetakan dan memverifikasi bahwa mereka muncul di bucket Amazon S3 Anda secara otomatis.

Pasang berbagi file NFS Anda di klien Anda

Gunakan prosedur berikut untuk memasang berbagi file NFS Anda di drive di klien Anda dan memetakannya ke bucket Amazon S3 Anda.

Untuk me-mount file share dan memetakannya ke bucket Amazon S3

1. Jika Anda menggunakan klien Microsoft Windows, kami sarankan Anda membuat berbagi file SMB dan mengaksesnya menggunakan klien SMB yang sudah diinstal pada klien Windows. Jika Anda menggunakan NFS, aktifkan Layanan untuk NFS di Windows.
2. Pasang berbagi file NFS Anda:

   - Untuk klien Linux, ketik perintah berikut di command prompt.

     ```
     sudo mount -t nfs -o nolock,hard [GatewayVMIPAddress]:/[FileShareName] [ClientMountPath]
     ```

   - Untuk klien Windows, ketik perintah berikut pada command prompt (cmd.exe).

     ```
     mount -o nolock -o mtype=hard [GatewayVMIPAddress]:/[FileShareName] [WindowsDriveLetter]
     ```

   Misalnya, pada klien Windows alamat IP VM Anda adalah 123.123.1.2 dan nama nama berbagi file Anda adalah. `test-fileshare` Misalkan juga bahwa Anda ingin memetakan ke drive T. Dalam hal ini, perintah Anda terlihat seperti berikut.

   ```
   mount -o nolock -o mtype=hard 123.123.1.2:/test-fileshare T:
   ```

   > **Note**
   >
   > Saat memasang berbagi file, perhatikan hal berikut:
   >
   > - Secara default, Windows menggunakan soft mount untuk berbagi NFS. Soft mount time out lebih mudah saat terjadi masalah koneksi. Sebaiknya gunakan hard mount untuk beban kerja kritis, karena hard mount lebih aman dan menyimpan data Anda dengan lebih baik. Untuk menggunakan hard mount, pastikan perintah Anda menggunakan `-o mtype=hard` sakelar.
   > - S3 File Gateway tidak mendukung penguncian file NFS. Selalu gunakan `-o nolock` opsi untuk mematikan penguncian file saat memasang berbagi file NFS.
   > - Anda mungkin memiliki kasus di mana folder dan objek ada di ember Amazon S3 dan memiliki nama yang sama. Dalam hal ini, jika nama objek tidak mengandung garis miring, hanya folder yang terlihat di File Gateway. Misalnya, jika bucket berisi objek bernama `test` atau `test/` dan folder bernama`test/test1`, hanya `test/` dan `test/test1` terlihat di File Gateway.

- Anda mungkin perlu melakukan remount file share Anda setelah reboot klien Anda.
- Jika Anda menggunakan klien Windows, periksa `mount` opsi Anda setelah pemasangan dengan menjalankan `mount` perintah tanpa opsi. Tanggapan harus mengonfirmasi bahwa berbagi file telah dipasang menggunakan opsi terbaru yang Anda berikan. Ini juga harus mengkonfirmasi bahwa Anda tidak menggunakan entri lama yang di-cache, yang membutuhkan setidaknya 60 detik untuk menghapusnya.

Langkah Selanjutnya

Uji Gateway File S3 Anda

Pasang berbagi file SMB Anda di klien Anda

Gunakan prosedur berikut untuk me-mount berbagi file SMB Anda dan memetakan ke drive yang dapat diakses oleh klien Anda. Bagian File Gateway konsol menunjukkan perintah mount yang didukung yang dapat Anda gunakan untuk klien SMB. Berikut ini, Anda dapat menemukan beberapa opsi tambahan untuk dicoba.

Anda dapat menggunakan beberapa metode berbeda untuk memasang berbagi file SMB, termasuk yang berikut ini:

- Command Prompt (`cmdkey`and`net use`) — Gunakan command prompt untuk me-mount file share Anda. Simpan kredensil Anda`cmdkey`, lalu pasang drive dengan `net use` dan sertakan `/savecred` sakelar `/persistent:yes` dan jika Anda ingin koneksi tetap ada di seluruh reboot sistem. Perintah spesifik yang Anda gunakan akan berbeda tergantung pada apakah Anda ingin memasang drive untuk akses Microsoft Active Directory (AD) atau akses pengguna tamu. Contohnya disediakan di bawah ini.
- File Explorer (Map Network Drive) - Gunakan Windows File Explorer untuk me-mount berbagi file Anda. Konfigurasikan pengaturan untuk menentukan apakah Anda ingin koneksi tetap ada di seluruh sistem reboot dan meminta kredensional jaringan.
- PowerShell script - Buat PowerShell skrip khusus untuk me-mount berbagi file Anda. Bergantung pada parameter yang Anda tentukan dalam skrip, koneksi dapat persisten di seluruh reboot sistem, dan bagian dapat terlihat atau tidak terlihat oleh sistem operasi saat dipasang.

> **Note**
>
> Jika Anda adalah pengguna Microsoft AD, tanyakan kepada administrator Anda untuk memastikan bahwa Anda memiliki akses ke berbagi file SMB sebelum memasang file share ke sistem lokal Anda.
> Jika Anda adalah pengguna tamu, pastikan Anda memiliki kata sandi pengguna tamu sebelum mencoba memasang berbagi file.

Untuk me-mount file share SMB Anda untuk pengguna Microsoft AD resmi menggunakan command prompt:

1. Pastikan pengguna Microsoft AD memiliki izin yang diperlukan untuk berbagi file SMB sebelum memasang file share ke sistem pengguna.
2. Masukkan yang berikut ini pada prompt perintah untuk me-mount file share:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes
   ```

Untuk me-mount file share SMB Anda dengan kombinasi kredensi login tertentu menggunakan command prompt:

1. Pastikan bahwa pengguna memiliki akses ke berbagi file SMB sebelum memasang file share ke sistem.
2. Masukkan yang berikut ini pada prompt perintah untuk menyimpan kredensil pengguna di Windows Credential Manager:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. Masukkan yang berikut ini pada prompt perintah untuk me-mount file share:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes /savecred
   ```

Untuk me-mount file share SMB Anda untuk pengguna tamu menggunakan command prompt:

1. Pastikan Anda memiliki kata sandi pengguna tamu sebelum memasang file share.

2. Ketik berikut ini di prompt perintah untuk menyimpan kredensi tamu di Windows Credential Manager:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```

3. Ketik berikut ini di command prompt.

   ```
   net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$Gateway
   ID\smbguest /persistent:yes /savecred
   ```

> **Note**
>
> Saat memasang berbagi file, perhatikan hal berikut:
>
> - Anda mungkin memiliki kasus di mana folder dan objek ada di ember Amazon S3 dan memiliki nama yang sama. Dalam hal ini, jika nama objek tidak mengandung garis miring, hanya folder yang terlihat di File Gateway. Misalnya, jika bucket berisi objek bernama `test` atau `test/` dan folder bernama`test/test1`, hanya `test/` dan `test/test1` terlihat di File Gateway.
> - Kecuali Anda mengonfigurasi koneksi berbagi file untuk menyimpan kredensil pengguna dan bertahan di seluruh sistem restart, Anda mungkin perlu melakukan remount file share setiap kali Anda memulai ulang sistem klien Anda.

Untuk memasang berbagi file SMB menggunakan Windows File Explorer

1. Tekan tombol Windows dan **File Explorer** ketik kotak Cari Windows, atau tekan**Win+E**.
2. Di panel navigasi, pilih PC ini. Kemudian, pada tab Komputer, pilih Map Network Drive.
3. Dalam kotak dialog Map Network Drive, pilih huruf drive untuk Drive.
4. Untuk Folder, ketik***[File Gateway IP]**[SMB File Share Name]***, atau pilih Browse untuk memilih berbagi file SMB Anda dari kotak dialog.
5. (Opsional) Pilih Sambungkan kembali saat mendaftar jika Anda ingin titik pemasangan tetap ada setelah reboot.
6. (Opsional) Pilih Connect menggunakan kredensi yang berbeda jika Anda ingin pengguna memasukkan login Microsoft AD atau kata sandi pengguna akun tamu.
7. Pilih Selesai untuk menyelesaikan titik pemasangan Anda.

> **Note**
>
> File atau direktori apa pun yang dimulai dengan karakter dot (`.`) akan ditandai disembunyikan di Windows. Untuk membuat file dan direktori ini terlihat, Anda harus memilih kotak centang Item tersembunyi pada tab Lihat di Windows File Explorer.

Anda dapat mengedit setelan berbagi file, mengedit pengguna dan grup yang diizinkan dan ditolak, dan mengubah kata sandi akses tamu dari Storage Gateway Management Console. Anda juga dapat menyegarkan data di cache berbagi file dan menghapus berbagi file dari konsol.

Untuk mengubah properti berbagi file SMB Anda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada panel navigasi, pilih Berbagi File.
3. Pada halaman Berbagi File, pilih kotak centang dengan berbagi file SMB yang ingin Anda ubah.
4. Untuk Tindakan, pilih tindakan yang Anda inginkan:
   - Pilih Edit pengaturan berbagi file untuk mengubah akses berbagi.
   - Pilih Edit allowed/denied pengguna untuk menambah atau menghapus pengguna dan grup, lalu ketik pengguna dan grup yang diizinkan dan ditolak ke dalam kotak Pengguna yang Diizinkan, Pengguna Ditolak, Grup yang Diizinkan, dan Grup yang Ditolak. Gunakan tombol Tambah Entri untuk membuat hak akses baru, dan tombol (X) untuk menghapus akses.

     > **Note**
     >
     > Grup harus diawali dengan `@` karakter. Format yang dapat diterima meliputi: `DOMAIN\User1user1`,`@group1`,, dan`@DOMAIN\group1`.
5. Setelah selesai, pilih Simpan.

   Saat Anda memasukkan pengguna dan grup yang diizinkan, Anda membuat daftar izin. Tanpa daftar izin, semua pengguna Microsoft AD yang diautentikasi dapat mengakses berbagi file SMB. Setiap pengguna dan grup yang ditandai sebagai ditolak ditambahkan ke daftar penolakan dan tidak dapat mengakses berbagi file SMB. Dalam kasus di mana pengguna atau grup berada di daftar penolakan dan daftar izinkan, daftar penolakan diutamakan.

Anda dapat mengaktifkan Daftar Kontrol Akses (ACLs) pada berbagi file SMB Anda. Untuk informasi tentang cara mengaktifkan ACLs, lihatMenggunakan Windows ACL untuk membatasi akses berbagi file SMB.

Langkah Selanjutnya

Uji Gateway File S3 Anda

Menggunakan berbagi file pada ember dengan objek yang sudah ada sebelumnya

Anda dapat mengekspor berbagi file di bucket Amazon S3 dengan objek yang dibuat di luar File Gateway menggunakan NFS atau SMB. Objek di bucket yang dibuat di luar gateway ditampilkan sebagai file di sistem file NFS atau SMB saat klien sistem file Anda mengaksesnya. Akses dan izin Antarmuka Sistem Operasi Portabel Standar (POSIX) digunakan dalam berbagi file. Saat Anda menulis file kembali ke bucket Amazon S3, file tersebut mengasumsikan properti dan hak akses yang Anda berikan kepada mereka.

Anda dapat mengunggah objek ke bucket S3 kapan saja. Agar file share menampilkan objek yang baru ditambahkan ini sebagai file, Anda perlu me-refresh bucket S3. Untuk informasi selengkapnya, lihat the section called “Menyegarkan cache objek bucket Amazon S3”.

> **Note**
>
> Kami tidak menyarankan memiliki banyak penulis untuk satu ember Amazon S3. Jika ya, pastikan untuk membaca bagian “Bisakah saya memiliki banyak penulis ke ember Amazon S3 saya?” di FAQ Storage Gateway.

Untuk menetapkan default metadata ke objek yang diakses menggunakan NFS, lihat Mengedit Default Metadata di. Mengelola Gateway File Amazon S3 Anda

Untuk SMB, Anda dapat mengekspor share menggunakan Microsoft AD atau akses tamu untuk bucket Amazon S3 dengan objek yang sudah ada sebelumnya. Objek yang diekspor melalui berbagi file SMB mewarisi kepemilikan dan izin POSIX dari direktori induk tepat di atasnya. Untuk objek di bawah folder root, root Access Control Lists (ACL) diwariskan. Untuk Root ACL, pemiliknya

`smbguest` dan izin untuk file adalah 666 dan direktorinya. 777 Ini berlaku untuk semua bentuk akses yang diautentikasi (Microsoft AD dan tamu).

Uji Gateway File S3 Anda

Gunakan prosedur berikut untuk menguji gateway Anda dengan menyalin file dan folder ke drive yang dipetakan dan memverifikasi bahwa mereka muncul di bucket Amazon S3 Anda secara otomatis.

Untuk mengunggah file dari klien Windows Anda ke Amazon S3

1. Pada klien Windows Anda, navigasikan ke drive tempat Anda memasang file share Anda. Nama drive Anda didahului dengan nama bucket S3 Anda.
2. Salin file atau folder ke drive.
3. Di Konsol Manajemen Amazon S3, navigasikan ke bucket yang dipetakan. Anda akan melihat file dan folder yang Anda salin di bucket Amazon S3 yang Anda tentukan.

   Anda dapat melihat berbagi file yang Anda buat di tab Berbagi file di AWS Storage Gateway Management Console.

Klien NFS atau SMB Anda dapat menulis, membaca, menghapus, mengganti nama, dan memotong file.

> **Note**
>
> File Gateways tidak mendukung pembuatan tautan keras atau simbolis pada berbagi file.

Ingatlah poin-poin ini tentang cara kerja File Gateways dengan S3:

- Pembacaan disajikan dari cache read-through. Dengan kata lain, jika data tidak tersedia, itu diambil dari S3 dan ditambahkan ke cache.
- Penulisan dikirim ke S3 melalui unggahan multipart yang dioptimalkan dengan menggunakan cache write-back.
- Baca dan tulis dioptimalkan sehingga hanya bagian yang diminta atau diubah yang ditransfer melalui jaringan.
- Menghapus menghapus objek dari S3.

- Direktori dikelola sebagai objek folder di S3, menggunakan sintaks yang sama seperti di konsol Amazon S3. Anda dapat mengganti nama direktori kosong.
- Kinerja operasi sistem file rekursif (misalnya`ls -l`) bergantung pada jumlah objek di bucket Anda.

Mengelola Gateway File Amazon S3 Anda

Topik di bagian ini memberikan informasi tentang cara mengelola sumber daya Amazon S3 File Gateway Anda. Manajemen gateway mencakup pemberian izin untuk gateway Anda untuk mengakses berbagi file dan bucket Amazon S3, mengedit informasi dan pengaturan untuk gateway dan berbagi file, menghapus berbagi file, menyegarkan objek yang di-cache, dan memahami indikator status operasional untuk gateway dan berbagi file.

Topik

- Edit 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.
- Memberikan akses dan izin- Pelajari cara menggunakan peran IAM untuk memberi gateway Anda izin akses untuk bucket Amazon S3 dan titik akhir VPC Amazon, mencegah masalah keamanan tertentu, dan menghubungkan berbagi file ke bucket di seluruh akun. AWS
- Hapus berbagi file- Pelajari cara menghapus file share menggunakan konsol Storage Gateway.
- Mengedit pengaturan SMB gateway- Pelajari cara mengedit pengaturan SMB tingkat gateway yang mengontrol strategi keamanan, otentikasi Direktori Aktif, akses tamu, izin grup lokal, dan visibilitas berbagi file untuk berbagi file SMB di gateway.
- Edit pengaturan berbagi file SMB- Pelajari cara mengedit pengaturan untuk mengonfigurasi nama, pencatatan, penyegaran cache, kelas penyimpanan, ekspor file, dan lainnya untuk berbagi file SMB.
- Batasi akses berbagi file SMB- Pelajari cara menambahkan pengguna atau grup yang diizinkan atau ditolak untuk membatasi akses ke berbagi file SMB Anda.
- Edit pengaturan berbagi file NFS- Pelajari cara mengedit pengaturan untuk mengonfigurasi nama, pencatatan, penyegaran cache, kelas penyimpanan, ekspor file, dan lainnya untuk berbagi file NFS.
- Edit default metadata berbagi file NFS- Pelajari cara mengedit nilai metadata default yang menyertakan izin Unix untuk file dan folder pada berbagi file NFS.
- Batasi akses berbagi file NFS- Pelajari cara membatasi akses ke klien dari alamat IP tertentu atau rentang IP untuk fileshare NFS Anda.
- Menyegarkan cache objek bucket Amazon S3- Pelajari cara menyegarkan cache objek bucket S3 untuk berbagi file dan mengonfigurasi jadwal untuk menyegarkan cache secara otomatis.

- Menggunakan Kunci Objek S3- Pelajari cara kerja Amazon S3 File Gateway dengan fitur S3 Object Lock.
- Status berbagi file- Pelajari cara melihat dan menafsirkan status berbagi file.
- Status gerbang- Pelajari cara melihat dan menafsirkan status gateway.
- Mengelola bandwidth untuk Gateway File Amazon S3 Anda- Pelajari cara membatasi throughput unggahan dari gateway Anda AWS untuk mengontrol jumlah bandwidth jaringan yang digunakan gateway.

Mengedit informasi dasar untuk S3 File Gateway

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.

Memberikan akses dan izin untuk berbagi file dan bucket

Setelah Gateway File S3 diaktifkan dan dijalankan, Anda dapat menambahkan berbagi file tambahan dan memberikan akses ke bucket Amazon S3, termasuk bucket yang Akun AWS berbeda dari gateway dan berbagi file Anda. Bagian berikut menjelaskan cara menggunakan peran IAM untuk memberi gateway Anda izin akses untuk bucket Amazon S3 dan titik akhir VPC, mencegah masalah keamanan tertentu, dan menghubungkan pembagian file ke bucket. Akun AWS

Untuk informasi tentang cara membuat berbagi file baru, lihatMembuat berbagi file.

Bagian ini berisi topik-topik berikut, yang memberikan informasi tambahan tentang cara memberikan akses dan izin untuk berbagi file dan bucket Amazon S3:

Topik

- Memberikan akses ke bucket Amazon S3- Pelajari cara memberikan akses kepada File Gateway untuk mengunggah file ke bucket Amazon S3, dan melakukan tindakan pada titik akses apa pun atau titik akhir Amazon Virtual Private Cloud (Amazon VPC) yang digunakan untuk terhubung ke bucket.
- Pencegahan "confused deputy" lintas layanan- Pelajari cara mencegah masalah keamanan umum di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan.
- Menggunakan berbagi file untuk akses lintas akun- Pelajari cara memberikan akses untuk akun Amazon Web Services dan pengguna akun tersebut untuk mengakses sumber daya milik akun Amazon Web Services lainnya.

Memberikan akses ke bucket Amazon S3

Saat Anda membuat berbagi file, Gateway File memerlukan akses untuk mengunggah file ke bucket Amazon S3, dan untuk melakukan tindakan pada titik akses atau titik akhir virtual private cloud (VPC) apa pun yang digunakan untuk terhubung ke bucket. Untuk memberikan akses ini, File Gateway Anda mengasumsikan peran AWS Identity and Access Management (IAM) yang terkait dengan kebijakan IAM yang memberikan akses ini.

Peran tersebut membutuhkan kebijakan IAM ini dan hubungan security token service trust (STS) untuk itu. Kebijakan menentukan tindakan yang dapat dilakukan peran. Selain itu, bucket S3 Anda dan titik akses terkait atau titik akhir VPC harus memiliki kebijakan akses yang memungkinkan peran IAM untuk mengaksesnya.

Anda dapat membuat kebijakan peran dan akses sendiri, atau Gateway File Anda dapat membuatnya untuk Anda. Jika File Gateway membuat kebijakan untuk Anda, kebijakan tersebut berisi daftar tindakan S3. Untuk informasi tentang peran dan izin, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan Pengguna IAM.

Contoh berikut adalah kebijakan kepercayaan yang memungkinkan File Gateway Anda untuk mengambil peran IAM.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Important

Storage Gateway dapat mengasumsikan peran layanan yang ada yang diteruskan menggunakan tindakan `iam:PassRole` kebijakan, tetapi tidak mendukung kebijakan IAM yang menggunakan kunci `iam:PassedToService` konteks untuk membatasi tindakan ke layanan tertentu.
Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna AWS Identity and Access Management :

- IAM: Lulus peran IAM ke layanan tertentu AWS

- Memberikan izin pengguna untuk meneruskan peran ke layanan AWS
- Kunci yang tersedia untuk IAM

Jika Anda tidak ingin File Gateway membuat kebijakan atas nama Anda, Anda dapat membuat kebijakan sendiri dan melampirkannya ke berbagi file Anda. Untuk informasi selengkapnya tentang cara melakukan ini, lihat Membuat berbagi file.

Kebijakan contoh berikut memungkinkan Gateway File Anda untuk melakukan semua tindakan Amazon S3 yang tercantum dalam kebijakan. Bagian pertama dari pernyataan memungkinkan semua tindakan yang terdaftar untuk dilakukan pada bucket S3 bernama`amzn-s3-demo-bucket`. Bagian kedua memungkinkan tindakan yang tercantum pada semua objek di`amzn-s3-demo-bucket`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
```

```
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Effect": "Allow"
        }
    ]
}
```

Contoh kebijakan berikut mirip dengan kebijakan sebelumnya, tetapi memungkinkan File Gateway Anda untuk melakukan tindakan yang diperlukan untuk mengakses bucket melalui titik akses.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Jika Anda perlu menghubungkan berbagi file ke bucket S3 melalui titik akhir VPC, lihat Kebijakan titik akhir untuk Amazon S3 di Panduan Pengguna.AWS PrivateLink

> **Note**
>
> Untuk bucket terenkripsi, fileshare harus menggunakan kunci di akun bucket S3 tujuan.

> **Note**
>
> Jika File Gateway Anda menggunakan SSE-KMS atau DSSE-KMS untuk enkripsi, pastikan peran IAM yang terkait dengan berbagi file mencakup izin KMS:Encrypt, KMS:Decrypt, kms:*, kms:, dan kms:. ReEncrypt GenerateDataKey DescribeKey Untuk informasi selengkapnya, lihat Menggunakan Kebijakan Berbasis Identitas (Kebijakan IAM) untuk Storage Gateway.

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan dalam kebijakan sumber daya untuk membatasi izin yang AWS Storage Gateway memberikan layanan lain ke sumber daya. Jika Anda menggunakan kedua kunci konteks kondisi global, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Nilai `aws:SourceArn` harus berupa ARN dari Storage Gateway yang terkait dengan berbagi file Anda.

Cara paling efektif untuk melindungi dari masalah "confused deputy" adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan

kunci kondisi konteks `aws:SourceArn` global dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:servicename::123456789012:*`.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan global di Storage Gateway untuk mencegah masalah deputi yang membingungkan.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Sid": "ConfusedDeputyPreventionExamplePolicy",
       "Effect": "Allow",
       "Principal": {
         "Service": "storagegateway.amazonaws.com"
       },
       "Action": "sts:AssumeRole",
       "Condition": {
         "StringEquals": {
           "aws:SourceAccount": "444455556666"
         },
         "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-
east-1:444455556666:gateway/sgw-123456DA"
        }
      }
    }
  ]
}
```

Menggunakan berbagi file untuk akses lintas akun

Akses lintas akun adalah ketika akun Amazon Web Services dan pengguna untuk akun tersebut diberikan akses ke sumber daya milik akun Amazon Web Services lainnya. Dengan File Gateways, Anda dapat menggunakan berbagi file di satu akun Amazon Web Services untuk mengakses objek di bucket Amazon S3 milik akun Amazon Web Services yang berbeda.

Untuk menggunakan berbagi file yang dimiliki oleh satu akun Amazon Web Services untuk mengakses bucket S3 di akun Amazon Web Services yang berbeda

1. Pastikan pemilik bucket S3 telah memberikan akses akun Amazon Web Services Anda ke bucket S3 yang perlu Anda akses dan objek di bucket tersebut. Untuk informasi tentang cara memberikan akses ini, lihat Contoh 2: Pemilik bucket yang memberikan izin bucket lintas akun di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Untuk daftar izin yang diperlukan, lihatMemberikan akses ke bucket Amazon S3.
2. Pastikan bahwa peran IAM yang digunakan berbagi file Anda untuk mengakses bucket S3 menyertakan izin untuk operasi seperti dan. `s3:GetObjectAcl` `s3:PutObjectAcl` Selain itu, pastikan bahwa peran IAM mencakup kebijakan kepercayaan yang memungkinkan akun Anda untuk mengambil peran IAM tersebut. Untuk contoh kebijakan kepercayaan semacam itu, lihatMemberikan akses ke bucket Amazon S3.

   Jika berbagi file menggunakan peran yang ada untuk mengakses bucket S3, Anda harus menyertakan izin untuk `s3:GetObjectAc` l dan `s3:PutObjectAcl` operasi. Peran tersebut juga membutuhkan kebijakan kepercayaan yang memungkinkan akun Anda untuk mengambil peran ini. Untuk contoh kebijakan kepercayaan semacam itu, lihatMemberikan akses ke bucket Amazon S3.
3. Pilih file Gateway yang dapat diakses oleh pemilik bucket S3 saat membuat berbagi file atau mengedit setelan berbagi file di rumah. https://console.aws.amazon.com/storagegateway/

Ketika Anda telah membuat atau memperbarui berbagi file untuk akses lintas akun dan memasang berbagi file di tempat, kami sangat menyarankan Anda menguji penyiapan Anda. Anda dapat melakukan ini dengan mencantumkan konten direktori atau menulis file pengujian dan memastikan file muncul sebagai objek di bucket S3.

> **Important**
>
> Pastikan untuk menyiapkan kebijakan dengan benar untuk memberikan akses lintas akun ke akun yang digunakan oleh berbagi file Anda. Jika tidak, pembaruan ke file melalui aplikasi lokal tidak akan menyebar ke bucket Amazon S3 yang sedang Anda gunakan.

Sumber daya

Untuk informasi tambahan tentang kebijakan akses dan daftar kontrol akses, lihat berikut ini:

Pedoman untuk menggunakan opsi kebijakan akses yang tersedia di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon

Ikhtisar Access Control List (ACL) di Panduan Pengguna Amazon Simple Storage Service

Hapus berbagi file

Jika Anda tidak lagi memerlukan berbagi file, Anda dapat menghapusnya dari konsol Storage Gateway. Saat Anda menghapus berbagi file, gateway terlepas dari bucket Amazon S3 tempat file berbagi peta. Namun, bucket S3 dan isinya tidak dihapus.

Jika gateway Anda mengunggah data ke bucket S3 saat Anda menghapus berbagi file, proses penghapusan tidak selesai hingga semua data diunggah. Berbagi file memiliki status DELETING hingga data benar-benar diunggah.

Jika Anda tidak ingin menunggu data Anda diunggah sepenuhnya, lihat prosedur Untuk menghapus file berbagi secara paksa nanti dalam topik ini.

Untuk menghapus berbagi file

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

Dalam kasus tertentu, Anda mungkin tidak ingin menunggu sampai semua data yang ditulis ke file pada file share Network File System (NFS) diunggah sebelum menghapus file share. Misalnya, Anda mungkin ingin sengaja membuang data yang ditulis tetapi belum diunggah, atau bucket Amazon S3 yang mendukung pembagian file mungkin telah dihapus, artinya mengunggah data yang ditentukan tidak lagi memungkinkan.

Dalam kasus ini, Anda dapat menghapus file share secara paksa dengan menggunakan Konsol Manajemen AWS atau operasi `DeleteFileShare` API. Operasi ini menghentikan proses upload data. Ketika itu terjadi, berbagi file memasuki status FORCE_DELETING. Untuk menghapus file share secara paksa menggunakan konsol Storage Gateway, lihat prosedur berikut.

Untuk menghapus file share secara paksa

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Dari halaman daftar Berbagi file, pilih berbagi file yang Anda tandai untuk dihapus dalam prosedur di atas untuk melihat detailnya. Setelah beberapa detik, pesan pemberitahuan penghapusan muncul di tab Detail.
3. Di pesan yang muncul di tab Detail, verifikasi ID berbagi file yang ingin Anda hapus secara paksa, pilih kotak konfirmasi, dan pilih Paksa hapus sekarang.

> **Note**
>
> Anda tidak dapat membatalkan operasi penghapusan paksa.
> Saat Anda menghapus file share secara paksa, potongan file yang ditransfer sebagian dari unggahan multi-bagian mungkin tetap ada di Amazon S3 di mana mereka dapat dikenakan biaya penyimpanan. Sebaiknya konfigurasi aturan siklus hidup bucket Amazon S3 untuk menghapus bagian file ini secara otomatis. Untuk informasi selengkapnya, lihat Praktik terbaik: mengelola unggahan multibagian.

Anda juga dapat menggunakan operasi DeleteFileShareAPI untuk menghapus file share secara paksa. Menghapus file share menggunakan API memerlukan izin kebijakan `storagegateway:DeleteFileShare` IAM.

Mengedit pengaturan SMB untuk gateway

Pengaturan SMB tingkat Gateway memungkinkan Anda mengonfigurasi strategi keamanan, otentikasi Direktori Aktif, akses tamu, izin grup lokal, dan visibilitas berbagi file untuk berbagi file SMB di gateway.

Untuk mengedit pengaturan SMB tingkat gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Gateway, lalu pilih gateway yang ingin Anda edit pengaturan SMB.
3. Dari menu tarik-turun Tindakan, pilih Edit pengaturan SMB, lalu pilih pengaturan yang ingin Anda edit.

Bagian ini berisi topik-topik berikut, yang memberikan informasi dan prosedur tambahan yang terkait dengan mengonfigurasi setiap pengaturan SMB individual untuk gateway Anda.

Topik

- Tetapkan tingkat keamanan gateway- Pelajari cara mengatur tingkat keamanan untuk menentukan persyaratan koneksi seperti penandatanganan dan enkripsi Blok Pesan Server (SMB), dan apakah akan mengizinkan koneksi dari klien SMB versi 1.
- Konfigurasikan otentikasi Direktori Aktif- Pelajari cara mengonfigurasi Direktori Aktif perusahaan atau Microsoft AD yang AWS Dikelola untuk akses terautentikasi pengguna ke berbagi file SMB Anda.
- Menyediakan akses tamu- Pelajari cara mengonfigurasi gateway Anda untuk mengizinkan akses tamu bagi setiap pengguna yang menyediakan nama pengguna dan kata sandi akun tamu yang benar.
- Konfigurasikan grup lokal- Pelajari cara mengonfigurasi grup lokal untuk memberikan izin berbagi file khusus kepada pengguna Active Directory.
- Tetapkan visibilitas berbagi file- Pelajari cara menentukan apakah saham di gateway terlihat saat mencantumkan saham ke pengguna.

Tetapkan tingkat keamanan untuk gateway Anda

Dengan menggunakan S3 File Gateway, Anda dapat menentukan tingkat keamanan untuk gateway Anda. Dengan menentukan tingkat keamanan ini, Anda dapat mengatur apakah gateway Anda harus memerlukan penandatanganan Blok Pesan Server (SMB) atau enkripsi SMB, atau apakah Anda ingin mengizinkan SMB versi 1.

Untuk mengkonfigurasi tingkat keamanan

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Gateway, lalu pilih gateway yang ingin Anda edit pengaturan SMB.
3. Dari menu tarik-turun Tindakan, pilih Edit pengaturan SMB, lalu pilih pengaturan keamanan SMB.
4. Untuk tingkat Keamanan, pilih salah satu dari berikut ini:

> **Note**
>
> Untuk informasi tentang mengonfigurasi setelan ini menggunakan AWS API, lihat Memperbarui SMBSecurity Strategi di Referensi AWS Storage Gateway API.
> Tingkat strategi keamanan yang lebih tinggi dapat memengaruhi kinerja gateway.

- Menerapkan AES256 enkripsi - Jika Anda memilih opsi ini, S3 File Gateway hanya mengizinkan koneksi dari SMBv3 klien yang menggunakan algoritma enkripsi AES 256-bit. Algoritma 128-bit tidak diperbolehkan. Opsi ini direkomendasikan untuk lingkungan yang menangani data sensitif. Ia bekerja dengan semua klien SMB saat ini di Microsoft Windows.
- Menerapkan enkripsi - Jika Anda memilih opsi ini, S3 File Gateway hanya mengizinkan koneksi dari SMBv3 klien yang telah mengaktifkan enkripsi. Algoritma 256-bit dan 128-bit diperbolehkan. Opsi ini direkomendasikan untuk lingkungan yang menangani data sensitif. Ia bekerja dengan semua klien SMB saat ini di Microsoft Windows.
- Menegakkan penandatanganan — Jika Anda memilih opsi ini, S3 File Gateway hanya mengizinkan koneksi dari SMBv2 atau SMBv3 klien yang telah mengaktifkan penandatanganan. Opsi ini berfungsi dengan semua klien SMB saat ini di Microsoft Windows.
- Klien dinegosiasikan — Jika Anda memilih opsi ini, permintaan dibuat berdasarkan apa yang dinegosiasikan oleh klien. Opsi ini direkomendasikan ketika Anda ingin memaksimalkan kompatibilitas di berbagai klien di lingkungan Anda.

> **Note**
>
> Untuk gateway yang diaktifkan sebelum 20 Juni 2019, tingkat keamanan default dinegosiasikan Klien.
> Untuk gateway yang diaktifkan pada 20 Juni 2019 dan yang lebih baru, tingkat keamanan default adalah Enforce encryption.

5. Pilih Simpan.

Gunakan Active Directory untuk mengautentikasi pengguna

Untuk menggunakan Active Directory perusahaan Anda atau AWS Managed Microsoft AD untuk akses terautentikasi pengguna ke berbagi file SMB Anda, edit setelan SMB untuk gateway Anda

dengan kredensi domain Microsoft AD Anda. Melakukan hal ini memungkinkan gateway Anda untuk bergabung dengan domain Direktori Aktif Anda dan memungkinkan anggota domain untuk mengakses berbagi file SMB.

> **Note**
>
> Dengan menggunakan Directory Service, Anda dapat membuat layanan domain Active Directory yang dihosting di file AWS Cloud.
> Untuk menggunakan gateway Amazon EC2, Anda harus membuat instans Amazon EC2 di VPC yang sama AWS Managed Microsoft AD dengan, menambahkan grup keamanan _WorkspaceMembers ke instans Amazon EC2, dan bergabung dengan domain AD menggunakan kredensi Admin dari. AWS Managed Microsoft AD AWS Managed Microsoft AD
> Untuk informasi selengkapnya AWS Managed Microsoft AD, lihat Panduan AWS Directory Service Administrasi.
> Untuk informasi selengkapnya tentang Amazon EC2, lihat Dokumentasi Amazon Elastic Compute Cloud.

Anda juga dapat mengaktifkan daftar kontrol akses (ACLs) pada berbagi file SMB Anda. Untuk informasi tentang cara mengaktifkan ACLs, lihatMenggunakan Windows ACL untuk membatasi akses berbagi file SMB.

Untuk mengaktifkan otentikasi Active Directory

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Gateway, lalu pilih gateway yang ingin Anda edit pengaturan SMB.
3. Dari menu tarik-turun Tindakan, pilih Edit pengaturan SMB, lalu pilih pengaturan Direktori Aktif.
4. Untuk nama Domain, masukkan nama domain Active Directory yang Anda inginkan untuk bergabung dengan gateway Anda.

   > **Note**
   >
   > Status Active Directory menunjukkan Terpisah ketika gateway tidak pernah bergabung dengan domain.
   > Akun layanan Active Directory Anda harus memiliki izin yang diperlukan. Untuk selengkapnya, lihat Persyaratan izin akun layanan Direktori Aktif Persyaratan izin .

Bergabung dengan domain membuat akun komputer Active Directory di wadah komputer default (yang bukan OU), menggunakan ID Gateway gateway sebagai nama akun (misalnya, SGW-1234ADE). Tidak mungkin untuk menyesuaikan nama akun ini.
Jika lingkungan Direktori Aktif Anda mengharuskan Anda melakukan pra-tahap akun untuk memfasilitasi proses bergabung dengan domain, Anda harus membuat akun ini sebelumnya.
Jika lingkungan Active Directory Anda memiliki OU yang ditunjuk untuk objek komputer baru, Anda harus menentukan OU tersebut saat bergabung dengan domain.
Jika gateway Anda tidak dapat bergabung dengan direktori Active Directory, coba gabungkan dengan alamat IP direktori dengan menggunakan operasi JoinDomainAPI.

5. Untuk pengguna Domain dan kata sandi Domain, masukkan kredensil untuk akun layanan Direktori Aktif yang akan digunakan gateway untuk bergabung dengan domain.
6. (Opsional) Untuk unit Organisasi (OU), masukkan OU yang ditunjuk yang digunakan Direktori Aktif Anda untuk objek komputer baru.
7. (Opsional) Untuk pengontrol Domain (DC), masukkan nama satu atau lebih di DCs mana gateway Anda akan terhubung ke Active Directory. Anda dapat memasukkan beberapa DCs sebagai daftar yang dipisahkan koma. Anda dapat membiarkan bidang ini kosong untuk memungkinkan DNS memilih DC secara otomatis.
8. Pilih Simpan perubahan.

Untuk membatasi akses berbagi file ke pengguna dan grup AD tertentu

1. Di konsol Storage Gateway, pilih file share yang ingin Anda batasi aksesnya.
2. Dari menu tarik-turun Tindakan, pilih Edit pengaturan akses berbagi file.
3. Di bagian Akses berbagi file pengguna dan grup, pilih pengaturan Anda.

   Untuk pengguna dan grup yang diizinkan, pilih Tambahkan pengguna yang diizinkan atau Tambahkan grup yang diizinkan dan masukkan pengguna atau grup AD yang ingin Anda izinkan akses berbagi file. Ulangi proses ini untuk memungkinkan sebanyak mungkin pengguna dan grup yang diperlukan.

   Untuk pengguna dan grup Ditolak, pilih Tambah pengguna yang ditolak atau Tambahkan grup yang ditolak dan masukkan pengguna atau grup AD yang ingin Anda tolak akses berbagi file. Ulangi proses ini untuk menolak sebanyak mungkin pengguna dan grup yang diperlukan.

> **Note**
>
> Bagian akses berbagi file pengguna dan grup hanya muncul jika Active Directory dipilih. Grup harus diawali dengan @ karakter. Format yang dapat diterima meliputi: `DOMAIN\User1`user1,`@group1`,, dan`@DOMAIN\group1`.
> Jika Anda mengonfigurasi daftar Pengguna dan Grup yang Diizinkan dan Ditolak, Windows tidak ACLs akan memberikan akses apa pun yang menggantikan daftar tersebut.
> Daftar Pengguna dan Grup yang Diizinkan dan Ditolak dievaluasi sebelumnya ACLs, dan mengontrol pengguna mana yang dapat memasang atau mengakses berbagi file. Jika ada pengguna atau grup yang ditempatkan pada daftar Diizinkan, daftar tersebut dianggap aktif, dan hanya pengguna tersebut yang dapat memasang berbagi file. Setelah pengguna memasang file share, ACLs maka berikan perlindungan yang lebih terperinci yang mengontrol file atau folder tertentu yang dapat diakses pengguna. Untuk informasi selengkapnya, lihat Mengaktifkan Windows ACLs pada berbagi file SMB baru.

4. Setelah selesai menambahkan entri, pilih Simpan.

Berikan akses tamu ke berbagi file Anda

Anda dapat mengonfigurasi Gateway File S3 Anda untuk memungkinkan akses tamu bagi setiap pengguna yang dapat memberikan nama pengguna dan kata sandi akun tamu yang benar. Jika Anda ingin ini menjadi satu-satunya metode di mana pengguna dapat mengakses gateway file Anda, maka Anda tidak perlu bergabung dengan gateway ke domain Microsoft Active Directory. Anda juga dapat menggunakan metode akses tamu ini untuk membuat berbagi file di S3 File Gateway yang merupakan anggota domain Active Directory.

Saat Anda mengonfigurasi berbagi file untuk menggunakan metode otentikasi Akses Tamu, nama pengguna akses tamu adalah`smbguest`. Sebelum Anda dapat membuat berbagi file menggunakan akses tamu, Anda perlu mengubah kata sandi default untuk `smbguest` pengguna.

Anda dapat menggunakan prosedur berikut untuk mengubah kata sandi untuk pengguna tamu`smbguest`.

Untuk mengubah kata sandi akses tamu

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

2. Pilih Gateway dari panel navigasi di sisi kiri halaman konsol, lalu pilih Nama gateway yang ingin Anda berikan akses tamu.
3. Dari menu tarik-turun Tindakan, pilih Edit pengaturan SMB, lalu pilih Pengaturan akses tamu.
4. Untuk kata sandi Tamu, masukkan kata sandi akses tamu yang ingin Anda atur, lalu pilih Simpan perubahan.

Konfigurasikan grup lokal untuk gateway Anda

Pengaturan Grup Lokal memungkinkan Anda memberikan izin khusus kepada pengguna Active Directory atau grup untuk berbagi file SMB di gateway Anda.

Anda dapat menggunakan pengaturan Grup Lokal untuk menetapkan izin Admin Gateway. Admin Gateway dapat menggunakan snap-in Shared Folder Microsoft Management Console untuk menutup paksa file yang terbuka dan terkunci.

> **Note**
>
> Anda harus menambahkan setidaknya satu pengguna atau grup Admin Gateway sebelum dapat bergabung dengan gateway Anda ke domain Direktori Aktif.

Untuk menetapkan Admin Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Gateway, lalu pilih gateway yang ingin Anda edit pengaturan SMB.
3. Dari menu tarik-turun Tindakan, pilih Edit pengaturan SMB, lalu pilih Pengaturan Grup Lokal.
4. Di bagian Pengaturan Grup Lokal, pilih pengaturan Anda. Bagian ini hanya muncul untuk berbagi file yang menggunakan Active Directory.

   Untuk Admin Gateway, tambahkan pengguna dan grup Direktori Aktif yang ingin Anda berikan izin Admin Gateway lokal. Tambahkan satu pengguna atau grup per baris, termasuk nama domain. Misalnya, **`corp\Domain Admins`**. Untuk membuat baris tambahan, pilih Tambahkan Admin Gateway baru.

> **Note**
>
> Mengedit Admin Gateway memutus dan menghubungkan kembali semua berbagi file SMB.

5. Pilih Simpan perubahan, lalu pilih Lanjutkan untuk mengakui pesan peringatan yang muncul.

Tetapkan visibilitas berbagi file

Visibilitas berbagi file mengontrol apakah pembagian di gateway terlihat saat mencantumkan saham kepada pengguna, seperti dalam tampilan bersih atau daftar penelusuran. Jika berbagi file pada gateway terlihat, maka klien dapat dengan mudah menemukan saham menggunakan browser file jika mereka tahu alamat IP gateway atau nama DNS. Jika berbagi file tidak terlihat, maka klien perlu mengetahui nama berbagi file selain IP gateway atau nama DNS untuk dapat menemukan pembagian.

> **Note**
>
> Pengaturan ini bukan metode yang efektif untuk mengamankan akses ke berbagi file dalam penerapan Anda. Untuk keamanan, kami sarankan untuk mengonfigurasi izin untuk membatasi akses ke pengguna dan grup tertentu. Untuk petunjuk, lihat Batasi akses pengguna dan grup untuk berbagi file SMB Anda.

Untuk mengatur visibilitas berbagi file

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Gateway, lalu pilih gateway yang ingin Anda edit pengaturan SMB.
3. Dari menu tarik-turun Tindakan, pilih Edit pengaturan SMB, lalu pilih Pengaturan visibilitas berbagi file.
4. Untuk status Visibilitas, pilih kotak centang jika Anda ingin pembagian di gateway ini muncul saat daftar gateway dibagikan kepada pengguna. Biarkan kotak centang tetap bersih jika Anda tidak ingin pembagian di gateway ini muncul saat daftar gateway dibagikan kepada pengguna.

Edit pengaturan untuk berbagi file SMB Anda

Anda dapat mengedit pengaturan berikut untuk berbagi file SMB yang ada:

- Nama berbagi file - pilih nama untuk berbagi file
- Log audit - aktifkan atau nonaktifkan log audit
- Daftar grup log yang ada - pilih grup log yang ada untuk log audit
- Waktu penyegaran cache file non-gateway - tentukan interval untuk menyegarkan cache berbagi file

> **Note**
>
> Menyetel nilai ini lebih pendek dari 30 menit dapat berdampak negatif pada kinerja gateway dalam situasi di mana sejumlah besar objek Amazon S3 sering dibuat atau dihapus.

- Upload peristiwa waktu penyelesaian - tentukan jumlah detik untuk menunggu setelah titik terakhir dalam waktu yang klien menulis ke file sebelum membuat pemberitahuan `ObjectUploaded`
- Kelas penyimpanan untuk objek baru - pilih kelas penyimpanan yang akan digunakan untuk objek baru yang dibuat di bucket Amazon S3 Anda
- Tebak tipe MIME - pilih apakah Anda ingin Storage Gateway menebak tipe MIME untuk objek yang diunggah berdasarkan ekstensi file
- File gateway dapat diakses oleh pemilik bucket S3 - pilih apakah akan membuat file di gateway dapat diakses oleh AWS akun yang memiliki bucket Amazon S3 yang ditautkan ke berbagi file
- Aktifkan pembayaran pemohon - pilih apakah akan meminta akun yang membaca atau meminta data dari berbagi file untuk membayar biaya akses, bukan pemilik bucket
- Ekspor sebagai - pilih apakah file diekspor dalam status baca-tulis atau hanya-baca
- Akses file dan direktori dikendalikan oleh - pilih apakah akan menggunakan izin Windows ACLs atau POSIX untuk mengontrol akses file dan direktori
- Kunci oportunistik (oplock) - pilih apakah izinkan berbagi file menggunakan penguncian oportunistik untuk mengoptimalkan strategi buffering file
- Sensitivitas kasus paksa - pilih apakah klien atau gateway mengontrol sensitivitas kasus untuk nama file dan direktori

> **Note**
>
> Jika berbagi file saat ini mengaktifkan sensitivitas huruf Force, menonaktifkannya dapat membuat file dengan nama yang identik tetapi kasus yang berbeda (misalnya, file.txt, File.txt) tidak dapat diakses. Hanya satu versi yang akan tetap dapat diakses oleh klien yang tidak peka huruf besar/kecil.

- Pencacahan berbasis akses untuk file dan direktori - pilih apakah akan membuat file dan folder pada share terlihat oleh semua pengguna selama pencacahan direktori, atau hanya untuk pengguna yang memiliki akses baca

> **Note**
>
> Anda tidak dapat mengedit berbagi file yang ada untuk menunjuk ke bucket atau titik akses baru, atau mengubah pengaturan titik akhir VPC. Anda dapat mengonfigurasi pengaturan tersebut hanya saat membuat berbagi file baru.

Untuk mengedit pengaturan berbagi file

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file, lalu pilih berbagi file yang ingin Anda perbarui.
3. Untuk Tindakan, pilih Edit setelan berbagi file.
4. Edit pengaturan apa pun yang ingin Anda ubah.
5. Pilih Simpan.

Batasi akses pengguna dan grup untuk berbagi file SMB Anda

Sebaiknya tambahkan pengguna atau grup yang diizinkan atau ditolak untuk membatasi akses ke berbagi file Anda. Jika tidak, berbagi file akan tersedia untuk semua pengguna yang diautentikasi.

Untuk mengedit setelan akses SMB

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file, lalu pilih berbagi file SMB yang ingin Anda edit.

3. Untuk Tindakan, pilih Edit setelan akses berbagi file.
4. Di bagian Akses berbagi file pengguna dan grup, pilih pengaturan Anda.

   Untuk pengguna dan grup yang diizinkan, pilih Tambahkan pengguna yang diizinkan atau Tambahkan grup yang diizinkan dan masukkan pengguna atau grup AD yang ingin Anda izinkan akses berbagi file. Ulangi proses ini untuk memungkinkan sebanyak mungkin pengguna dan grup yang diperlukan. Setiap pengguna yang tidak ada dalam daftar pengguna dan grup yang Diizinkan akan ditolak aksesnya.

   Untuk pengguna dan grup Ditolak, pilih Tambah pengguna yang ditolak atau Tambahkan grup yang ditolak dan masukkan pengguna atau grup AD yang ingin Anda tolak akses berbagi file. Ulangi proses ini untuk menolak sebanyak mungkin pengguna dan grup yang diperlukan. Jika daftar Pengguna dan grup yang Diizinkan kosong, semua pengguna selain yang ada di daftar pengguna dan grup yang Ditolak akan diberikan akses.

   > **Note**
   >
   > Masukkan hanya nama pengguna atau grup AD. Nama domain tersirat oleh keanggotaan gateway di AD tertentu tempat gateway bergabung.
   > Jika Anda tidak menentukan pengguna atau grup yang diizinkan atau ditolak, pengguna AD yang diautentikasi dapat mengekspor berbagi file.

Ubah metode enkripsi sisi server untuk berbagi file yang ada

Prosedur berikut menjelaskan cara mengubah metode enkripsi sisi server untuk berbagi file NFS atau SMB yang ada menggunakan konsol Storage Gateway. Untuk melakukan tindakan ini menggunakan Storage Gateway API, lihat Perbarui NFSFile Bagikan atau Perbarui SMBFile Bagikan di Referensi API AWS Storage Gateway.

> **Note**
>
> Memperbarui metode enkripsi menerapkan metode baru ke objek yang ada yang disimpan di bucket Amazon S3 setelah pembaruan.
> Jika Anda mengonfigurasi File Gateway untuk menggunakan SSE-KMS untuk enkripsi, Anda harus menambahkan,`kms:Encrypt`,,,, `kms:Decrypt` `kms:ReEncrypt*` `kms:GenerateDataKey`, dan `kms:DescribeKey` izin secara manual

ke peran IAM yang terkait dengan berbagi file. Untuk informasi selengkapnya, lihat Menggunakan Kebijakan Berbasis Identitas (Kebijakan IAM) untuk Storage Gateway.

Untuk mengubah metode enkripsi sisi server untuk berbagi file NFS atau SMB

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file, lalu pilih berbagi file yang ingin Anda ubah metode enkripsi.
3. Untuk Tindakan, pilih Edit enkripsi berbagi file.
4. Untuk Enkripsi, pilih jenis enkripsi yang ingin Anda gunakan untuk file saat istirahat di Amazon S3:

   - Untuk menggunakan enkripsi sisi server yang dikelola dengan Amazon S3 (SSE-S3), pilih S3-Managed Keys (SSE-S3). Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
   - Untuk menggunakan enkripsi sisi server yang dikelola dengan AWS Key Management Service (SSE-KMS), pilih KMS-Managed Keys (SSE-KMS). Untuk kunci KMS Primer, pilih kunci AWS KMS yang ada, atau pilih Buat kunci KMS baru untuk membuat kunci KMS baru di konsol Key Management Service (). AWS AWS KMS

     Untuk informasi selengkapnya AWS KMS, lihat Apa itu Layanan Manajemen AWS Kunci? di Panduan AWS Key Management Service Pengembang.
   - Untuk menggunakan enkripsi sisi server dual-layer yang dikelola dengan AWS Key Management Service (DSSE-KMS), pilih Enkripsi sisi server dual-layer dengan kunci (DSSE-KMS). AWS Key Management Service Untuk kunci KMS Primer, pilih kunci AWS KMS yang ada, atau pilih Buat kunci KMS baru untuk membuat kunci KMS baru di konsol Key Management Service (). AWS AWS KMS

     Untuk informasi selengkapnya tentang DSSE-KMS, lihat Menggunakan enkripsi sisi server dua lapis dengan AWS KMS kunci di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

     > **Note**
     >
     > Ada biaya tambahan untuk menggunakan DSSE-KMS dan kunci. AWS KMS Untuk informasi selengkapnya, lihat harga AWS KMS.

Untuk menentukan AWS KMS kunci dengan alias yang tidak terdaftar atau menggunakan AWS KMS kunci dari AWS akun yang berbeda, Anda harus menggunakan. AWS Command Line Interface Tombol KMS asimetris tidak didukung. Untuk informasi selengkapnya, lihat Membuat SMBFile Bagikan di Referensi API AWS Storage Gateway.

5. Pilih Simpan perubahan setelah selesai.

Edit pengaturan untuk berbagi file NFS Anda

Gunakan prosedur berikut untuk mengedit pengaturan untuk berbagi file NFS yang ada setelah Anda membuatnya.

> **Note**
>
> Anda tidak dapat mengedit berbagi file yang ada untuk menunjuk ke bucket atau titik akses baru, atau mengubah pengaturan titik akhir VPC. Anda dapat mengonfigurasi pengaturan tersebut hanya saat membuat berbagi file baru.

Untuk mengedit pengaturan berbagi file

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file, lalu pilih berbagi file yang ingin Anda perbarui.
3. Untuk Tindakan, pilih Edit setelan berbagi file.
4. Untuk nama berbagi file, masukkan nama untuk berbagi file.
5. Untuk log Audit, pilih salah satu dari berikut ini:

   - Untuk membuat grup log baru untuk berbagi file ini, pilih Buat grup log baru.
   - Untuk mengirim pemberitahuan kesehatan dan sumber daya untuk berbagi file ini ke grup log yang ada, pilih Gunakan dan grup log yang ada, lalu pilih grup yang diinginkan dari daftar.
   - Untuk menonaktifkan pencatatan untuk berbagi file ini, pilih Nonaktifkan logging.

   Untuk informasi selengkapnya tentang log audit, lihat Memahami log audit Gateway File S3.
6. Untuk waktu penyegaran cache file non-gateway, pilih Setel interval penyegaran, lalu atur waktu dalam Menit atau Hari untuk menyegarkan cache berbagi file menggunakan Time To Live (TTL).

TTL adalah lamanya waktu sejak penyegaran terakhir. Setelah interval TTL berlalu, mengakses direktori menyebabkan File Gateway menyegarkan konten direktori itu dari bucket Amazon S3.

> **Note**
>
> Menyetel nilai ini lebih pendek dari 30 menit dapat berdampak negatif pada kinerja gateway dalam situasi di mana sejumlah besar objek Amazon S3 sering dibuat atau dihapus.

7. Untuk Waktu penyelesaian Upload event, pilih Setel waktu penyelesaian, lalu masukkan waktu penyelesaian dalam hitungan detik. Waktu penyelesaian mengontrol penundaan minimum antara operasi penulisan klien terbaru dan pembuatan notifikasi `ObjectUploaded` log. Karena klien dapat membuat banyak penulisan kecil ke file dalam waktu singkat, kami sarankan untuk mengatur parameter ini selama mungkin untuk menghindari menghasilkan beberapa notifikasi untuk file yang sama secara berurutan. Untuk informasi selengkapnya, lihat Mendapatkan notifikasi unggahan file.
8. Untuk kelas Storage untuk objek baru, pilih kelas penyimpanan dari daftar dropdown. Untuk informasi selengkapnya tentang kelas penyimpanan, lihat Menggunakan kelas penyimpanan dengan File Gateway.
9. Di bawah metadata Object, lakukan hal berikut:

   a. Pilih jenis Guess MIME jika Anda ingin mengizinkan Storage Gateway menebak jenis media untuk objek yang diunggah berdasarkan ekstensi filenya.

   b. Pilih file Gateway yang dapat diakses oleh pemilik bucket S3, jika Anda ingin AWS akun yang memiliki bucket S3 memiliki kepemilikan penuh atas file yang dibuat oleh gateway, termasuk izin baca, tulis, edit, dan hapus.
10. Pilih Aktifkan peminta bayar jika Anda ingin pemohon file daripada pemilik bucket membayar biaya permintaan data dan mengunduh dari bucket S3.
11.
12. Untuk tingkat Akses, pilih salah satu dari berikut ini:

    - Root squash (default): Akses untuk superuser jarak jauh (root) dipetakan ke UID (65534) dan GID (65534).
    - Semua squash: Semua akses pengguna dipetakan ke User ID (UID) (65534) dan Group ID (GID) (65534).
    - Tanpa root squash: Superuser jarak jauh (root) menerima akses sebagai root.

13. Untuk Ekspor sebagai, pilih salah satu dari berikut ini:

    - Untuk memungkinkan klien membaca dan menulis file pada berbagi file, pilih Baca/Tulis.
    - Untuk memungkinkan klien membaca file tetapi tidak menulis ke berbagi file, pilih Read-only.

    > **Note**
    >
    > Untuk berbagi file yang dipasang pada klien Microsoft Windows, jika Anda memilih Read-only, Anda mungkin melihat pesan tentang kesalahan tak terduga yang mencegah Anda membuat folder. Anda dapat mengabaikan pesan ini.

14. Setelah selesai mengedit pengaturan, pilih Simpan perubahan.

Edit default metadata untuk berbagi file NFS Anda

Jika Anda tidak menyetel nilai metadata untuk file atau direktori di bucket, Gateway File S3 akan menetapkan nilai metadata default. Nilai-nilai ini termasuk izin Unix untuk file dan folder. Anda dapat mengedit default metadata di konsol Storage Gateway.

Saat Gateway File S3 Anda menyimpan file dan folder di Amazon S3, izin file Unix disimpan dalam metadata objek. Saat Gateway File S3 Anda menemukan objek yang tidak disimpan oleh Gateway File S3, objek ini diberi izin file Unix default. Anda dapat menemukan izin Unix default dalam tabel berikut.

Metadata	Deskripsi
Izin direktori	Mode direktori Unix dalam bentuk “nnnn”. Misalnya, “0666" mewakili mode akses untuk semua direktori di dalam file share. Nilai defaultnya adalah 0777.
Izin file	Mode file Unix dalam bentuk “nnnn”. Misalnya, “0666" mewakili mode file di dalam berbagi file. Nilai defaultnya adalah 0666.
ID Pengguna	ID pemilik default untuk file dalam berbagi file. Nilai defaultnya adalah 65534.

Metadata	Deskripsi
ID Grup	ID grup default untuk berbagi file. Nilai defaultnya adalah 65534.

Untuk mengedit default metadata

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file, lalu pilih berbagi file yang ingin Anda perbarui.
3. Untuk Tindakan, pilih Edit default metadata file.
4. Di kotak dialog Edit metadata file default, berikan informasi metadata dan pilih Simpan.

Batasi akses klien untuk berbagi file NFS Anda

Kami merekomendasikan mengedit pengaturan akses klien NFS untuk menentukan daftar alamat IP klien tertentu atau rentang blok CIDR untuk klien NFS yang diizinkan untuk terhubung ke berbagi file NFS Anda. Jika Anda memilih untuk tidak membatasi akses, klien mana pun di jaringan Anda dapat memasang ke berbagi file Anda.

Untuk membatasi akses klien untuk berbagi file NFS Anda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file dari panel navigasi di sisi kiri halaman konsol, lalu pilih ID berbagi file dari berbagi file NFS yang ingin Anda edit.
3. Dari menu tarik-turun Tindakan, pilih Edit pengaturan akses berbagi file.

   Bagian objek Access menampilkan daftar alamat IP dan blok CIDR yang saat ini diizinkan untuk terhubung ke berbagi file NFS. Jika akses saat ini tidak terbatas, Anda akan melihat entri di bawah Klien yang diizinkan untuk blok CIDR 0.0.0.0/0, yang menunjukkan bahwa semua IPv4 alamat yang mungkin diizinkan untuk terhubung.
4. Di bawah Klien yang diizinkan, di sebelah kanan blok CIDR 0.0.0.0/0, pilih Hapus.
5. Pilih Tambah klien, lalu berikan alamat IP atau rentang alamat dalam notasi CIDR untuk klien yang ingin Anda izinkan.

6. Ulangi langkah sebelumnya untuk menambahkan lebih banyak alamat IP atau rentang seperlunya. Jika membuat kesalahan atau perlu mencabut akses, Anda dapat memilih Hapus di sebelah kanan alamat IP atau rentang yang ingin Anda hapus dari daftar.
7. Pilih Simpan perubahan setelah selesai.

Menyegarkan cache objek bucket Amazon S3

Saat klien NFS atau SMB Anda melakukan operasi sistem file, gateway Anda menyimpan inventaris objek di cache objek Amazon S3 yang terkait dengan berbagi file Anda. Gateway Anda menggunakan inventaris yang di-cache ini untuk mengurangi latensi dan frekuensi permintaan Amazon S3. Operasi ini tidak mengimpor file ke penyimpanan cache S3 File Gateway. Ini hanya memperbarui inventaris yang di-cache untuk mencerminkan perubahan dalam inventaris objek di cache objek Amazon S3.

Untuk menyegarkan cache objek bucket S3 untuk berbagi file Anda, pilih metode yang paling sesuai dengan kasus penggunaan Anda dari daftar berikut, lalu selesaikan prosedur yang sesuai di bawah ini.

> **Note**
>
> Terlepas dari metode yang Anda gunakan, daftar direktori untuk pertama kalinya menginisialisasinya, yang menyebabkan gateway mencantumkan konten meta data direktori dari Amazon S3. Waktu yang diperlukan untuk menginisialisasi direktori sebanding dengan jumlah entri dalam direktori itu.

Topik

- Konfigurasikan jadwal penyegaran cache otomatis menggunakan konsol Storage Gateway
- Konfigurasikan jadwal penyegaran cache otomatis menggunakan AWS Lambda CloudWatch aturan Amazon
- Lakukan penyegaran cache manual menggunakan konsol Storage Gateway
- Lakukan penyegaran cache manual menggunakan Storage Gateway API

Konfigurasikan jadwal penyegaran cache otomatis menggunakan konsol Storage Gateway

Prosedur berikut mengonfigurasi jadwal penyegaran cache otomatis berdasarkan nilai Time To Live (TTL) yang Anda tentukan. Sebelum Anda mengonfigurasi jadwal penyegaran cache berbasis TTL, pertimbangkan hal berikut:

- TTL diukur sebagai lamanya waktu sejak refresh cache terakhir untuk direktori tertentu.
- Penyegaran cache berbasis TTL hanya terjadi ketika direktori tertentu diakses setelah periode TTL yang ditentukan kedaluwarsa.
- Penyegaran tidak rekursif. Itu hanya terjadi pada direktori tertentu yang diakses.
- Penyegaran menimbulkan biaya API Amazon S3 hanya pada direktori yang belum disinkronkan sejak kedaluwarsa TTL.
  - Direktori hanya disinkronkan jika diakses oleh aktivitas NFS atau SMB.
  - Sinkronisasi tidak terjadi lebih sering daripada periode TTL yang Anda tentukan.
- Mengonfigurasi penyegaran cache berbasis TTL hanya disarankan jika Anda sering memperbarui konten bucket Amazon S3 secara langsung, di luar alur kerja antara gateway dan bucket Amazon S3.
- Operasi NFS dan SMB yang mengakses direktori dengan kedaluwarsa TTLs akan diblokir sementara gateway menyegarkan isi direktori.

> **Note**
>
> Karena penyegaran cache dapat memblokir operasi akses direktori, kami sarankan untuk mengonfigurasi periode TTL terpanjang yang praktis untuk penerapan Anda.

Untuk mengonfigurasi jadwal penyegaran cache otomatis menggunakan konsol Storage Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file.
3. Pilih berbagi file yang ingin Anda konfigurasikan jadwal penyegarannya.
4. Untuk Tindakan, pilih Edit setelan berbagi file.
5. Untuk Penyegaran cache otomatis dari S3 setelahnya, pilih kotak centang dan atur waktu dalam hari, jam, dan menit untuk menyegarkan cache berbagi file menggunakan Time To Live

(TTL). TTL adalah lamanya waktu sejak penyegaran terakhir setelah itu akses ke direktori akan menyebabkan File Gateway untuk pertama menyegarkan konten direktori itu dari bucket Amazon S3.

6. Pilih Simpan perubahan.

Konfigurasikan jadwal penyegaran cache otomatis menggunakan AWS Lambda CloudWatch aturan Amazon

Untuk mengonfigurasi jadwal penyegaran cache otomatis menggunakan AWS Lambda CloudWatch aturan Amazon

1. Identifikasi bucket S3 yang digunakan oleh S3 File Gateway.
2. Periksa apakah bagian Acara kosong. Ini mengisi secara otomatis nanti.
3. Buat peran IAM, dan izinkan Hubungan Kepercayaan untuk Lambda`lambda.amazonaws.com`.
4. Gunakan kebijakan berikut.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

5. Buat fungsi Lambda dari konsol Lambda.
6. Gunakan fungsi berikut untuk tugas Lambda Anda.

```
import json
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406474878:share/
share-E51FBS9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. Untuk peran Eksekusi, pilih peran IAM yang Anda buat.
8. Opsional: tambahkan pemicu untuk Amazon S3 dan pilih acara ObjectCreatedatau. ObjectRemoved

> **Note**
>
> `RefreshCache`perlu menyelesaikan satu proses sebelum memulai yang lain. Saat Anda membuat atau menghapus banyak objek dalam bucket, performa mungkin menurun. Oleh karena itu, kami sarankan untuk tidak menggunakan pemicu S3. Sebagai gantinya, gunakan CloudWatch aturan Amazon yang dijelaskan berikut.

9. Buat CloudWatch aturan di CloudWatch konsol dan tambahkan jadwal. Umumnya, kami merekomendasikan tarif tetap 30 menit. Namun, Anda dapat menggunakan 1-2 jam pada ember S3 besar.
10. Tambahkan pemicu baru untuk CloudWatch acara dan pilih aturan yang baru saja Anda buat.
11. Simpan konfigurasi Lambda Anda. Pilih Uji.
12. Pilih S3 PUT dan sesuaikan tes dengan kebutuhan Anda.
13. Tes harus berhasil. Jika tidak, ubah JSON sesuai kebutuhan Anda dan uji ulang.
14. Buka konsol Amazon S3, dan verifikasi bahwa acara yang Anda buat dan ARN fungsi Lambda ada.
15. Unggah objek ke bucket S3 Anda menggunakan konsol Amazon S3 atau. AWS CLI

CloudWatch Konsol menghasilkan CloudWatch output yang mirip dengan yang berikut ini.

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::amzn-s3-demo-bucket', u'name':
 u'MY-GATEWAY-NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}},
 u's3SchemaVersion': u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

Pemanggilan Lambda memberi Anda output yang mirip dengan yang berikut ini.

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

Bagian NFS Anda yang dipasang pada klien Anda akan mencerminkan pembaruan ini.

> **Note**
>
> Untuk cache yang memperbarui pembuatan atau penghapusan objek besar dalam ember besar dengan jutaan objek, pembaruan mungkin memakan waktu berjam-jam.

16. Hapus objek Anda secara manual menggunakan konsol Amazon S3 atau. AWS CLI
17. Lihat bagian NFS yang dipasang pada klien Anda. Verifikasi bahwa objek Anda hilang (karena cache Anda diperbarui).
18. Periksa CloudWatch log Anda untuk melihat log penghapusan Anda dengan acara tersebut. `ObjectRemoved:Delete`

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
}
```

> **Note**
>
> Untuk pekerjaan cron atau tugas terjadwal, acara CloudWatch log Anda adalahu`'detail-type': u'Scheduled Event'`.

Lakukan penyegaran cache manual menggunakan konsol Storage Gateway

Untuk melakukan penyegaran cache manual menggunakan konsol Storage Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Berbagi file, lalu pilih berbagi file yang ingin Anda lakukan penyegaran.
3. Untuk Tindakan, pilih Segarkan cache.

   Waktu yang dibutuhkan proses penyegaran tergantung pada jumlah objek yang di-cache di gateway dan jumlah objek yang ditambahkan atau dihapus dari bucket S3.

Lakukan penyegaran cache manual menggunakan Storage Gateway API

Prosedur berikut melakukan penyegaran cache manual menggunakan Storage Gateway API. Sebelum Anda melakukan penyegaran cache berbasis API, pertimbangkan hal berikut:

- Anda dapat menentukan penyegaran rekursif atau non-rekursif.
- Penyegaran rekursif lebih intensif sumber daya, dan lebih mahal.
- Penyegaran menimbulkan biaya API Amazon S3 hanya pada direktori yang Anda berikan sebagai argumen dalam permintaan, dan keturunan direktori tersebut jika Anda menentukan penyegaran rekursif.
- Penyegaran dijalankan bersamaan dengan operasi lain saat gateway sedang digunakan.
  - Operasi NFS dan SMB umumnya tidak diblokir selama penyegaran, kecuali penyegaran aktif untuk direktori yang diakses oleh operasi.
  - Gateway tidak dapat menentukan apakah konten cache saat ini sudah basi, dan menggunakan kontennya saat ini untuk operasi NFS dan SMB terlepas dari kesegarannya.
  - Karena penyegaran cache menggunakan sumber daya perangkat keras virtual gateway, kinerja gateway mungkin berdampak negatif saat penyegaran sedang berlangsung.
- Melakukan penyegaran cache berbasis API hanya disarankan jika Anda memperbarui konten bucket Amazon S3 secara langsung, di luar alur kerja antara gateway dan bucket Amazon S3.

> **Note**
>
> Jika Anda mengetahui direktori tertentu tempat Anda memperbarui konten Amazon S3 di luar alur kerja gateway, sebaiknya tentukan direktori ini dalam permintaan penyegaran berbasis API untuk mengurangi biaya API Amazon S3 dan dampak kinerja gateway.

Untuk melakukan penyegaran cache manual menggunakan Storage Gateway API

- Kirim permintaan HTTP POST untuk menjalankan `RefreshCache` operasi dengan parameter yang Anda inginkan melalui Storage Gateway API. Untuk informasi selengkapnya, lihat RefreshCachedi Referensi API AWS Storage Gateway.

  > **Note**
  >
  > Mengirim `RefreshCache` permintaan hanya memulai operasi penyegaran cache. Ketika penyegaran cache selesai, itu tidak berarti bahwa penyegaran file selesai. Untuk

menentukan bahwa operasi penyegaran file selesai sebelum Anda memeriksa file baru di berbagi file gateway, gunakan `refresh-complete` notifikasi. Untuk melakukan ini, Anda dapat berlangganan untuk diberi tahu melalui CloudWatch acara Amazon. Untuk informasi selengkapnya, lihat Mendapatkan pemberitahuan tentang operasi file.

Menggunakan Kunci Objek S3 dengan Amazon S3 File Gateway

Amazon S3 File Gateway mendukung akses bucket S3 yang mengaktifkan Kunci Objek Amazon S3. Amazon S3 Object Lock memungkinkan Anda menyimpan objek menggunakan model “Write Once Read Many” (WORM). Saat menggunakan Kunci Objek Amazon S3, Anda dapat mencegah objek di bucket S3 dihapus atau ditimpa. Amazon S3 Object Lock bekerja sama dengan pembuatan versi objek untuk melindungi data Anda.

Jika Anda mengaktifkan Amazon S3 Object Lock, Anda masih dapat memodifikasi objek. Misalnya, dapat ditulis, dihapus, atau diganti namanya melalui berbagi file di S3 File Gateway. Ketika Anda memodifikasi objek dengan cara ini, S3 File Gateway menempatkan versi baru dari objek tanpa mempengaruhi versi sebelumnya (yaitu, objek terkunci).

Misalnya, Jika Anda menggunakan antarmuka S3 File Gateway NFS atau SMB untuk menghapus file dan objek S3 yang sesuai terkunci, gateway menempatkan penanda penghapusan S3 sebagai versi objek berikutnya, dan membiarkan versi objek asli di tempatnya. Demikian pula, Jika Gateway File S3 memodifikasi konten atau metadata dari objek yang terkunci, versi baru objek diunggah dengan perubahan, tetapi versi asli objek yang terkunci tetap tidak berubah.

Untuk informasi selengkapnya tentang Kunci Objek Amazon S3, lihat Mengunci objek menggunakan Kunci Objek S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Memahami status berbagi file

Anda dapat melihat kesehatan berbagi file secara sekilas dengan melihat statusnya. Jika status menunjukkan bahwa berbagi file berfungsi normal, tidak ada tindakan yang diperlukan di pihak Anda. Jika status menunjukkan bahwa ada masalah, Anda dapat menyelidiki untuk menentukan apakah tindakan mungkin diperlukan.

Anda dapat melihat status berbagi file di konsol Storage Gateway di kolom Status. Berbagi file yang berfungsi dengan baik menunjukkan status AVAILABLE. Ini harus menjadi status sebagian besar waktu.

Tabel berikut menjelaskan status berbagi file, apa artinya, dan apakah tindakan mungkin diperlukan.

Status	Arti
AVAILABLE	Berbagi file dikonfigurasi dengan benar dan tersedia untuk digunakan. Ini adalah status standar untuk berbagi file yang berfungsi dengan baik.
CREATING	Berbagi file belum sepenuhnya dibuat dan belum siap untuk digunakan. Status CREATING adalah transisi. Tidak ada tindakan yang diperlukan. Jika berbagi file macet dalam status ini, itu mungkin karena gateway VM kehilangan koneksi ke AWS.
UPDATING	Konfigurasi berbagi file sedang diperbarui. Status UPDATE adalah transisi. Tidak ada tindakan yang diperlukan. Jika berbagi file macet dalam status ini, itu mungkin karena gateway VM kehilangan koneksi ke AWS.
DELETING	Berbagi file sedang dihapus. Berbagi file tidak dihapus sampai semua data diunggah ke AWS. Status DELETING bersifat transisi, dan tidak ada tindakan yang diperlukan.
FORCE_DELETING	Berbagi file sedang dihapus secara paksa. Berbagi file segera dihapus dan data tidak diunggah ke AWS. Status FORCE_DELETING bersifat transisi, dan tidak ada tindakan yang diperlukan.
TIDAK TERSEDIA	Berbagi file dalam keadaan tidak sehat. Tindakan diperlukan. Beberapa kemungkinan penyebabnya termasuk kesalahan kebijakan peran atau pemetaan ke bucket Amazon S3 yang tidak ada. Ketika masalah yang menyebabkan status tidak sehat teratasi, file share kembali ke status AVAILABLE.

Memahami status gateway

Setiap gateway dalam penyebaran AWS Storage Gateway Anda memiliki status terkait yang memberi tahu Anda sekilas tentang kesehatan gateway tersebut. Sebagian besar waktu, status menunjukkan bahwa gateway berfungsi normal dan tidak ada tindakan yang diperlukan di pihak Anda. Dalam

beberapa kasus, status menunjukkan masalah yang mungkin atau mungkin tidak memerlukan tindakan dari pihak Anda.

Anda dapat melihat status untuk setiap gateway dalam penyebaran Anda di halaman Gateways dari konsol Storage Gateway. Status gateway muncul di kolom Status di sebelah nama gateway. Gateway yang berfungsi normal memiliki status`RUNNING`.

Dalam tabel berikut, Anda dapat menemukan deskripsi dari setiap status gateway, dan apakah Anda harus bertindak berdasarkan status. Sebuah gateway harus memiliki `RUNNING` status semua atau sebagian besar waktu itu digunakan.

Status	Arti
`RUNNING`	Gateway dikonfigurasi dengan benar dan tersedia untuk digunakan.
`OFFLINE`	Gateway Anda mungkin dalam `OFFLINE` status karena satu atau beberapa alasan berikut: • Gateway tidak dapat mencapai titik akhir layanan Storage Gateway. • Pintu gerbang mengalami shutdown yang tidak terduga. • Gateway memiliki disk cache terkait yang terputus, telah dimodifikasi, atau gagal.

Mengelola bandwidth untuk Gateway File Amazon S3 Anda

Anda dapat membatasi throughput unggahan dari gateway Anda AWS untuk mengontrol jumlah bandwidth jaringan yang digunakan gateway. Secara default, gateway yang diaktifkan tidak memiliki batas tarif.

Anda dapat mengonfigurasi bandwidth-rate-limit jadwal menggunakan Konsol Manajemen AWS, Kit Pengembangan AWS Perangkat Lunak (SDK), atau AWS Storage Gateway API (lihat UpdateBandwidthRateLimitScheduledi Referensi API AWS Storage Gateway.). Dengan menggunakan jadwal batas tingkat bandwidth, Anda dapat mengonfigurasi batas untuk berubah secara otomatis sepanjang hari atau minggu. Untuk informasi selengkapnya, lihat Melihat dan mengedit bandwidth-rate-limit jadwal untuk gateway Anda menggunakan konsol Storage Gateway.

Anda dapat memantau throughput upload gateway menggunakan `CloudBytesUploaded` metrik pada tab Monitoring di konsol Storage Gateway, atau di Amazon CloudWatch.

> **Note**
>
> Batas kecepatan bandwidth hanya berlaku untuk unggahan file Storage Gateway. Operasi gateway lainnya tidak terpengaruh.
> Pembatasan laju bandwidth bekerja dengan menyeimbangkan throughput semua file yang diunggah, dirata-ratakan setiap detik. Meskipun dimungkinkan untuk unggahan untuk melewati batas laju bandwidth secara singkat untuk setiap mikro atau milidetik tertentu, ini biasanya tidak menghasilkan lonjakan besar dalam jangka waktu yang lebih lama.
> Mengkonfigurasi batas kecepatan bandwidth dan jadwal saat ini tidak didukung untuk jenis Amazon FSx File Gateway.

Topik

- Melihat dan mengedit bandwidth-rate-limit jadwal untuk gateway Anda menggunakan konsol Storage Gateway
- Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for Java
- Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for .NET
- Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS Tools for Windows PowerShell

Melihat dan mengedit bandwidth-rate-limit jadwal untuk gateway Anda menggunakan konsol Storage Gateway

Bagian ini menjelaskan cara melihat dan mengedit jadwal batas laju bandwidth untuk gateway Anda.

Untuk melihat dan mengedit jadwal batas laju bandwidth

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 saat ini ditampilkan di halaman jadwal batas laju Edit bandwidth. Secara default, gateway baru tidak memiliki batas bandwidth-rate yang ditentukan.
4. (Opsional) Pilih Tambahkan batas laju bandwidth baru untuk menambahkan interval baru yang dapat dikonfigurasi ke jadwal. Untuk setiap interval yang Anda tambahkan, masukkan informasi berikut:

- Kecepatan unggah - Masukkan batas kecepatan unggah, dalam megabit per detik (Mbps). Nilai minimum adalah 100 Mbps.
- Hari dalam seminggu — Pilih hari atau hari selama setiap minggu ketika Anda ingin interval diterapkan. Anda dapat menerapkan interval pada hari kerja (Senin sampai Jumat), akhir pekan (Sabtu dan Minggu), setiap hari dalam seminggu, atau pada satu hari tertentu setiap minggu. Untuk menerapkan batas bandwidth-rate secara seragam dan terus-menerus setiap hari dan setiap saat, pilih Tidak ada jadwal.
- Waktu mulai - Masukkan waktu mulai untuk interval bandwidth, menggunakan format HH: MM dan offset zona waktu dari UTC untuk gateway Anda.

  > **Note**
  >
  > bandwidth-rate-limitInterval Anda dimulai pada awal menit yang Anda tentukan di sini.

- Waktu akhir - Masukkan waktu akhir untuk interval bandwidth, menggunakan format HH: MM dan offset zona waktu dari GMT untuk gateway Anda.

  > **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.

5. (Opsional) Ulangi langkah sebelumnya seperlunya sampai bandwidth-rate-limit jadwal Anda selesai. Jika Anda perlu menghapus interval dari jadwal Anda, pilih Hapus.

   > **Important**
   >
   > Bandwidth-rate-limitinterval tidak bisa tumpang tindih. Waktu mulai suatu interval harus terjadi setelah waktu akhir dari interval sebelumnya, dan sebelum waktu mulai interval berikutnya.

6. Setelah selesai, pilih Simpan perubahan.

Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for Java

Dengan memperbarui batas kecepatan bandwidth secara terprogram, Anda dapat menyesuaikan batas ini secara otomatis selama periode waktu—misalnya, dengan menggunakan tugas terjadwal. Contoh berikut menunjukkan cara memperbarui batas bandwidth-rate gateway menggunakan. AWS SDK for Java Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan aplikasi konsol Java. Untuk informasi selengkapnya, lihat Memulai di Panduan AWS SDK for Java Pengembang.

Example: Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for Java

Contoh kode Java berikut memperbarui batas bandwidth-rate gateway. Untuk menggunakan kode contoh ini, Anda harus memberikan titik akhir layanan, gateway Anda Amazon Resource Name (ARN), dan batas upload. 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.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   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 = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

        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, null); // download rate not
supported by S3 File Gateways

        }

        private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
            try
            {
                BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

                String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
```

```
                System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
                System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
            }
            catch (AmazonClientException ex)
            {
                System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
            }
        }
    }
```

Memperbarui Batas Tingkat Bandwidth Gateway Menggunakan AWS SDK for .NET

Dengan memperbarui batas kecepatan bandwidth secara terprogram, Anda dapat menyesuaikan batas ini secara otomatis selama periode waktu—misalnya, dengan menggunakan tugas terjadwal. Contoh berikut menunjukkan cara memperbarui batas bandwidth-rate gateway dengan menggunakan AWS Software Development Kit (SDK) untuk.NET. Untuk menggunakan kode contoh, Anda harus terbiasa dengan menjalankan aplikasi konsol.NET. Untuk informasi selengkapnya, lihat Memulai di Panduan AWS SDK for .NET Pengembang.

Example: Memperbarui Batas Tingkat Bandwidth Gateway dengan Menggunakan AWS SDK for .NET

Contoh kode C # berikut memperbarui batas kecepatan bandwidth gateway. Untuk menggunakan kode contoh ini, Anda harus memberikan titik akhir layanan, gateway Anda Amazon Resource Name (ARN), dan batas upload. 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 = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a Storage Gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);

                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
            }

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
 BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
 BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
 List<BandwidthRateLimitInterval>();
```

```
                bandwidthRateLimitIntervals.Add(noScheduleInterval);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                  new UpdateBandwidthRateLimitScheduleRequest()
                     .withGatewayARN(gatewayARN)
                     .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

                  UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                  String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                  Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                  Console.WriteLine("Upload bandwidth limit = " + uploadRate + " 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 kecepatan bandwidth secara terprogram, Anda dapat menyesuaikan batas ini 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 Nama Sumber Daya Amazon (ARN) dan batas unggahan.

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule

    .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 = 100 * 1024 * 1024
    $gatewayARN = "*** provide gateway ARN ***"

    $bandwidthRateLimitInterval = New-Object
 Amazon.StorageGateway.Model.BandwidthRateLimitInterval
    $bandwidthRateLimitInterval.StartHourOfDay = 0
    $bandwidthRateLimitInterval.StartMinuteOfHour = 0
    $bandwidthRateLimitInterval.EndHourOfDay = 23
    $bandwidthRateLimitInterval.EndMinuteOfHour = 59
    $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
    $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
 $UploadBandwidthRate

    #Update Bandwidth Rate Limits
    Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                        -BandwidthRateLimitInterval
 @($bandwidthRateLimitInterval)

    $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN
```

```
    Write-Output("`nGateway: " + $gatewayARN);
    Write-Output("`nNew bandwidth throttle schedule: " +
$schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

Memantau Storage Gateway

Topik di bagian ini menjelaskan cara memantau gateway menggunakan Amazon CloudWatch, termasuk memantau penyimpanan cache dan sumber daya lain yang terkait dengan gateway. 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 Cloud. AWS 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 Anda. Storage Gateway juga menyediakan CloudWatch alarm, kecuali alarm resolusi tinggi, tanpa biaya tambahan. Untuk informasi selengkapnya tentang CloudWatch harga, lihat CloudWatch harga Amazon. Untuk informasi selengkapnya CloudWatch, lihat Panduan CloudWatch Pengguna Amazon.

Topik

- Memahami CloudWatch alarm- Pelajari informasi dasar tentang CloudWatch alarm, termasuk status alarm dan konfigurasi yang disarankan.
- Buat CloudWatch alarm yang direkomendasikan- Pelajari bagaimana Anda dapat dengan cepat dan otomatis mengonfigurasi semua CloudWatch alarm yang direkomendasikan sebagai bagian dari proses penyiapan File Gateway awal.
- Buat CloudWatch alarm khusus- Pelajari cara membuat CloudWatch alarm khusus untuk memantau metrik tertentu menggunakan kriteria evaluasi khusus untuk memicu status alarm dan mengirim pemberitahuan.
- Memantau Gateway File Gateway S3 Anda- Pelajari cara melihat CloudWatch log dan log audit, dan temukan informasi tentang gateway spesifik dan metrik sistem file berbagi file yang dilaporkan oleh gateway Anda.

Memahami CloudWatch alarm

CloudWatch alarm memantau informasi tentang gateway Anda berdasarkan metrik dan ekspresi. Anda dapat menambahkan CloudWatch alarm untuk gateway dan melihat statusnya di konsol

Storage Gateway. Untuk setiap alarm, Anda menentukan kondisi yang akan mengaktifkan 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
- File gagal diunggah: `FilesFailingUpload` >= 1 untuk 1 titik data dalam 5 menit
- Berbagi file tidak tersedia: `FileSharesUnavailable` >= 1 untuk 1 titik data dalam 5 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 yang merupakan bagian dari klaster Ketersediaan VMware Tinggi, 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 status CloudWatch 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, lihatBuat 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 Mengonfigurasi Gateway File Amazon S3 Mengonfigurasi Gateway FSx File Anda. Jika Anda ingin menambahkan atau memperbarui CloudWatch alarm yang direkomendasikan untuk gateway yang ada setelah Anda menyelesaikan penyiapan pertama kali, 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 di sisi kiri halaman, pilih Gateway, lalu pilih gateway yang ingin Anda buat alarm yang direkomendasikan. CloudWatch
3. Pada halaman Detail untuk 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.

Buat 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 Gateway File Gateway S3 Anda

Anda dapat memantau Gateway File S3 dan sumber daya terkait AWS Storage Gateway dengan menggunakan CloudWatch metrik Amazon dan log audit. Anda juga dapat menggunakan CloudWatch Acara untuk mendapatkan pemberitahuan ketika operasi file Anda selesai.

Topik

Mendapatkan log kesehatan S3 FSx File Gateway dengan grup CloudWatch log

Anda dapat menggunakan Amazon CloudWatch Logs untuk mendapatkan informasi tentang kesehatan Gateway File S3 dan sumber daya terkait. Anda dapat menggunakan log untuk memantau gateway Anda untuk kesalahan yang ditemuinya. Selain itu, Anda dapat menggunakan filter

CloudWatch langganan Amazon untuk mengotomatiskan pemrosesan informasi log secara real time. Untuk informasi selengkapnya, lihat Pemrosesan Data Log Secara Real-time dengan Langganan di Panduan CloudWatch Pengguna Amazon.

Misalnya, Anda dapat mengonfigurasi grup CloudWatch log untuk memantau gateway dan mendapatkan pemberitahuan saat Gateway File S3 gagal mengunggah file ke bucket Amazon S3. Anda dapat mengonfigurasi grup baik ketika Anda mengaktifkan gateway atau setelah gateway Anda diaktifkan dan aktif dan berjalan. Untuk informasi tentang cara mengonfigurasi grup CloudWatch log saat mengaktifkan gateway, lihatMengonfigurasikan Gateway File Amazon S3. Untuk informasi umum tentang grup CloudWatch log, lihat Bekerja dengan Grup Log dan Aliran Log di Panduan CloudWatch Pengguna Amazon.

Berikut ini adalah contoh kesalahan yang dilaporkan oleh S3 File Gateway.

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/amzn-s3-demo-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

Kesalahan ini berarti bahwa Gateway File S3 tidak dapat mengunggah objek `myFolder/myFile.text` ke Amazon S3 karena telah beralih dari kelas penyimpanan Standar Amazon S3 ke Pengambilan Fleksibel Gletser S3 atau kelas penyimpanan S3 Glacier Deep Archive.

Dalam log kesehatan gateway sebelumnya, item-item ini menentukan informasi yang diberikan:

- `source: share-E1A2B34C`menunjukkan berbagi file yang mengalami kesalahan ini.
- `"type": "InaccessibleStorageClass"`menunjukkan jenis kesalahan yang terjadi. Dalam hal ini, kesalahan ini ditemui ketika gateway mencoba mengunggah objek yang ditentukan ke Amazon S3 atau membaca dari Amazon S3. Namun, dalam hal ini, objek tersebut telah beralih ke Amazon Glacier. Nilai `"type"` dapat berupa kesalahan apa pun yang ditemui S3 File Gateway. Untuk daftar kemungkinan kesalahan, lihatPemecahan masalah: Masalah File Gateway.
- `"operation": "S3Upload"`menunjukkan bahwa kesalahan ini terjadi ketika gateway mencoba mengunggah objek ini ke S3.

- `"key": "myFolder/myFile.text"`menunjukkan objek yang menyebabkan kegagalan.
- `gateway": "sgw-B1D123D4`menunjukkan Gateway File S3 yang mengalami kesalahan ini.
- `"timestamp": "1565740862516"`menunjukkan waktu terjadinya kesalahan.

Untuk informasi tentang cara memecahkan masalah kesalahan yang mungkin dilaporkan oleh S3 File Gateway Gateway, lihat. Pemecahan masalah: Masalah File Gateway

Mengonfigurasi grup CloudWatch log setelah gateway Anda diaktifkan

Prosedur berikut menunjukkan cara mengkonfigurasi Grup CloudWatch Log setelah gateway Anda diaktifkan.

Untuk mengonfigurasi grup CloudWatch log agar berfungsi dengan Gateway File Gateway S3 Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda konfigurasikan untuk grup CloudWatch log.
3. Untuk Tindakan, pilih Edit informasi gateway.
4. Untuk Pilih cara mengatur grup log, pilih salah satu dari berikut ini:
   - 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.
   - Nonaktifkan logging jika Anda tidak ingin memantau gateway Anda menggunakan grup CloudWatch log.
5. Pilih Simpan perubahan.
6. Untuk melihat log kesehatan untuk gateway Anda, lakukan hal berikut:
   1. Di panel navigasi, pilih Gateway, lalu pilih gateway yang Anda konfigurasikan untuk grup CloudWatch log.
   2. Pilih tab Detail, dan di bawah log Kesehatan, pilih CloudWatchLog. Halaman detail grup Log terbuka di CloudWatch konsol.

Menggunakan CloudWatch metrik Amazon

Anda bisa mendapatkan data pemantauan untuk Gateway File S3 Anda dengan menggunakan API Konsol Manajemen AWS atau CloudWatch API. Konsol menampilkan serangkaian grafik berdasarkan data mentah dari CloudWatch API. CloudWatch API juga dapat digunakan melalui salah satu AWS SDKsatau alat CloudWatch API Amazon. Tergantung kebutuhan, Anda mungkin lebih memilih menggunakan grafik yang ditampilkan di konsol atau diterima dari API.

Terlepas dari metode mana yang Anda gunakan untuk bekerja dengan metrik, Anda harus menentukan informasi berikut:

- Dimensi metrik untuk bekerja dengan. Dimensi adalah pasangan nama-nilai yang membantu Anda mengidentifikasi metrik secara unik. Dimensi untuk Storage Gateway adalah `GatewayId` dan`GatewayName`. Di CloudWatch konsol, Anda dapat menggunakan `Gateway Metrics` tampilan untuk memilih dimensi khusus gateway. Untuk informasi selengkapnya tentang dimensi, lihat Dimensi di Panduan CloudWatch Pengguna Amazon.
- Nama metrik, seperti `ReadBytes`.

Tabel berikut merangkum jenis data metrik Storage Gateway yang tersedia untuk Anda.

Ruang CloudWatch nama Amazon	Dimensi	Deskripsi
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Dimensi ini menyaring data metrik yang menjelaskan aspek gateway. Anda dapat mengidentifikasi Gateway File S3 untuk bekerja dengan menentukan dimensi `GatewayId` dan dimensi. `GatewayName` Data throughput dan latensi gateway didasarkan pada semua pembagian file di gateway. Data tersedia secara otomatis dalam periode 5 menit tanpa biaya.

Bekerja dengan gateway dan metrik file 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

Mendapatkan pemberitahuan tentang operasi file

Storage Gateway dapat memulai CloudWatch Peristiwa berikut ketika operasi file Anda selesai:

- Anda bisa mendapatkan pemberitahuan saat gateway menyelesaikan pengunggahan asinkron file Anda dari berbagi file ke Amazon S3. Gunakan `NotificationPolicy` parameter untuk meminta pemberitahuan unggahan file. Ini mengirimkan pemberitahuan untuk setiap unggahan file yang telah selesai ke Amazon S3. Untuk informasi selengkapnya, lihat Mendapatkan notifikasi unggahan file.
- Anda bisa mendapatkan pemberitahuan saat gateway menyelesaikan pengunggahan asinkron file kerja Anda dari berbagi file ke Amazon S3. Gunakan operasi NotifyWhenUploadedAPI untuk meminta pemberitahuan unggahan set file yang berfungsi. Ini mengirimkan pemberitahuan ketika semua file dalam set file yang berfungsi telah diunggah ke Amazon S3. Untuk informasi selengkapnya, lihat Mendapatkan pemberitahuan unggahan set file yang berfungsi.
- Anda bisa mendapatkan pemberitahuan saat gateway selesai menyegarkan cache untuk bucket S3 Anda. Saat Anda menjalankan RefreshCacheoperasi melalui konsol Storage Gateway atau API, berlangganan notifikasi saat operasi selesai. Untuk informasi selengkapnya, lihat Mendapatkan pemberitahuan cache refresh.

Ketika operasi file yang Anda minta selesai, Storage Gateway mengirimkan pemberitahuan melalui CloudWatch Acara. Anda dapat mengonfigurasi CloudWatch Acara untuk mengirim pemberitahuan melalui target peristiwa seperti Amazon SNS, Amazon SQS, atau fungsi. AWS Lambda Misalnya, Anda dapat mengonfigurasi target Amazon SNS untuk mengirim notifikasi ke konsumen Amazon SNS seperti email atau pesan teks. Untuk informasi tentang CloudWatch Acara, lihat Apa itu CloudWatch Acara?

Untuk mengatur pemberitahuan CloudWatch Acara

1. Buat target, seperti topik Amazon SNS atau fungsi Lambda, untuk dipanggil saat peristiwa yang Anda minta di Storage Gateway terjadi.
2. Buat aturan di konsol CloudWatch Acara untuk memanggil target berdasarkan peristiwa di Storage Gateway.
3. Dalam aturan, buat pola acara untuk jenis acara. Pemberitahuan dikirim saat acara cocok dengan pola aturan ini.
4. Pilih target dan konfigurasikan pengaturannya.

Contoh berikut menunjukkan aturan yang memulai jenis peristiwa tertentu di gateway yang ditentukan dan di AWS Wilayah tertentu. Misalnya, Anda dapat menentukan `Storage Gateway File Upload Event` sebagai jenis acara.

```
{
   "source":[
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

Untuk informasi tentang cara menggunakan aturan CloudWatch Acara, lihat Membuat aturan CloudWatch Peristiwa yang memicu peristiwa di Panduan Pengguna CloudWatch Acara Amazon.

Mendapatkan notifikasi unggahan file

Ada dua kasus penggunaan di mana Anda dapat menggunakan pemberitahuan unggahan file:

- Untuk mengotomatiskan pemrosesan file yang diunggah di cloud, Anda dapat memanggil `NotificationPolicy` parameter dan mendapatkan kembali ID notifikasi. Notifikasi yang terjadi ketika file telah diunggah memiliki ID notifikasi yang sama dengan yang dikembalikan oleh API. Jika Anda memetakan ID notifikasi ini untuk melacak daftar file yang Anda unggah, Anda dapat memulai pemrosesan file yang diunggah AWS ketika peristiwa dengan ID yang sama dihasilkan.

- Untuk kasus penggunaan distribusi konten, Anda dapat memiliki dua Gateway File S3 yang dipetakan ke bucket Amazon S3 yang sama. Klien berbagi file untuk Gateway1 dapat mengunggah file baru ke Amazon S3, dan file dibaca oleh klien berbagi file di Gateway2. File diunggah ke Amazon S3, tetapi tidak terlihat oleh Gateway2 karena menggunakan versi file yang di-cache secara lokal di Amazon S3. Untuk membuat file terlihat di Gateway2, Anda dapat menggunakan `NotificationPolicy` parameter untuk meminta pemberitahuan unggahan file dari Gateway1 untuk memberi tahu Anda ketika file unggahan selesai. Anda kemudian dapat menggunakan CloudWatch Acara untuk secara otomatis mengeluarkan RefreshCachepermintaan untuk berbagi file di Gateway2. Ketika RefreshCachepermintaan selesai, file baru terlihat di Gateway2.

Example Contoh — Pemberitahuan unggahan file

Contoh berikut menunjukkan pemberitahuan unggahan file yang dikirimkan kepada Anda CloudWatch saat acara cocok dengan aturan yang Anda buat. Pemberitahuan ini dalam format JSON. Anda dapat mengonfigurasi notifikasi ini agar dikirimkan ke target sebagai pesan teks. `detail-type` adalah `Storage Gateway Object Upload Event`.

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "amzn-s3-demo-bucket",
    }
}
```

Nama bidang	Deskripsi
versi	Versi terbaru dari kebijakan IAM.
id	ID yang mengidentifikasi kebijakan IAM.
jenis-detail	Deskripsi acara yang memulai pemberitahuan yang dikirim.
sumber	AWS Layanan yang merupakan sumber permintaan dan pemberitahuan.
akun	ID AWS akun tempat permintaan dan pemberitahuan dibuat.
Waktu	Ketika permintaan untuk mengunggah file ke Amazon S3 dibuat.
region	AWS Wilayah tempat permintaan dan pemberitahuan dikirim.
sumber daya	Sumber daya Storage Gateway yang berlaku untuk kebijakan tersebut.
ukuran objek	Ukuran objek dalam byte.
waktu modifikasi	Waktu klien memodifikasi file.
objek-kunci	Jalur ke file .
tipe-acara	CloudWatch Peristiwa yang memulai notifikasi.
prefix	Nama awalan bucket S3.
nama-ember	Nama bucket S3.

Mendapatkan pemberitahuan unggahan set file yang berfungsi

Ada dua kasus penggunaan di mana Anda dapat menggunakan pemberitahuan unggahan set file yang berfungsi:

- Untuk mengotomatiskan pemrosesan file yang diunggah di cloud, Anda dapat memanggil `NotifyWhenUploaded` API dan mendapatkan kembali ID notifikasi. Pemberitahuan yang terjadi ketika kumpulan file yang berfungsi telah diunggah memiliki ID notifikasi yang sama dengan yang dikembalikan oleh API. Jika Anda memetakan ID notifikasi ini untuk melacak daftar file yang Anda unggah, Anda dapat memulai pemrosesan kumpulan file kerja yang diunggah AWS ketika peristiwa dengan ID yang sama dihasilkan.
- Untuk kasus penggunaan distribusi konten, Anda dapat memiliki dua Gateway File S3 yang dipetakan ke bucket Amazon S3 yang sama. Klien berbagi file untuk Gateway1 dapat mengunggah file baru ke Amazon S3, dan file dibaca oleh klien berbagi file di Gateway2. File diunggah ke Amazon S3, tetapi tidak terlihat oleh Gateway2 karena menggunakan versi file yang di-cache secara lokal di S3. Untuk membuat file terlihat di Gateway2, gunakan operasi NotifyWhenUploadedAPI untuk meminta pemberitahuan unggahan file dari Gateway1, untuk memberi tahu Anda saat pengunggahan kumpulan file yang berfungsi selesai. Anda kemudian dapat menggunakan CloudWatch Acara untuk secara otomatis mengeluarkan RefreshCachepermintaan untuk berbagi file di Gateway2. Ketika RefreshCachepermintaan selesai, file baru terlihat di Gateway2. Operasi ini tidak mengimpor file ke penyimpanan cache gateway. Ini hanya memperbarui inventaris yang di-cache untuk mencerminkan perubahan dalam inventaris objek di bucket S3.

Example Contoh — Pemberitahuan unggahan set file yang berfungsi

Contoh berikut menunjukkan pemberitahuan unggahan set file yang berfungsi yang dikirimkan kepada Anda CloudWatch saat acara cocok dengan aturan yang Anda buat. Pemberitahuan ini dalam format JSON. Anda dapat mengonfigurasi notifikasi ini agar dikirimkan ke target sebagai pesan teks. `detail-type` adalah `Storage Gateway File Upload Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway File Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
```

```
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

Nama bidang	Deskripsi
versi	Versi terbaru dari kebijakan IAM.
id	ID yang mengidentifikasi kebijakan IAM.
jenis-detail	Deskripsi acara yang memulai pemberitahuan yang dikirim.
sumber	AWS Layanan yang merupakan sumber permintaan dan pemberitahuan.
akun	ID AWS akun tempat permintaan dan pemberitahuan dibuat.
Waktu	Ketika permintaan untuk mengunggah file ke Amazon S3 dibuat.
region	AWS Wilayah tempat permintaan dan pemberitahuan dikirim.
sumber daya	Sumber daya Storage Gateway yang berlaku untuk kebijakan tersebut.
tipe-acara	CloudWatch Peristiwa yang memulai notifikasi.
notifikasi-id	ID yang dihasilkan secara acak dari notifikasi yang dikirim. ID ini dalam format UUID. Ini adalah ID notifikasi yang dikembalikan saat `NotifyWhenUploaded` dipanggil.
permintaan-diterima	Ketika gateway menerima `NotifyWhenUploaded` permintaan.

Nama bidang	Deskripsi
selesai	Ketika semua file dalam set kerja diunggah ke Amazon S3.

Mendapatkan pemberitahuan cache refresh

Untuk kasus penggunaan notifikasi cache refresh, Anda dapat memiliki dua Gateway File S3 yang dipetakan ke bucket Amazon S3 yang sama dan klien NFS untuk Gateway1 mengunggah file baru ke bucket S3. File diunggah ke Amazon S3, tetapi tidak muncul di Gateway2 sampai Anda menyegarkan cache. Ini karena Gateway2 menggunakan versi file yang di-cache secara lokal di Amazon S3. Anda mungkin ingin melakukan sesuatu dengan file di Gateway2 saat cache penyegaran selesai. File besar bisa memakan waktu beberapa saat untuk muncul di Gateway2, jadi Anda mungkin ingin diberi tahu saat penyegaran cache selesai. Anda dapat meminta pemberitahuan cache refresh dari Gateway2 untuk memberi tahu Anda ketika semua file terlihat di Gateway2.

Example Contoh — Segarkan pemberitahuan cache

Contoh berikut menunjukkan pemberitahuan cache refresh yang dikirimkan kepada Anda CloudWatch saat acara cocok dengan aturan yang Anda buat. Pemberitahuan ini dalam format JSON. Anda dapat mengonfigurasi notifikasi ini agar dikirimkan ke target sebagai pesan teks. `detail-type` adalah `Storage Gateway Refresh Cache Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
```

```
        "folderList": [
            "/"
        ]
    }
}
```

Nama bidang	Deskripsi
versi	Versi terbaru dari kebijakan IAM.
id	ID yang mengidentifikasi kebijakan IAM.
jenis-detail	Deskripsi jenis acara yang memulai notifikasi yang dikirim.
sumber	AWS Layanan yang merupakan sumber permintaan dan pemberitahuan.
akun	ID AWS akun tempat permintaan dan pemberitahuan dibuat.
Waktu	Ketika permintaan untuk me-refresh file dalam set kerja dibuat.
region	AWS Wilayah tempat permintaan dan pemberitahuan dikirim.
sumber daya	Sumber daya Storage Gateway yang berlaku untuk kebijakan tersebut.
tipe-acara	CloudWatch Peristiwa yang memulai notifikasi.
notifikasi-id	ID yang dihasilkan secara acak dari notifikasi yang dikirim. ID ini dalam format UUID. Ini adalah ID notifikasi yang dikembalikan saat Anda meneleponRefreshCache .
dimulai	ketika gateway menerima RefreshCache permintaan dan penyegaran dimulai.

Nama bidang	Deskripsi
selesai	Saat penyegaran set kerja selesai.
folderList	Daftar jalur folder yang dipisahkan koma yang disegarkan dalam cache. Defaultnya adalah [”/"].

Memahami metrik gateway

Tabel berikut menjelaskan metrik yang mencakup S3 File Gateways. Setiap gateway memiliki satu set metrik yang terkait dengannya. Beberapa metrik khusus gateway memiliki nama yang sama dengan metrik tertentu. file-share-specific Metrik ini mewakili jenis pengukuran yang sama, tetapi dicakup ke gateway daripada berbagi file.

Selalu tentukan apakah Anda ingin bekerja dengan gateway atau berbagi file saat bekerja dengan metrik tertentu. Secara khusus, saat bekerja dengan metrik gateway, Anda harus menentukan `Gateway Name` gateway yang data metriknya ingin Anda lihat. 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 yang dapat Anda gunakan untuk mendapatkan informasi tentang Gateway File S3.

Metrik	Deskripsi
`AuditNotifications`	Metrik ini melaporkan jumlah log audit yang dipancarkan. Unit: Hitungan

Metrik	Deskripsi
`AvailabilityNotifications`	Metrik ini melaporkan jumlah pemberitahuan kesehatan terkait ketersediaan yang dihasilkan oleh gateway dalam periode pelaporan. Unit: Hitungan
`CacheFileSize`	Metrik ini melacak ukuran file di cache gateway. Gunakan metrik ini dengan `Average` statistik untuk mengukur ukuran rata-rata file di cache gateway. Gunakan metrik ini dengan `Max` statistik untuk mengukur ukuran maksimum file di cache gateway. Unit: Byte
`CacheFree`	Metrik ini melaporkan jumlah byte yang tersedia di cache gateway. Unit: Byte
`CacheHitPercent`	Persentase operasi membaca aplikasi dari gateway yang dilayani dari cache. Sampel diambil pada akhir periode pelaporan. Ketika tidak ada operasi baca aplikasi dari gateway, metrik ini melaporkan 100 persen. 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
`CachePercentUsed`	Persentase cache data yang digunakan di seluruh gateway. Sampel diambil pada akhir periode pelaporan. Unit: Persen
`CacheUsed`	Metrik ini melaporkan jumlah byte yang digunakan dalam cache gateway. Unit: Byte
`CloudBytesDownloaded`	Jumlah total byte yang diunduh gateway AWS selama periode pelaporan. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur IOPS. Unit: Byte

Metrik	Deskripsi
`CloudBytesUploaded`	Jumlah total byte yang diunggah gateway AWS selama periode pelaporan. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur input/output operasi per detik (IOPS). Unit: Byte
`FilesFailingUpload`	Metrik ini melacak jumlah file yang gagal diunggah. AWS File-file ini akan menghasilkan pemberitahuan kesehatan yang berisi informasi lebih lanjut tentang masalah ini. Gunakan metrik ini dengan `Sum` statistik untuk menunjukkan jumlah file yang saat ini gagal diunggah. AWS Unit: Hitungan
`FileSharesUnavailable`	Metrik ini memberikan jumlah pembagian file di gateway ini yang berada dalam status Tidak Tersedia. Jika metrik ini melaporkan bahwa pembagian file tidak tersedia, kemungkinan besar ada masalah dengan gateway yang dapat menyebabkan gangguan pada alur kerja Anda. Disarankan untuk membuat alarm ketika metrik ini melaporkan nilai bukan nol. Unit: Hitungan

Metrik	Deskripsi
FilesRenamed	Metrik ini melacak jumlah file yang diganti namanya dalam periode pelaporan. Unit: Hitungan
HealthNotifications	Metrik ini melaporkan jumlah pemberitahuan kesehatan yang dihasilkan oleh gateway ini dalam periode pelaporan. Unit: Hitungan
IndexEvictions	Metrik ini melaporkan jumlah file yang metadatanya diusir dari indeks cache metadata file untuk memberi ruang bagi entri baru. Gateway mempertahankan indeks metadata ini, yang dihuni dari AWS Cloud sesuai permintaa n. Unit: Hitungan
IndexFetches	Metrik ini melaporkan jumlah file yang metadatanya diambil. Gateway mempertah ankan indeks metadata file yang di-cache, yang diisi dari Cloud sesuai permintaan. AWS Unit: Hitungan
IoWaitPercent	Metrik ini melaporkan persentase waktu CPU menunggu respons dari disk lokal. Unit: Persen
MemTotalBytes	Metrik ini melaporkan jumlah total memori pada gateway. Unit: Byte

Metrik	Deskripsi
MemUsedBytes	Metrik ini melaporkan jumlah memori yang digunakan pada gateway. Unit: Byte
NfsSessions	Metrik ini melaporkan jumlah sesi NFS yang aktif di gateway. Unit: Hitungan
RootDiskFreeBytes	Metrik ini melaporkan jumlah byte yang tersedia pada disk root gateway. Jika laporan metrik ini kurang dari 20 GB gratis, Anda harus meningkatkan ukuran disk root. Untuk meningkatkan ukuran disk root, Anda dapat meningkatkan ukuran disk root yang ada pada VM. Saat VM di-boot ulang, gateway mengenali peningkatan ukuran pada disk root. Unit: Byte
S3GetObjectRequestTime	Metrik ini melaporkan waktu gateway untuk menyelesaikan permintaan objek S3 get. Unit: Milidetik
S3PutObjectRequestTime	Metrik ini melaporkan waktu gateway untuk menyelesaikan permintaan objek put S3. Unit: Milidetik
S3UploadPartRequestTime	Metrik ini melaporkan waktu gateway untuk menyelesaikan permintaan bagian unggahan S3. Unit: Milidetik

Metrik	Deskripsi
`SmbV1Sessions`	Metrik ini melaporkan jumlah SMBv1 sesi yang aktif di gateway. Unit: Hitungan
`SmbV2Sessions`	Metrik ini melaporkan jumlah SMBv2 sesi yang aktif di gateway. Unit: Hitungan
`SmbV3Sessions`	Metrik ini melaporkan jumlah SMBv3 sesi yang aktif di gateway. Unit: Hitungan
`TotalCacheSize`	Metrik ini melaporkan ukuran total cache. Unit: Byte
`UserCpuPercent`	Metrik ini melaporkan persentase waktu yang dihabiskan untuk pemrosesan gateway. Unit: Persen

Memahami metrik berbagi file

Anda dapat menemukan informasi berikut tentang metrik Storage Gateway yang mencakup berbagi file. Setiap file share memiliki satu set metrik yang terkait dengannya. Beberapa metrik khusus berbagi file memiliki nama yang sama dengan metrik khusus gateway tertentu. Metrik ini mewakili jenis pengukuran yang sama, tetapi dicakup ke berbagi file sebagai gantinya.

Selalu tentukan apakah Anda ingin bekerja dengan gateway atau metrik berbagi file sebelum bekerja dengan metrik. Secara khusus, saat bekerja dengan metrik berbagi file, Anda harus menentukan `File share ID` yang mengidentifikasi berbagi file yang Anda minati untuk melihat 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 pembagian file Anda.

Metrik	Deskripsi
`CacheHitPercent`	Persentase operasi membaca aplikasi dari berbagi file yang disajikan dari cache. Sampel diambil pada akhir periode pelaporan. Ketika tidak ada operasi pembacaan aplikasi dari berbagi file, metrik ini melaporkan 100 persen. Unit: Persen
`CachePercentDirty`	Kontribusi berbagi file terhadap 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. **Note** Gunakan `CachePercentDirty` metrik gateway untuk melihat persentase keseluruhan cache gateway yang belum dipertahankan. AWS

Metrik	Deskripsi
	Unit: Persen
`CachePercentUsed`	Persentase cache data yang digunakan di seluruh gateway. Sampel diambil pada akhir periode pelaporan. Metrik khusus berbagi file ini melaporkan nilai yang sama dengan metrik khusus gateway yang sesuai. Unit: Persen
`CloudBytesUploaded`	Jumlah total byte yang diunggah gateway AWS selama periode pelaporan. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur IOPS. Unit: Byte
`CloudBytesDownloaded`	Jumlah total byte yang diunduh gateway AWS selama periode pelaporan. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur input/output operasi per detik (IOPS). Unit: Byte

Metrik	Deskripsi
`FilesFailingUpload`	Metrik ini melacak jumlah file yang gagal diunggah. AWS File-file ini akan menghasilkan pemberitahuan kesehatan yang berisi informasi lebih lanjut tentang masalah ini. Gunakan metrik ini dengan `Sum` statistik untuk menunjukkan jumlah file yang saat ini gagal diunggah. AWS Unit: Hitungan
`ReadBytes`	Jumlah total byte yang dibaca dari aplikasi lokal Anda dalam periode pelaporan untuk berbagi file. Gunakan metrik ini dengan `Sum` statistik untuk mengukur throughput dan dengan `Samples` statistik untuk mengukur IOPS. Unit: Byte
`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: Byte

Memahami log audit File Gateway S3

Log audit Amazon S3 File Gateway (S3 File Gateway) memberi Anda detail tentang akses pengguna ke file dan folder dalam berbagi file. Anda dapat menggunakannya untuk memantau aktivitas pengguna dan mengambil tindakan jika pola aktivitas yang tidak pantas diidentifikasi.

Operasi

Tabel berikut menjelaskan operasi akses file log audit S3 FSx File Gateway.

Nama operasi	Definisi
Baca Data	Baca isi file.
Tulis Data	Ubah isi file.
Buat	Buat file atau folder baru.
Ubah Nama	Ganti nama file atau folder yang ada.
Delete	Hapus file atau folder.
Tulis Atribut	Perbarui metadata file atau folder (ACLs, pemilik, grup, izin).

Atribut

Tabel berikut menjelaskan atribut akses file log audit S3 File Gateway.

Atribut	Definisi
`accessMode`	Pengaturan izin untuk objek.
`accountDomain` (Hanya SMB)	Domain Active Directory (AD) yang menjadi milik akun klien.
`accountName` (Hanya SMB)	Nama pengguna Active Directory klien.
`bucket`	Nama ember S3.
`clientGid` (Hanya NFS)	Pengidentifikasi grup pengguna yang mengakses objek.
`clientUid` (Hanya NFS)	Pengidentifikasi pengguna yang mengakses objek.
`ctime`	Waktu konten atau metadata objek dimodifik asi, ditetapkan oleh klien.

Atribut	Definisi
`groupId`	Pengidentifikasi untuk pemilik grup objek.
`fileSizeInBytes`	Ukuran file dalam byte, ditetapkan oleh klien pada waktu pembuatan file.
`gateway`	ID Storage Gateway.
`mtime`	Kali ini konten objek dimodifikasi, ditetapkan oleh klien.
`newObjectName`	Jalur lengkap ke objek baru setelah diganti namanya.
`objectName`	Jalur penuh ke objek.
`objectType`	Mendefinisikan apakah objek adalah file atau folder.
`operation`	Nama operasi akses objek.
`ownerId`	Pengidentifikasi untuk pemilik objek.
`securityDescriptor` (Hanya SMB)	Menampilkan daftar kontrol akses diskresioner (DACL) yang disetel pada objek, dalam format SDDL.
`shareName`	Nama saham yang sedang diakses.
`source`	ID dari file share yang sedang diaudit.
`sourceAddress`	Alamat IP mesin klien berbagi file.
`status`	Status operasi. Hanya keberhasilan yang dicatat (kegagalan dicatat dengan pengecual ian kegagalan yang timbul dari izin ditolak).
`timestamp`	Waktu operasi terjadi berdasarkan stempel waktu OS gateway.

Atribut	Definisi
`version`	Versi format log audit.

Atribut dicatat per operasi

Tabel berikut menjelaskan atribut log audit S3 File Gateway yang dicatat di setiap operasi akses file.

	Baca data	Tulis data	Buat folder	Buat file	Ganti nama file/ folder	Hapus file/ folder	Tulis atribut (ubah ACL - hanya SMB)	Tulis atribut (chown)	Tulis atribut (chmod)	Tulis atribut (chgrp)
`access e`			X	X					X	
`accoun main (I SMB)`	X	X	X	X	X	X	X	X	X	X
`accoun me (Ha SMB)`	X	X	X	X	X	X	X	X	X	X
`bucket`	X	X	X	X	X	X	X	X	X	X
`client` (Hanya NFS)	X	X	X	X	X	X		X	X	X
`client` (Hanya NFS)	X	X	X	X	X	X		X	X	X
`ctime`			X	X						

	Baca data	Tulis data	Buat folder	Buat file	Ganti nama file/ folder	Hapus file/ folder	Tulis atribut (ubah ACL - hanya SMB)	Tulis atribut (chown)	Tulis atribut (chmod)	Tulis atribut (chgrp)
groupI			X	X						
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObj Name					X					
object e	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securi escrip (Hanya SMB)							X	X		
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X

	Baca data	Tulis data	Buat folder	Buat file	Ganti nama file/ folder	Hapus file/ folder	Tulis atribut (ubah ACL - hanya SMB)	Tulis atribut (chown)	Tulis atribut (chmod)	Tulis atribut (chgrp)
`source ress`	X	X	X	X	X	X	X	X	X	X
`status`	X	X	X	X	X	X	X	X	X	X
`timest`	X	X	X	X	X	X	X	X	X	X
`versic`	X	X	X	X	X	X	X	X	X	X

Buat laporan cache untuk Gateway File S3 Anda

S3 File Gateway dapat menghasilkan laporan metadata untuk file yang saat ini berada di cache unggahan lokal untuk berbagi file tertentu. Anda dapat menerapkan filter dan kriteria tambahan yang menentukan jenis file cache tertentu yang muncul dalam laporan. Anda dapat menggunakan laporan ini untuk membantu mengidentifikasi dan menyelesaikan masalah gateway. Misalnya, jika file gagal diunggah dari gateway ke Amazon S3, Anda dapat membuat laporan yang mencantumkan file tertentu yang gagal diunggah, dan alasan kegagalan unggahan. Laporan adalah file CSV yang berisi daftar file yang cocok dengan set parameter filter yang Anda tentukan. File keluaran disimpan sebagai objek Amazon S3 di lokasi bucket yang Anda tentukan saat mengonfigurasi laporan. Untuk membuat laporan cache menggunakan AWS Storage Gateway API, lihat StartCacheReportdi Referensi API Storage Gateway. Untuk membuat laporan cache di konsol Storage Gateway, gunakan prosedur berikut.

Prasyarat

- Gateway Anda harus memiliki `s3:PutObject` dan `s3:AbortMultipartUpload` izin untuk bucket Amazon S3 tempat Anda ingin menyimpan laporan cache.
- Tidak ada laporan cache lain yang saat ini sedang dalam proses untuk berbagi file.
- Harus ada kurang dari 10 laporan cache yang ada untuk berbagi file.

- Gateway harus online dan terhubung ke AWS.
- Disk root gateway harus memiliki setidaknya 20GB ruang kosong.

Untuk membuat laporan cache menggunakan konsol Storage Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah/.
2. Di panel navigasi di sisi kiri halaman, pilih Berbagi file, lalu pilih berbagi file yang ingin Anda buat laporan cache.
3. Dari menu tarik-turun Tindakan, pilih Buat laporan cache.
4. Untuk lokasi Amazon S3, masukkan bucket Amazon S3 dan awalan lokasi tempat Anda ingin menyimpan objek file CSV laporan cache yang sudah selesai di Amazon S3. Untuk memilih bucket dan awalan dari penyimpanan Amazon S3 yang ada, pilih Browse S3.
5. Untuk peran IAM, lakukan salah satu hal berikut untuk menentukan peran IAM yang memberikan izin Gateway File Anda untuk membuat dan menyimpan laporan cache Anda:

   - Untuk menentukan peran IAM yang ada, pilih peran dari daftar drop-down.
   - Untuk membuat peran IAM baru secara manual, pilih Buat peran, lalu buat peran baru menggunakan konsol IAM.

   > **Note**
   >
   > Peran IAM yang Anda tentukan harus memiliki izin berikut ini untuk menuliskan objek ke lokasi Amazon S3 bucket laporan, dan untuk menghentikan unggahan multibagian ke bucket laporan:
   >
   > - `s3:PutObject`
   > - `s3:AbortMultipartUpload`
   >
   > Peran juga harus memungkinkan `storagegateway.amazonaws.com` layanan untuk mengambil peran menggunakan `sts:AssumeRole` tindakan.

6. Untuk filter Laporan, lakukan salah satu hal berikut untuk menentukan file mana yang akan disertakan dalam laporan cache:

   - Untuk menyertakan semua file cache yang saat ini gagal diunggah ke Amazon S3, pilih Semua file yang gagal diunggah.

- Untuk menyertakan hanya file-file yang gagal diunggah ke Amazon S3 karena alasan tertentu, pilih Alasan kegagalan unggahan khusus saja. Kemudian, untuk alasan Kegagalan, pilih satu atau beberapa alasan berikut:
  - Kelas penyimpanan yang tidak dapat diakses - Gateway tidak dapat mengakses kelas penyimpanan Amazon S3 tempat objek disimpan. Untuk informasi selengkapnya, lihat Kesalahan: InaccessibleStorageClass.
  - Status objek tidak valid - Status file di gateway tidak cocok dengan statusnya di Amazon S3. Untuk informasi selengkapnya, lihat Kesalahan: InvalidObjectState.
  - Objek hilang - Objek telah dihapus atau dipindahkan di Amazon S3. Untuk informasi selengkapnya, lihat Kesalahan: ObjectMissing.
  - Akses S3 Ditolak - Peran IAM akses bucket Amazon S3 tidak mengizinkan gateway untuk melakukan operasi pengunggahan. Untuk informasi selengkapnya, lihat Kesalahan: S3 AccessDenied.

> **Note**
>
> Flag Files Failing Upload diatur ulang setiap 24 jam dan selama reboot gateway. Jika laporan ini menangkap file setelah reset, tetapi sebelum ditandai lagi, mereka tidak akan dilaporkan sebagai File Failing Upload.

7. Untuk Menggunakan titik akhir VPC untuk terhubung ke S3? , lakukan salah satu hal berikut untuk menentukan bagaimana gateway Anda akan terhubung ke bucket Amazon S3:

   - Untuk terhubung langsung tanpa menggunakan Amazon VPC, pilih Connect langsung ke bucket.
   - Untuk menelusuri daftar titik akhir VPC Amazon yang ada, pilih Pilih titik akhir VPC, lalu tentukan titik akhir dari daftar drop-down titik akhir VPC yang muncul.
   - Untuk menentukan titik akhir VPC Amazon yang ada dengan nama DNS-nya, pilih Masukkan nama DNS titik akhir VPC, lalu masukkan nama DNS di bidang nama DNS titik akhir VPC yang muncul.

   > **Note**
   >
   > Jika berbagi file Anda menggunakan titik akhir VPC untuk terhubung ke Amazon S3 untuk operasi normal, sebaiknya gunakan VPC yang sama saat mengonfigurasi laporan

cache. Pembuatan laporan cache akan gagal jika gateway tidak dapat terhubung ke bucket Amazon S3 karena alasan apa pun, termasuk konfigurasi VPC yang tidak valid.

8. (Opsional) Di bawah Tag - opsional, pilih Tambahkan tag baru, lalu masukkan Kunci dan Nilai untuk laporan cache Anda.

   Tag adalah pasangan nilai kunci peka huruf besar/kecil yang membantu Anda mengkategorikan sumber daya Storage Gateway Anda. Menambahkan tag dapat membuat pemfilteran dan pencarian laporan cache Anda lebih mudah. Anda dapat mengulangi langkah ini untuk menambahkan hingga 50 tag.

9. Pilih Buat laporan setelah selesai.

   Storage Gateway mulai menghasilkan laporan. Anda dapat memeriksa kemajuan dan melihat status pada tab Laporan cache pada halaman detail untuk berbagi file.

Melihat dan mengelola laporan cache untuk S3 File Gateway Anda

Laporan cache mencantumkan file yang saat ini berada di cache lokal untuk berbagi file tertentu, sesuai dengan filter dan kriteria yang Anda tentukan. Anda dapat melihat daftar laporan cache yang ada untuk berbagi file tertentu, memeriksa kemajuan dan status laporan, dan menghapus laporan yang tidak lagi Anda perlukan menggunakan AWS Storage Gateway API atau konsol Storage Gateway.

Untuk mengelola laporan cache menggunakan API, lihat bagian berikut di Referensi API Storage Gateway:

- ListCacheReports
- DescribeCacheReport
- CancelCacheReport
- DeleteCacheReport

Untuk mengelola laporan cache di konsol Storage Gateway, gunakan prosedur berikut.

Untuk mengelola laporan cache menggunakan konsol Storage Gateway

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

2. Di panel navigasi di sisi kiri halaman, pilih Berbagi file, lalu pilih berbagi file yang ingin Anda kelola laporan cache.
3. Pada halaman Detail untuk berbagi file, pilih tab Laporan cache. Tab ini mencantumkan laporan cache yang ada untuk berbagi file, dan memberikan informasi tentang status, kemajuan, dan jalur objek tempat file laporan disimpan di Amazon S3.
4. Lakukan salah satu tindakan berikut:

   - Untuk melihat detail tambahan untuk laporan tertentu, seperti ARN laporan dan tag terkait, pilih laporan dari kolom ID Laporan.
   - Untuk menentukan beberapa laporan yang akan dikelola secara bersamaan, pilih laporan menggunakan kolom kotak centang.
5. Untuk mengelola satu atau beberapa laporan, pilih salah satu dari berikut ini dari menu tarik-turun Tindakan:

   - Hapus laporan cache — Ini menghapus catatan laporan cache dari database Storage Gateway. Hapus catatan untuk laporan cache usang untuk memberi ruang bagi laporan baru. Setiap berbagi file dapat memiliki hingga 10 laporan cache yang ada kapan saja.

     > **Note**
     >
     > Menghapus catatan laporan cache menggunakan prosedur ini tidak menghapus objek file laporan dari Amazon S3.

   - Batalkan laporan — Ini membatalkan laporan yang sedang berlangsung. Batalkan laporan yang sedang berlangsung jika Anda membuat kesalahan selama konfigurasi laporan, atau jika laporan membutuhkan waktu yang sangat lama untuk diselesaikan. Konfirmasikan pembatalan saat diminta.

     > **Note**
     >
     > Waktu penyelesaian dapat bervariasi secara signifikan tergantung pada jumlah file dalam cache. Biasanya, sebagian besar laporan selesai dalam 5 menit.

   Konsol Storage Gateway menampilkan pesan yang menunjukkan hasil tindakan pembatalan atau penghapusan.

Memahami informasi yang disediakan dalam laporan cache S3 File Gateway

Laporan cache mencantumkan file yang saat ini berada di cache lokal untuk berbagi file tertentu, sesuai dengan filter dan kriteria yang Anda tentukan. Setiap laporan cache mencakup informasi berikut:

- Bucket — Bucket Amazon S3 atau Access Point yang terkait dengan berbagi file.
- S3 ObjectKey — Objek Amazon S3 yang menyimpan data dan metadata untuk file ini. Objek ini memiliki data terbaru yang telah diunggah ke S3, tetapi bisa jadi data yang hilang yang gagal diunggah ke S3.
- FilePath— Jalur file untuk entri file di cache gateway. Di sinilah Anda dapat menemukan file saat memasang dan menjelajahi berbagi file.
- RenamedTo— Jalur baru dari file yang diganti namanya. Saat Anda mengganti nama file pada file share Anda, gateway perlu melacak lokasi lama dan baru file tersebut. Bidang ini menunjukkan ke mana file dipindahkan, membantu Anda melacak operasi penggantian nama file - bahkan jika file telah diganti namanya beberapa kali. Informasi ini sangat berguna ketika Anda perlu memahami bagaimana file dalam berbagi file Anda sesuai dengan objek di bucket Amazon S3 Anda.

  Contoh berikut menunjukkan entri laporan cache untuk skenario kompleks yang melibatkan file yang ditimpa langsung di Amazon S3, sementara juga diganti namanya melalui File Gateway. Dalam skenario ini, gateway mengunggah file `A.txt` ke S3, dan kemudian mengusir konten file untuk membuat ruang di cache lokal. Objek S3 terkait kemudian ditimpa langsung di S3 — bukan melalui tindakan yang diambil oleh gateway — yang mengakibatkan ketidakcocokan antara objek `InvalidObjectState` S3 dan apa yang diharapkan gateway. Pada saat yang sama, file `A.txt` diubah namanya menjadi `B.txt` melalui gateway.

Bucket	S3 ObjectK	FilePat	Renam	Tipe	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplo	Upload or	SizeInB es	IsWholeFi leInCache
sample ket-iad	A.txt	/B.txt		FAIL	BETU	SALAH	SALAH	BETUL	Invalid(jectSta	4	SALAH

Bucket	S3 ObjectK	FilePat	Renam	Tipe	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplc	Upload or	SizeInE es	IsWholeFi leInCache
sample ket-iad	A.txt	/A.txt	/B.txt	FAIL	BETU	SALAH	BETUL	SALAH		4	SALAH

- Jenis - Menunjukkan apakah entri adalah untuk `FILE` atau`DIRECTORY`.
- IsDirty— Laporkan `TRUE` jika ada jenis perubahan pada file yang belum diunggah ke Amazon S3. Ini termasuk perubahan metadata seperti nama file dan read/write izin, bahkan jika data file tidak berubah.
- IsDataDirty— Laporkan `TRUE` jika ada perubahan pada data file yang belum diunggah ke Amazon S3.
- IsDeleted— Melaporkan `TRUE` jika file telah dihapus di gateway. Jika file ditandai sebagai dihapus, maka itu akan selalu ditandai sebagai kotor.
- IsFailingToUpload— Laporkan `TRUE` jika ada masalah saat mengunggah file ke Amazon S3. Status ini disetel ulang setiap 24 jam untuk memungkinkan gateway mencoba ulang unggahan dan memeriksa apakah masalah telah teratasi. Gateway menolak operasi penulisan baru untuk file yang gagal diunggah. Jika gateway tidak memiliki seluruh file dalam cache, maka gateway juga menolak operasi baca.
- UploadError— Kesalahan yang mencegah file diunggah ke Amazon S3. Untuk informasi selengkapnya dan langkah-langkah yang disarankan untuk mengatasi kesalahan ini, lihat Pemecahan Masalah: Masalah Gateway File.
- SizeInBytes— Ukuran total file.
- IsWholeFileInCache— Laporkan `TRUE` jika semua data file saat ini disimpan di cache gateway. Jika ini BENAR untuk file yang gagal diunggah ke Amazon S3, maka gateway akan memungkinkan file dibaca.

Mempertahankan gateway Anda

Mempertahankan Anda Amazon S3 File Gateway melibatkan melakukan pemeliharaan umum untuk mengoptimalkan kinerja gateway Anda. Tugas-tugas ini umum untuk semua jenis gateway.

Bagian ini berisi topik-topik berikut, yang menjelaskan konsep dan prosedur yang terkait dengan pemeliharaan Anda:

Topik

- Mengelola pembaruan gateway— Pelajari cara mengaktifkan atau menonaktifkan pembaruan pemeliharaan, dan memodifikasi jadwal jendela pemeliharaan untuk File Gateway Anda.
- Melakukan tugas pemeliharaan menggunakan konsol lokal— Pelajari cara melakukan tugas pemeliharaan menggunakan konsol lokal gateway.
- 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.
- Mengganti yang sudah ada Gerbang File S3 dengan contoh baru— Pelajari cara mengganti S3 File Gateway Gateway Anda dengan instance baru saat Anda ingin meningkatkan kinerja atau menanggapi pemberitahuan untuk memigrasi gateway.
- 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 pembaruan gateway

Storage Gateway terdiri dari komponen layanan cloud terkelola dan komponen alat gateway yang Anda terapkan baik lokal, atau di instans Amazon EC2 di cloud. AWS 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 instalasi atau kontennya 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 tidak berfungsi.
Storage Gateway secara otomatis dan teratur menambal alat untuk menjaga keamanan dan stabilitas. Peralatan Storage Gateway menggunakan Amazon Linux sebagai sistem operasi dasar mereka. Anda dapat memeriksa status masalah Kerentanan Umum dan Eksposur (CVE) yang terdeteksi di Pusat Keamanan Amazon Linux. Tambalan CVE diterapkan secara otomatis dalam waktu 30 hari setelah dirilis, seperti yang ditunjukkan di Pusat Keamanan Amazon Linux. Patch dipasang selama jadwal pemeliharaan gateway Anda, asalkan gateway Anda online.
Storage Gateway tidak mendukung pembaruan gateway Amazon EC2 secara manual menggunakan arahan cloud-init. Jika Anda menggunakan metode ini untuk memperbarui gateway, Anda mungkin mengalami masalah interoperabilitas yang mencegah Anda mengaktifkan atau menggunakan alat gateway.

Perbarui frekuensi dan perilaku yang diharapkan

AWS memperbarui komponen layanan cloud sesuai kebutuhan tanpa menyebabkan gangguan pada gateway yang digunakan. Peralatan gateway yang Anda gunakan menerima jenis pembaruan berikut:

- Pemeliharaan - Pembaruan rutin yang dapat mencakup peningkatan sistem operasi dan perangkat lunak, perbaikan untuk mengatasi stabilitas, kinerja, dan keamanan, dan akses ke fitur baru.
- Mendesak - Pembaruan penting yang mencakup perbaikan yang diperlukan untuk masalah yang langsung memengaruhi keamanan, kinerja, atau daya tahan gateway Anda. Pembaruan mendesak dapat dirilis kapan saja, di luar irama normal pemeliharaan bulanan dan pembaruan fitur.

Semua pembaruan bersifat kumulatif, dan pemutakhiran gateway ke versi saat ini saat diterapkan. Untuk informasi tentang perubahan spesifik yang disertakan dalam setiap pembaruan, lihat Catatan Rilis untuk Perangkat Lunak Gateway Appliance.

Semua pembaruan alat gateway 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.

Saat Anda menerapkan dan mengaktifkan gateway Anda, jadwal jendela pemeliharaan default ditetapkan. Anda dapat mengubah jadwal jendela pemeliharaan kapan saja. Anda juga dapat mematikan pembaruan pemeliharaan, tetapi kami sarankan untuk membiarkannya dihidupkan.

> **Note**
>
> Pembaruan mendesak 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 Dasbor AWS Health. Untuk informasi selengkapnya, lihat Dasbor AWS Health. 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 periode pemeliharaan yang dikonfigurasi. Untuk informasi selengkapnya, lihat Memodifikasi jadwal jendela pemeliharaan gateway .

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/home.
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/home.
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. Jadwal pemeliharaan tidak dapat ditetapkan untuk dimulai pada hari 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/home.
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.

Melakukan tugas pemeliharaan menggunakan konsol lokal

Bagian ini berisi topik berikut, yang memberikan informasi tentang cara melakukan tugas pemeliharaan menggunakan konsol lokal alat gateway. Anda dapat melakukan tugas ini dengan mengakses konsol lokal melalui mesin virtual lokal atau instans Amazon EC2 yang meng-host perangkat gateway Anda. 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 platform Linux Kernel-based Virtual Machine (KVM), VMware ESXi, atau Microsoft Manager. Hyper-V
- Melakukan tugas pada konsol lokal mesin virtual- Pelajari cara menggunakan konsol lokal untuk melakukan pengaturan 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 lokal gateway Amazon EC2- Pelajari cara masuk ke konsol lokal untuk melakukan pengaturan dasar dan tugas konfigurasi lanjutan untuk gateway Amazon EC2, 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 Manager. Hyper-V

Topik

Mengakses Konsol Lokal Gateway dengan Linux KVM

Ada berbagai cara untuk mengkonfigurasi mesin virtual yang berjalan di KVM, tergantung pada distribusi Linux yang digunakan. Petunjuk untuk mengakses opsi konfigurasi KVM dari baris perintah ikuti. Instruksi mungkin berbeda tergantung pada implementasi KVM Anda.

Untuk mengakses konsol lokal gateway Anda dengan KVM

1. Gunakan perintah berikut untuk membuat daftar VM yang saat ini tersedia di KVM.

   ```
   # virsh list
   ```

   Perintah mengembalikan daftar VM 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 Masuk ke konsol lokal File 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 Masuk ke konsol lokal File 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 kredenal 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 Masuk ke konsol lokal File 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 pada konsol lokal mesin virtual

Untuk File Gateway yang digunakan di lokasi, Anda dapat melakukan tugas pemeliharaan berikut menggunakan konsol lokal host VM. Tugas-tugas ini umum untuk hypervisor VMware Hyper-V, Microsoft, dan Linux Kernel-based Virtual Machine (KVM).

Topik

- Masuk ke konsol lokal File Gateway- Pelajari cara masuk ke konsol lokal tempat Anda dapat mengonfigurasi pengaturan jaringan gateway dan mengubah kata sandi default.

- Mengkonfigurasi proxy HTTP- Pelajari cara mengkonfigurasi Storage Gateway untuk merutekan semua lalu lintas AWS endpoint melalui server proxy.
- Mengonfigurasi pengaturan jaringan gateway Anda- Pelajari cara mengkonfigurasi gateway Anda untuk menggunakan DHCP atau alamat IP statis.
- Menguji konektivitas jaringan gateway Anda- Pelajari cara menggunakan konsol lokal gateway untuk menguji konektivitas jaringan.
- Melihat status sumber daya sistem gateway Anda- Pelajari cara memeriksa inti CPU virtual gateway Anda, ukuran volume root, dan RAM.
- Mengkonfigurasi server Network Time Protocol (NTP) untuk gateway Anda- Pelajari cara melihat dan mengedit konfigurasi server Network Time Protocol (NTP) dan menyinkronkan waktu pada gateway Anda dengan host hypervisor Anda.
- Menjalankan perintah Storage Gateway di konsol lokal- Pelajari cara menjalankan perintah konsol lokal untuk melakukan tugas-tugas seperti menyimpan tabel routing, menghubungkan ke Dukungan, dan banyak lagi.

Masuk ke konsol lokal File Gateway

Ketika VM siap bagi Anda untuk masuk, layar login akan ditampilkan. Jika ini adalah pertama kalinya Anda masuk ke konsol lokal VM, Anda menggunakan kredenal masuk sementara untuk masuk. Kredensi sementara ini memberi Anda akses ke menu tempat Anda dapat mengonfigurasi pengaturan jaringan gateway dan mengubah kata sandi dari konsol lokal. Nama pengguna awal adalah `admin` dan kata sandi sementara adalah`password`. Anda harus mengubah kata sandi saat masuk pertama.

Untuk mengubah kata sandi sementara

1. Pada menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk Gateway Console.
2. Jalankan perintah `passwd`. Untuk informasi tentang cara menjalankan perintah, lihat Menjalankan perintah Storage Gateway di konsol lokal.

Mengatur kata sandi konsol lokal dari konsol Storage Gateway

Anda juga dapat mengelola kata sandi konsol lokal dari konsol berbasis web Storage Gateway. Setiap pembaruan kata sandi yang berhasil dibuat dengan konsol berbasis web akan mengganti kata sandi yang digunakan oleh konsol lokal gateway VM, termasuk kata sandi sementara jika Anda

belum pernah masuk secara lokal. Jika gateway saat ini tidak dapat dijangkau melalui jaringan, proses pembaruan kata sandi akan gagal.

Untuk mengatur kata sandi konsol lokal di konsol Storage Gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.
2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda atur kata sandi baru.
3. Untuk Tindakan, pilih Setel Kata Sandi Konsol Lokal.
4. Dalam kotak dialog Setel Kata Sandi Konsol Lokal, masukkan kata sandi baru, konfirmasikan kata sandi, lalu pilih Simpan.

   Kata sandi baru Anda menggantikan kata sandi saat ini. Layanan Storage Gateway tidak menyimpan, menyimpan, atau mencatat kata sandi tetapi mentransmisikannya dengan aman melalui saluran terenkripsi ke VM, di mana ia disimpan dengan aman.

   > **Note**
   >
   > Kata sandi dapat terdiri dari karakter apa pun pada keyboard dan panjangnya bisa 1—512 karakter.

Mengkonfigurasi proxy HTTP

File Gateways mendukung konfigurasi proxy HTTP.

> **Note**
>
> Satu-satunya konfigurasi proxy yang didukung File Gateways adalah HTTP.

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 informasi tentang persyaratan jaringan untuk gateway Anda, lihatPersyaratan jaringan dan firewall.

Untuk mengkonfigurasi proxy HTTP untuk File Gateway

1. Masuk ke konsol lokal gateway Anda:
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal VMware ESXi, lihat. Mengakses Konsol Lokal Gateway dengan VMware ESXi
   - Untuk informasi selengkapnya tentang masuk ke konsol Hyper-V lokal Microsoft, lihatAkses 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. Dari menu utama AWS Appliance Activation - Configuration, masukkan angka yang sesuai untuk memilih Configure HTTP Proxy.
3. Dari menu AWS Appliance Activation HTTP Proxy Configuration, masukkan angka yang sesuai untuk tugas yang ingin Anda lakukan:
   - Konfigurasi HTTP proxy - Anda akan perlu untuk menyediakan nama host dan port untuk menyelesaikan konfigurasi.
   - Lihat konfigurasi proxy HTTP saat ini - Jika proxy HTTP tidak dikonfigurasi, pesan akan `HTTP Proxy not configured` ditampilkan. Jika proxy HTTP dikonfigurasi, nama host dan port proxy ditampilkan.
   - Hapus konfigurasi proxy HTTP - Pesan `HTTP Proxy Configuration Removed` ditampilkan.
4. Mulai ulang VM Anda untuk menerapkan pengaturan konfigurasi HTTP Anda.

Mengonfigurasi pengaturan 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:
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal VMware ESXi, lihat. Mengakses Konsol Lokal Gateway dengan VMware ESXi

- Untuk informasi selengkapnya tentang masuk ke konsol Hyper-V lokal Microsoft, lihatAkses 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 Konfigurasi Jaringan.
3. Dari menu Konfigurasi Jaringan, lakukan salah satu tugas berikut:

Untuk Melakukan Tugas Ini	Lakukan Ini
Dapatkan informasi tentang adaptor jaringan Anda	Masukkan angka yang sesuai untuk memilih Deskripsikan Adaptor. Daftar nama adaptor muncul, dan Anda diminta untuk memasukkan 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 ketika Anda mengkonfigurasi alamat IP statis atau ketika Anda mengatur adaptor default gateway Anda.

Untuk Melakukan Tugas Ini	Lakukan Ini
Konfigurasikan perutean DHCP	Masukkan angka yang sesuai untuk memilih Konfigurasi DHCP. Anda diminta untuk mengonfigurasi 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 memasukkan informasi berikut untuk mengonfigurasi 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 aktif 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 menggunakan 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.
Lihat konfigurasi nama host gateway Anda	Masukkan angka yang sesuai untuk memilih Lihat Konfigurasi Nama Host. Nama host gateway Anda, mode akuisisi, domain, dan ranah Direktori Aktif ditampilkan.

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`**
Edit konfigurasi DNS gateway Anda	Masukkan angka yang sesuai untuk memilih Edit Konfigurasi DNS. Adaptor server DNS primer dan sekunder yang tersedia akan ditampilkan. Anda diminta untuk memberikan alamat IP baru.

Untuk Melakukan Tugas Ini	Lakukan Ini
Lihat konfigurasi DNS gateway Anda	Masukkan angka yang sesuai untuk memilih Lihat Konfigurasi DNS. Adaptor server DNS primer dan sekunder yang tersedia akan ditampilkan. **Note** Untuk beberapa versi VMware hypervisor, Anda dapat mengedit konfigurasi adaptor di menu ini.
Lihat tabel perutean	Masukkan angka yang sesuai untuk memilih Lihat Rute. Rute default gateway Anda ditampilkan.

Menguji konektivitas jaringan gateway Anda

Anda dapat menggunakan konsol lokal gateway Anda untuk menguji konektivitas jaringan Anda. Tes ini dapat berguna ketika Anda memecahkan masalah jaringan dengan gateway Anda.

Untuk menguji konektivitas jaringan gateway Anda

1. Masuk ke konsol lokal gateway Anda:
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal VMware ESXi, lihat. Mengakses Konsol Lokal Gateway dengan VMware ESXi
   - Untuk informasi selengkapnya tentang masuk ke konsol Hyper-V lokal Microsoft, lihatAkses 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 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 informasi selengkapnya tentang masuk ke konsol VMware ESXi, lihat. Mengakses Konsol Lokal Gateway dengan VMware ESXi
   - Untuk informasi selengkapnya tentang masuk ke konsol Hyper-V lokal Microsoft, lihatAkses Konsol Lokal Gateway dengan Microsoft Hyper-V.

- Untuk informasi selengkapnya tentang masuk ke konsol lokal KVM, lihat. Mengakses Konsol Lokal Gateway dengan Linux KVM

2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Lihat Pemeriksaan Sumber Daya Sistem.

   Setiap sumber daya menampilkan [OK], [PERINGATAN], atau [GAGAL], yang menunjukkan status sumber daya sebagai berikut:

Pesan	Deskripsi
[OK]	Sumber daya telah lulus pemeriksaan sumber daya sistem.
[PERINGATAN]	Sumber daya tidak memenuhi persyaratan yang disarankan, tetapi gateway Anda dapat terus berfungsi. Storage Gateway 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.

Mengkonfigurasi server Network Time Protocol (NTP) untuk gateway Anda

Anda dapat melihat dan mengedit konfigurasi server Network Time Protocol (NTP) dan menyinkronkan waktu VM di gateway Anda dengan host hypervisor Anda.

Untuk mengelola waktu sistem

1. Masuk ke konsol lokal gateway Anda:

- Untuk informasi selengkapnya tentang masuk ke konsol lokal VMware ESXi, lihat. Mengakses Konsol Lokal Gateway dengan VMware ESXi
- Untuk informasi selengkapnya tentang masuk ke konsol Hyper-V lokal Microsoft, lihatAkses 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 Manajemen Waktu Sistem.
3. Dari menu Manajemen Waktu Sistem, masukkan angka yang sesuai untuk melakukan salah satu tugas berikut.

Untuk Melakukan Tugas Ini	Lakukan Ini
Lihat dan sinkronkan waktu VM Anda dengan waktu server NTP.	Masukkan angka yang sesuai untuk memilih Lihat dan Sinkronisasi Waktu Sistem. Waktu VM Anda saat ini ditampilkan. File Gateway Anda menentukan perbedaan waktu dari VM gateway Anda, dan waktu server NTP Anda meminta Anda untuk menyinkronkan waktu VM dengan waktu NTP. Setelah gateway Anda digunakan dan dijalankan, dalam beberapa skenario waktu VM gateway dapat melayang. Misalnya, misalkan ada pemadaman jaringan yang berkepanj angan dan host dan gateway hypervisor Anda tidak mendapatkan pembaruan waktu. Dalam hal ini, waktu VM gateway berbeda dari waktu sebenarnya. Ketika ada penyimpangan waktu, perbedaan terjadi antara waktu yang dinyataka n saat operasi seperti snapshot terjadi dan waktu sebenarnya saat operasi terjadi.

Untuk Melakukan Tugas Ini	Lakukan Ini
	Untuk gateway yang digunakan pada VMware ESXi, mengatur waktu host hypervisor dan menyinkronkan waktu VM ke host sudah cukup untuk menghindari penyimpangan waktu. Untuk informasi selengkapnya, lihat Sinkronisasi waktu VM dengan waktu host VMware. Untuk gateway yang digunakan di Microsoft Hyper-V, Anda harus memeriksa waktu VM Anda secara berkala. Untuk informasi selengkapnya, lihat Sinkronisasi waktu VM dengan Hyper-V atau waktu host Linux KVM. Untuk gateway yang digunakan di KVM, Anda dapat memeriksa dan menyinkronkan waktu VM menggunakan antarmuka `virsh` baris perintah untuk KVM.
Edit konfigurasi server NTP Anda	Masukkan angka yang sesuai untuk memilih Edit Konfigurasi NTP. Anda diminta untuk menyediakan server NTP pilihan dan sekunder.
Lihat konfigurasi server NTP Anda	Masukkan angka yang sesuai untuk memilih Lihat Konfigurasi NTP. Konfigurasi server NTP Anda ditampilkan.

Menjalankan perintah Storage Gateway di konsol lokal

Konsol lokal VM di Storage Gateway membantu menyediakan lingkungan yang aman untuk mengonfigurasi dan mendiagnosis masalah dengan gateway Anda. Dengan menggunakan perintah konsol lokal, Anda dapat melakukan tugas pemeliharaan seperti menyimpan tabel perutean, menghubungkan ke Dukungan, dan sebagainya.

Untuk menjalankan konfigurasi atau perintah diagnostik

1. Masuk ke konsol lokal gateway Anda:

   - Untuk informasi selengkapnya tentang masuk ke konsol lokal VMware ESXi, lihat. Mengakses Konsol Lokal Gateway dengan VMware ESXi
   - Untuk informasi selengkapnya tentang masuk ke konsol Hyper-V lokal Microsoft, lihatAkses 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 jaringan gateway Anda.

Perintah	Fungsi
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 jaringan gateway Anda.
iptables	Alat administrasi untuk penyaringan paket IPv4 dan NAT.
ip6tables	Alat administrasi untuk penyaringan paket IPv6 dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.
nping	Kumpulkan output dari nping untuk pemecahan masalah jaringan.
saluran dukungan terbuka	Connect to AWS Support Untuk petunjuk tentang cara mengaktifkan akses AWS dukungan, lihat Anda ingin AWS Support membantu memecahkan masalah gateway EC2 Anda gateway EC2 Anda.
passwd	Perbarui token otentikasi.
simpan-iptables	Pertahankan tabel IP.
simpan-routing-tabel	Simpan entri tabel routing yang baru ditambahk an.

Perintah	Fungsi
tcptraceroute	Kumpulkan output traceroute pada lalu lintas TCP ke tujuan.
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.

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.

Melakukan tugas di konsol lokal gateway Amazon EC2

Beberapa tugas pemeliharaan mengharuskan Anda masuk ke konsol lokal saat menjalankan gateway yang diterapkan pada instans Amazon EC2. Bagian ini menjelaskan cara masuk ke konsol lokal dan melakukan tugas pemeliharaan.

Topik

- Masuk ke konsol lokal gateway Amazon EC2 Anda- Pelajari cara menghubungkan dan masuk ke konsol lokal gateway instans Amazon EC2 Anda dengan menggunakan klien Secure Shell (SSH).
- Merutekan gateway Anda yang digunakan di Amazon EC2 melalui proxy HTTP- Pelajari cara mengonfigurasi proxy Socket Secure versi 5 (SOCKS5) antara AWS dan gateway yang digunakan pada instans Amazon EC2.

- Menguji konektivitas jaringan gateway Anda- Pelajari cara menggunakan konsol lokal gateway untuk menguji konektivitas jaringan antara gateway Anda dan berbagai sumber daya jaringan.
- Melihat status sumber daya sistem gateway Anda- Pelajari cara menggunakan konsol lokal gateway untuk memeriksa inti CPU virtual gateway Anda, ukuran volume root, dan RAM.
- Menjalankan perintah Storage Gateway di konsol lokal untuk gateway Amazon EC2- Pelajari cara menjalankan perintah konsol lokal untuk melakukan tugas-tugas seperti menyimpan tabel routing, menghubungkan ke Dukungan, dan banyak lagi.
- Mengonfigurasi pengaturan jaringan gateway Amazon EC2 Anda- Pelajari cara menggunakan konsol lokal untuk melihat dan mengonfigurasi pengaturan jaringan seperti DNS dan nama host untuk gateway pada instans Amazon EC2.

Masuk ke konsol lokal gateway Amazon EC2 Anda

Anda masuk ke konsol lokal gateway pada instans Amazon EC2 menggunakan klien Secure Shell (SSH). Untuk informasi selengkapnya, lihat Connect ke instans Anda di Panduan Pengguna Amazon EC2. Untuk menghubungkan dengan cara ini, Anda memerlukan key pair SSH yang Anda tentukan saat meluncurkan instance Anda. Untuk informasi tentang pasangan kunci Amazon EC2, lihat pasangan kunci Amazon EC2 di Panduan Pengguna Amazon EC2.

Untuk masuk ke konsol lokal gateway

1. Hubungkan ke instans Amazon EC2 menggunakan SSH dan masuk sebagai pengguna admin.
2. Setelah Anda masuk, Anda melihat menu utama Aktivasi AWS Alat - Konfigurasi, dari mana Anda dapat melakukan berbagai tugas.

Untuk mempelajari tentang tugas ini	Lihat Topik Ini
Konfigurasikan proxy HTTP untuk gateway Anda	Merutekan gateway Anda yang digunakan di Amazon EC2 melalui proxy HTTP
Konfigurasikan pengaturan jaringan untuk gateway Anda	Mengonfigurasi pengaturan jaringan gateway Amazon EC2 Anda
Uji konektivitas jaringan	Menguji konektivitas jaringan gateway Anda
Lihat pemeriksaan sumber daya sistem	Melihat status sumber daya sistem gateway Anda.

Untuk mempelajari tentang tugas ini	Lihat Topik Ini
Jalankan perintah konsol Storage Gateway	Menjalankan perintah Storage Gateway di konsol lokal untuk gateway Amazon EC2

Untuk mematikan gateway, masuk**0**.

Untuk keluar dari sesi konfigurasi, masukkan**X**.

Merutekan gateway Anda yang digunakan di Amazon EC2 melalui proxy HTTP

Storage Gateway mendukung konfigurasi proxy Socket Secure versi 5 (SOCKS5) antara gateway yang digunakan di Amazon EC2 dan. AWS

Jika gateway Anda harus menggunakan server proxy untuk berkomunikasi ke internet, maka Anda perlu mengkonfigurasi pengaturan proxy HTTP untuk gateway Anda. Anda melakukan ini dengan menentukan alamat IP dan nomor port untuk host yang menjalankan proxy Anda. Setelah Anda melakukannya, Storage Gateway merutekan semua lalu lintas AWS endpoint melalui server proxy Anda. Komunikasi antara gateway dan titik akhir dienkripsi, bahkan saat menggunakan proxy HTTP.

Untuk merutekan lalu lintas internet gateway Anda melalui server proxy lokal

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, lihat Masuk ke konsol lokal gateway Amazon EC2 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 HTTP proxy - Anda akan perlu untuk menyediakan nama host dan port untuk menyelesaikan konfigurasi.
   - Lihat konfigurasi proxy HTTP saat ini - Jika proxy HTTP tidak dikonfigurasi, pesan akan `HTTP Proxy not configured` ditampilkan. Jika proxy HTTP dikonfigurasi, nama host dan port proxy ditampilkan.
   - Hapus konfigurasi proxy HTTP - Pesan `HTTP Proxy Configuration Removed` ditampilkan.

Menguji konektivitas jaringan gateway Anda

Anda dapat menggunakan konsol lokal gateway Anda untuk menguji konektivitas jaringan Anda. Tes ini dapat berguna ketika Anda memecahkan masalah jaringan dengan gateway Anda.

Untuk menguji konektivitas gateway Anda

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, lihat Masuk ke konsol lokal gateway Amazon EC2 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 File Gateway Anda dimulai, ia memeriksa inti CPU virtual, ukuran volume root, dan RAM. Ini kemudian menentukan apakah sumber daya sistem yang tersedia cukup untuk gateway

Anda berfungsi dengan baik. Anda dapat melihat hasil pemeriksaan sumber daya sistem dengan menggunakan konsol lokal gateway.

Untuk melihat status pemeriksaan sumber daya sistem

1. Masuk ke konsol lokal di Gateway File Amazon EC2 Anda. Untuk petunjuk, lihat Masuk ke konsol lokal gateway Amazon EC2 Anda.
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Lihat Pemeriksaan Sumber Daya Sistem.

   Konsol lokal gateway menampilkan [OK], [PERINGATAN], atau [GAGAL] untuk menunjukkan status sumber daya sebagai berikut:

Pesan	Deskripsi
[OK]	Sumber daya telah lulus pemeriksaan sumber daya sistem.
[PERINGATAN]	Sumber daya tidak memenuhi persyaratan yang disarankan, tetapi gateway Anda dapat terus berfungsi. Konsol lokal gateway menampilkan pesan yang menjelaskan hasil pemeriksaan sumber daya.
[GAGAL]	Sumber daya tidak memenuhi persyaratan minimum. Gateway Anda mungkin tidak berfungsi dengan baik. Konsol lokal gateway menampilkan pesan yang menjelaskan hasil pemeriksaan sumber daya.

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

Menjalankan perintah Storage Gateway di konsol lokal untuk gateway Amazon EC2

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, lihat Masuk ke konsol lokal gateway Amazon EC2 Anda.
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 jaringan gateway Anda.
ip	Menampilkan/memanipulasi routing, perangkat , dan terowongan.

Perintah	Fungsi
	Note Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus. Untuk petunjuk, lihat jaringan gateway Anda.
iptables	Alat administrasi untuk penyaringan paket IPv4 dan NAT.
ip6tables	Alat administrasi untuk penyaringan paket IPv6 dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.
nping	Kumpulkan output dari nping untuk pemecahan masalah jaringan.
saluran dukungan terbuka	Connect to AWS Support
simpan-iptables	Pertahankan tabel IP.
simpan-routing-tabel	Simpan entri tabel routing yang baru ditambahkan.
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.

Mengonfigurasi pengaturan jaringan gateway Amazon EC2 Anda

Anda dapat melihat dan mengonfigurasi pengaturan jaringan untuk Gateway File Amazon EC2 Anda dengan menggunakan konsol lokal gateway.

Untuk mengkonfigurasi pengaturan jaringan Anda

1. Masuk ke konsol lokal di Gateway File Amazon EC2 Anda. Untuk petunjuk, lihat Masuk ke konsol lokal gateway Amazon EC2 Anda.
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Konfigurasi Jaringan.
3. Dari menu AWS Appliance Activation - Network Configuration, masukkan angka yang sesuai untuk tugas yang ingin Anda lakukan:

   - Edit Konfigurasi DNS - Konsol lokal gateway menampilkan adaptor yang tersedia untuk server DNS primer dan sekunder. Konsol kemudian meminta Anda untuk memberikan alamat IP baru.
   - Lihat Konfigurasi DNS - Konsol lokal gateway menampilkan adaptor yang tersedia untuk server DNS primer dan sekunder.
   - Konfigurasi Nama Host - Konsol lokal gateway meminta Anda untuk memilih apakah gateway akan menggunakan nama host statis yang Anda tentukan, atau apakah itu akan memperoleh nama host secara otomatis melalui DCHP atau RDNS.

     > **Note**
     >
     > Jika Anda memilih untuk mengonfigurasi nama host statis untuk gateway Anda, Anda harus membuat catatan A di sistem DNS Anda yang mengarahkan alamat IP gateway ke nama host statisnya.

   - Lihat Konfigurasi Nama Host - Konsol lokal gateway menampilkan nama host, mode akuisisi, domain, dan ranah Direktori Aktif untuk Gateway File Amazon EC2 Anda.

Mematikan VM gateway Anda

Anda mungkin perlu mematikan atau me-reboot VM Anda untuk pemeliharaan, seperti saat menerapkan patch ke hypervisor Anda. Anda mematikan VM gateway lokal menggunakan antarmuka hypervisor, dan instans Amazon EC2 menggunakan konsol Amazon EC2.

Important

Jika Anda berhenti dan memulai gateway Amazon EC2 yang menggunakan penyimpanan sementara, gateway akan offline secara permanen. Ini terjadi karena disk penyimpanan fisik diganti. Tidak ada solusi untuk masalah ini. Satu-satunya resolusi adalah menghapus gateway dan mengaktifkan yang baru pada instans EC2 baru.

Mengganti yang sudah ada Gerbang File S3 dengan contoh baru

Note

Jika Anda melakukan migrasi Storage Gateway AL2 ke AL2023, sebelum memulai, pastikan Anda telah menyelesaikan semua item dalam Pre-migration Daftar Periksa di Kampanye Migrasi Storage Gateway AL2 ke AL2023.

Anda dapat mengganti Gateway File File Gateway S3 yang sudah ada dengan instance baru saat data dan kebutuhan kinerja Anda bertambah, atau jika Anda menerima pemberitahuan untuk AWS memigrasi gateway Anda. Anda mungkin perlu melakukan ini jika Anda ingin memindahkan gateway Anda ke platform host yang lebih baik atau instans Amazon EC2 yang lebih baru, atau untuk menyegarkan perangkat keras server yang mendasarinya.

Ada dua metode untuk mengganti S3 File Gateway File Gateway yang ada. Tabel berikut menjelaskan manfaat dan kelemahan masing-masing metode. Dengan menggunakan informasi ini, pilih metode yang paling cocok untuk lingkungan gateway Anda, lalu lihat langkah-langkah prosedur di bagian yang sesuai berikut.

Note

Jika Anda perlu masuk ke konsol lokal Storage Gateway baru untuk menyelesaikan salah satu metode, nama pengguna awal adalah admin, dan kata sandi sementara adalah kata sandi.

> **Important**
>
> Gunakan petunjuk ini hanya untuk memigrasi peralatan gateway yang menjalankan versi 1.x. Anda tidak dapat menggunakannya untuk memigrasikan peralatan gateway yang menjalankan versi yang lebih rendah.

	Metode 1: Migrasikan disk cache dan ID Gateway ke instance pengganti*	Metode 2: Contoh pengganti an dengan disk cache kosong dan ID Gateway baru
Cache data disk	Data pada disk cache dipertahankan. Metode ini berguna jika gateway Anda memiliki disk cache yang besar, atau jika aplikasi Anda sensitif terhadap penundaan yang disebabkan oleh operasi pembacaan di luar cache.	Data dalam cache diunduh dari AWS cloud. Metode ini optimal untuk beban kerja berat tulis, jika aplikasi Anda dapat mentolerir penundaan yang disebabkan oleh pembacaan di luar cache.
Waktu down	Gateway Anda akan offline selama 1-2 jam selama proses migrasi.	Berbagi file selalu tersedia, tetapi klien akan mengalami downtime cutover pendek saat beralih dari satu file share ke file lainnya selama transisi ke instance baru. **Note** Menulis ke satu bucket Amazon S3 dari dua berbagi file secara bersamaan tidak didukung, jadi semua klien harus dipetakan ulang dari satu share ke

	Metode 1: Migrasikan disk cache dan ID Gateway ke instance pengganti*	Metode 2: Contoh pengganti an dengan disk cache kosong dan ID Gateway baru
		share lainnya secara bersamaan, bukan secara bertahap.
ID Gerbang	Gateway baru mewarisi ID Gateway dari gateway yang digantikannya.	Gateway dan gateway pengganti yang ada memiliki ID Gateway yang terpisah dan unik.

	Metode 1: Migrasikan disk cache dan ID Gateway ke instance pengganti*	Metode 2: Contoh pengganti an dengan disk cache kosong dan ID Gateway baru
Implikasi biaya	Pelestarian data yang di-cache menghilangkan kebutuhan untuk mengunduh ulang, sehingga tidak ada biaya tambahan S3.	Metode ini dapat menimbulk an biaya tambahan, terutama jika pengambilan data dari S3 diperlukan. Pendekata n ini juga dapat menghasil kan biaya pengambilan data S3 yang substansif jika berbagi file yang didukung oleh bucket S3 menggunak an kelas penyimpanan seperti S3, S3, S3 One Intelligent-Tiering Zone-IA, atau objek yang dialihkan Standard-IA ke GLACIER melalui kebijakan siklus hidup S3. Dalam kasus berbagi file SMB, jika ACL root dikonfigu rasi pada berbagi file, itu harus diterapkan kembali ke gateway yang dimigrasi. Tindakan ini akan menerapka n pengaturan secara rekursif ke semua objek dalam file share, memperkenalkan beberapa implikasi biaya.

> **Note**
>
> Migrasi hanya dapat dilakukan antara gateway dari jenis yang sama. Misalnya, Anda tidak dapat memigrasikan pengaturan atau data dari Gateway File FSx ke Gateway File S3.

Metode 1: Migrasikan disk cache dan ID Gateway ke instance pengganti

Untuk memigrasikan Gerbang File S3disk cache dan ID Gateway ke instance pengganti:

1. Hentikan aplikasi apa pun yang menulis ke S3 File Gateway File Gateway yang ada.
2. Gunakan langkah-langkah berikut untuk memperbarui gateway ke versi terbaru

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

   b. Di panel navigasi, pilih Gateways, lalu pilih S3 File Gateway lama yang ingin Anda migrasikan.

   c. Pilih Perbarui Sekarang jika tersedia. Jika tidak, gateway Anda sudah ada di versi terbaru.
3. Verifikasi bahwa `CachePercentDirty` metrik pada tab Pemantauan untuk Gateway File S3 yang ada Gateway adalah. `0`
4. Matikan Gateway File Gateway Gateway S3 yang ada dengan mematikan mesin virtual host (VM) menggunakan kontrol hypervisornya.

   Untuk informasi selengkapnya tentang mematikan instans Amazon EC2, lihat Menghentikan dan memulai instans Anda di Panduan Pengguna Amazon EC2.

   Untuk informasi selengkapnya tentang mematikan KVM, VMware, atau VM, lihat dokumentasi hypervisor Hyper-V Anda.
5. Lepaskan semua disk, termasuk disk root dan disk cache dari VM gateway lama.

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

   Jika Anda menggunakan instans Amazon EC2 sebagai VM untuk Gateway File FSx File Gateway S3 lihat Melepaskan volume Amazon EBS dari instans Windows atau Lepaskan volume Amazon EBS dari instans Linux di Panduan Pengguna Amazon EC2.

   Untuk informasi tentang melepaskan disk dari KVM, VMware, atau VM, lihat dokumentasi untuk Hyper-V hypervisor Anda.
6. Buat instance VM hypervisor S3 File Gateway baru, tetapi jangan aktifkan sebagai gateway. Pada langkah selanjutnya, VM baru ini akan mengasumsikan identitas gateway lama.

Untuk informasi selengkapnya tentang membuat VM hypervisor Storage Gateway baru, lihat Memilih Platform Host dan Mengunduh VM.

> **Important**
>
> Gunakan gambar S3 File Gateway untuk VM baru. Gambar untuk jenis gateway yang berbeda (misalnya, Volume Gateway atau Tape Gateway) akan menyebabkan gateway yang dimigrasi gagal untuk memulai.

> **Note**
>
> Jangan menambahkan disk cache untuk VM baru. VM ini akan menggunakan disk cache yang sama yang digunakan oleh VM lama.

> **Note**
>
> Setelah mengunduh VM, tutup wizard konsol. Jangan lanjutkan dengan aktivasi pada saat ini.

7. Konfigurasikan VM Storage Gateway baru Anda untuk menggunakan pengaturan 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 gateway Anda, lihat Mengonfigurasi parameter jaringan.

   Jika VM gateway Anda harus menggunakan proxy Socket Secure versi 5 (SOCKS5) untuk terhubung ke internet, lihat Merutekan gateway Anda yang digunakan di EC2 melalui proxy HTTP.

> **Note**
>
> Anda dapat menggunakan kembali alamat IP statis atau nama host yang sama dari VM gateway lama untuk menghindari konfigurasi ulang klien NFS atau SMB.

8. Mulai Storage Gateway VM baru.
9. Lampirkan semua disk yang Anda lepaskan dari VM gateway lama ke VM gateway baru. Ini termasuk disk root gateway lama dan disk cache. Jangan lepaskan disk root gateway VM baru itu sendiri.

> **Note**
>
> Agar berhasil bermigrasi, semua disk harus tetap tidak berubah. Mengubah ukuran disk atau nilai lainnya menyebabkan inkonsistensi dalam metadata yang mencegah migrasi berhasil.

10. Memulai proses migrasi gateway dengan menghubungkan ke konsol lokal VM gateway baru, atau membuat permintaan web ke alamat IP VM gateway baru (dijelaskan di bawah).

    a. Untuk menggunakan konsol lokal, pilih opsi untuk Migrasi Gateway dan berikan ID gateway yang ada saat diminta. Anda akan diberikan petunjuk untuk menyalin pengaturan yang diterapkan sebelumnya pada gateway lama ke gateway baru. Anda dapat memilih untuk menerapkannya atau mengonfigurasinya secara manual nanti. Lihat Mengakses Konsol Lokal Gateway.

    b. Atau, Anda dapat 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 diselesaikan, Anda akan melihat pesan yang mengonfirmasi migrasi yang berhasil.

11. Tunggu status gateway ditampilkan sebagai Berjalan di AWS Storage Gateway konsol. Tergantung pada bandwidth yang tersedia, ini bisa memakan waktu hingga 10 menit.
12. Hentikan Storage Gateway VM yang baru.
13. Lepaskan disk root gateway lama, yang ID volumenya Anda catat sebelumnya, dari gateway baru.
14. Mulai Storage Gateway VM baru.
15. Jika gateway Anda telah bergabung ke domain Direktori Aktif, bergabung kembali dengan domain tersebut. Untuk petunjuk, lihat Menggunakan Active Directory untuk mengautentikasi pengguna.

> **Note**
>
> Anda harus menyelesaikan langkah ini bahkan jika status S3 File Gateway Gateway muncul sebagai Bergabung.

16. Jika gateway Anda menggunakan metode otentikasi Akses Tamu SMB, kata sandi harus dimasukkan kembali. Untuk petunjuk, lihat Menyediakan akses tamu ke berbagi file Anda.
17. Konfirmasikan bahwa saham Anda tersedia di alamat IP VM gateway baru, lalu hapus VM gateway lama.

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

Untuk informasi selengkapnya tentang menghapus instans Amazon EC2, lihat Mengakhiri instans Anda di Panduan Pengguna Amazon EC2. Untuk informasi selengkapnya tentang menghapus KVM, VMware, atau Hyper-V VM, lihat dokumentasi untuk hypervisor Anda.

Metode 2: Contoh penggantian dengan disk cache kosong dan ID Gateway baru

Untuk mengatur pengganti Gerbang File S3 contoh dengan disk cache kosong dan ID Gateway baru:

1. Hentikan aplikasi apa pun yang menulis ke S3 File Gateway File Gateway yang ada. Verifikasi bahwa `CachePercentDirty` metrik pada tab Pemantauan adalah `0` sebelum Anda mengatur pembagian file di gateway baru.
2. Gunakan AWS Command Line Interface (AWS CLI) untuk mengumpulkan dan menyimpan informasi konfigurasi tentang S3 File Gateway FSx File Gateway dengan melakukan hal berikut:

   a. Simpan informasi konfigurasi gateway untuk S3 File Gateway File Gateway.

   ```
   aws storagegateway describe-gateway-information --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   Perintah ini mengeluarkan blok JSON yang berisi metadata tentang gateway, seperti namanya, antarmuka jaringan, zona waktu yang dikonfigurasi, dan statusnya (apakah gateway sedang berjalan).

   b. Simpan pengaturan Blok Pesan Server (SMB) dari Gateway File S3 File Gateway.

   ```
   aws storagegateway describe-smb-settings --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   Perintah ini mengeluarkan blok JSON yang berisi metadata tentang berbagi file SMB, seperti nama domainnya, status Microsoft Active Directory, apakah kata sandi tamu disetel, dan jenis strategi keamanan.

   c.
   - Gunakan perintah berikut untuk berbagi file SMB.

   ```
   aws storagegateway describe-smb-file-shares --file-share-arn-list
    "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
   ```

   Perintah ini mengeluarkan blok JSON yang berisi metadata tentang berbagi file SMB, seperti namanya, kelas penyimpanan, status, peran IAM Amazon Resource Name (ARN), daftar klien yang diizinkan mengakses S3 File Gateway , dan jalur yang digunakan oleh klien SMB untuk mengidentifikasi titik pemasangan.

- Gunakan perintah berikut untuk berbagi file NFS.

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

Perintah ini mengeluarkan blok JSON yang berisi metadata tentang berbagi file NFS, seperti namanya, kelas penyimpanan, status, peran IAM ARN, daftar klien yang diizinkan untuk mengakses S3 File Gateway , dan jalur yang digunakan oleh klien NFS untuk mengidentifikasi titik pemasangan.

3. Buat Gateway File S3 baru Gateway dengan pengaturan dan konfigurasi yang sama dengan gateway lama. Jika perlu, lihat informasi yang Anda simpan di Langkah 2.
4. Buat berbagi file baru untuk gateway baru dengan pengaturan dan konfigurasi yang sama dengan berbagi file yang dikonfigurasi pada gateway lama. Jika perlu, lihat informasi yang Anda simpan di Langkah 2.

> **Note**
>
> Anda sekarang dapat menyalin konfigurasi berbagi file antar gateway. Untuk informasi selengkapnya, lihat Menyalin berbagi file.

5. Konfirmasikan bahwa gateway baru Anda berfungsi dengan benar, lalu remap/cut -over klien Anda dari berbagi file lama ke berbagi file baru dengan cara yang paling sesuai dengan lingkungan Anda.
6. Konfirmasikan bahwa gateway baru Anda berfungsi dengan benar, lalu hapus gateway lama dari konsol Storage Gateway.

> **Important**
>
> Sebelum Anda menghapus Gateway File S3 Gateway, pastikan bahwa tidak ada aplikasi yang saat ini menulis ke cache gateway itu. Jika Anda menghapus gateway saat sedang digunakan, kehilangan data dapat terjadi.

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

7. Hapus instance gateway VM atau Amazon EC2 lama.

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.

Ketika Anda menghapus gateway, itu tidak lagi muncul di Konsol AWS Storage Gateway Manajemen dan koneksi 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.

Menghapus Gateway Anda dengan Menggunakan Storage Gateway Console

Prosedur untuk menghapus gateway adalah sama untuk semua jenis gateway. Namun, tergantung pada jenis gateway yang ingin Anda hapus dan host tempat gateway digunakan, Anda mungkin harus melakukan tugas tambahan untuk menghapus sumber daya yang terkait dengan gateway. Menghapus sumber daya ini membantu Anda menghindari membayar sumber daya yang tidak Anda rencanakan untuk digunakan.

> **Note**
>
> Untuk gateway yang digunakan pada instans Amazon EC2, instans akan tetap ada hingga Anda menghapusnya.
>
> Untuk gateway yang digunakan pada mesin virtual (VM), setelah Anda menghapus gateway, VM gateway masih ada di lingkungan virtualisasi Anda. Untuk menghapus VM, gunakan klien VMware vSphere, Hyper-V Microsoft Manager, Kernel-based atau Linux 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/home.
2. Pilih Gateway, lalu pilih satu atau beberapa gateway untuk dihapus.
3. Untuk Tindakan, pilih Hapus gateway. Kotak dialog konfirmasi muncul.

> **Warning**
>
> Sebelum Anda melakukan langkah ini, pastikan bahwa tidak ada aplikasi yang saat ini menulis ke volume gateway. Jika Anda menghapus gateway saat sedang digunakan, kehilangan data dapat terjadi. Ketika gateway dihapus, tidak ada cara untuk mendapatkannya kembali.

4. Pastikan Anda ingin menghapus gateway yang ditentukan, lalu ketik kata hapus di kotak konfirmasi, dan pilih Hapus.
5. (Opsional) Jika Anda ingin memberikan umpan balik tentang gateway yang dihapus, lengkapi kotak dialog umpan balik, lalu pilih Kirim. Jika tidak, pilih Lewati.

> **Important**
>
> Anda tidak lagi membayar biaya perangkat lunak setelah menghapus gateway, tetapi sumber daya seperti bucket Amazon S3 dan instans Amazon EC2 tetap ada. Anda dapat menghapus gateway Amazon EC2 instans setelah gateway file dihapus. Jika Anda tidak memerlukan data di bucket Amazon S3 yang terkait dengan pembagian file, Anda dapat memilih untuk menghapus bucket Amazon S3 Anda. Untuk petunjuk, lihat Menghapus bucket Anda.

Kinerja dan optimasi

Bagian ini menjelaskan panduan dan praktik terbaik untuk mengoptimalkan kinerja File Gateway.

Topik

Panduan kinerja dasar untuk S3 File Gateway Gateway

Di bagian ini, Anda dapat menemukan panduan untuk penyediaan perangkat keras untuk S3 File Gateway VM Anda. Konfigurasi instance yang tercantum dalam tabel adalah contoh, dan disediakan untuk referensi.

Untuk kinerja terbaik, ukuran disk cache harus disetel ke ukuran set kerja aktif. Menggunakan beberapa disk lokal untuk cache meningkatkan kinerja penulisan dengan memparalelkan akses ke data dan mengarah ke IOPS yang lebih tinggi.

> **Note**
>
> Kami tidak menyarankan menggunakan penyimpanan sementara. Untuk informasi tentang penggunaan penyimpanan sementara, lihat. Menggunakan penyimpanan singkat dengan gateway EC2
> Untuk instans Amazon EC2, jika Anda memiliki lebih dari 5 juta objek di bucket S3 dan Anda menggunakan volume SSD Tujuan Umum, volume EBS root minimum 350 GiB diperlukan untuk kinerja gateway yang dapat diterima saat memulai. Untuk informasi tentang cara meningkatkan ukuran volume, lihat Memodifikasi volume EBS menggunakan volume elastis (konsol).
> Batas ukuran yang disarankan untuk direktori individual dalam yang Anda sambungkan ke File Gateway adalah 10.000 file per direktori. Anda dapat menggunakan File Gateway dengan direktori yang memiliki lebih dari 10.000 file, tetapi kinerja mungkin terpengaruh.

Dalam tabel berikut, operasi baca klik cache dibaca dari berbagi file yang disajikan dari cache. Operasi gagal baca cache dibaca dari berbagi file yang disajikan dari Amazon S3.

Tabel berikut menunjukkan contoh konfigurasi S3 File Gateway.

Kinerja S3 File Gateway pada klien Linux

Contoh Konfigurasi	Protokol	Tulis throughput (ukuran file 1 GB)	Cache menekan throughput baca	Cache melewatkan throughput baca
Disk root: 80 GB, io1 SSD, 4.000 IOPS Disk cache: 512 GiB cache, io1, 1.500 IOPS yang disediakan Kinerja jaringan minimum: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protokol NFS direkomendasikan untuk Linux	NFSv3 - 1 utas	110 MiB/sec (0,92 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 utas	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	NFSv4 - 1 utas	130 MiB/sec (1,1 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)
	NFSv4 - 8 utas	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 utas	115 MiB/sec (1,0 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 utas	190 MiB/sec (1,6 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
Peralatan Perangkat Keras Storage Gateway	NFSv3 - 1 utas	265 MiB/sec (2,2 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 utas	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)

Contoh Konfigurasi	Protokol	Tulis throughput (ukuran file 1 GB)	Cache menekan throughput baca	Cache melewatkan throughput baca
Kinerja jaringan minimum: 10 Gbps	NFSv4 - 1 utas	310 MiB/sec (2,6 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)
	NFSv4 - 8 utas	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 utas	275 MiB/sec (2,4 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 utas	455 MiB/sec (3,8 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
Disk root: 80 GB, io1 SSD, 4.000 IOPS Disk cache: Disk cache NVME 4 x 2 TB Kinerja jaringan minimum: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protokol NFS direkomendasikan untuk Linux	NFSv3 - 1 utas	300 MiB/sec (2,5 Gbps)	590 MiB/sec (4,9 Gbps)	325 MiB/sec (2,7 Gbps)
	NFSv3 - 8 utas	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)
	NFSv4 - 1 utas	355 MiB/sec (3,0 Gbps)	590 MiB/sec (4,9 Gbps)	340 MiB/sec (2,9 Gbps)
	NFSv4 - 8 utas	575 MiB/sec (4,8 Gbps)	590 MiB/sec (4,9 Gbps)	575 MiB/sec (4,8 Gbps)
	SMBV3 - 1 utas	230 MiB/sec (1,9 Gbps)	325 MiB/sec (2,7 Gbps)	245 MiB/sec (2,0 Gbps)
	SMBV3 - 8 utas	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)

Kinerja File Gateway pada klien Windows

Contoh Konfigurasi	Protokol	Tulis throughput (ukuran file 1 GB)	Cache menekan throughput baca	Cache melewatkan throughput baca
Disk root: 80 GB, io1 SSD, 4.000 IOPS Disk cache: 512 GiB cache, io1, 1.500 IOPS yang disediakan Kinerja jaringan minimum: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protokol SMB direkomendasikan untuk Windows	SMBV3 - 1 utas	150 MiB/sec (1,3 Gbps)	180 MiB/sec (1,5 Gbps)	20 MiB/sec (0,2 Gbps)
	SMBV3 - 8 utas	190 MiB/sec (1,6 Gbps)	335 MiB/sec (2,8 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 utas	95 MiB/sec (0,8 Gbps)	130 MiB/sec (1,1 Gbps)	20 MiB/sec (0,2 Gbps)
	NFSv3 - 8 utas	190 MiB/sec (1,6 Gbps)	330 MiB/sec (2,8 Gbps)	190 MiB/sec (1,6 Gbps)
Peralatan Perangkat Keras Storage Gateway Kinerja jaringan minimum: 10 Gbps	SMBV3 - 1 utas	230 MiB/sec (1,9 Gbps)	255 MiB/sec (2,1 Gbps)	20 MiB/sec (0,2 Gbps)
	SMBV3 - 8 utas	835 MiB/sec (7,0 Gbps)	475 MiB/sec (4,0 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 utas	135 MiB/sec (1,1 Gbps)	185 MiB/sec (1,6 Gbps)	20 MiB/sec (0,2 Gbps)
	NFSv3 - 8 utas	545 MiB/sec (4,6 Gbps)	470 MiB/sec (4,0 Gbps)	190 MiB/sec (1,6 Gbps)

Contoh Konfigurasi	Protokol	Tulis throughput (ukuran file 1 GB)	Cache menekan throughput baca	Cache melewatkan throughput baca
Disk root: 80 GB, io1 SSD, 4.000 IOPS Disk cache: Disk cache NVME 4 x 2 TB Kinerja jaringan minimum: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protokol SMB direkomendasikan untuk Windows	SMBV3 - 1 utas	230 MiB/sec (1,9 Gbps)	265 MiB/sec (2,2 Gbps)	30 MiB/sec (0,3 Gbps)
	SMBV3 - 8 utas	835 MiB/sec (7,0 Gbps)	780 MiB/sec (6,5 Gbps)	250 MiB/sec (2,1 Gbps)
	NFSv3 - 1 utas	135 MiB/sec (1.1. Gbps)	220 MiB/sec (1,8 Gbps)	30 MiB/sec (0,3 Gbps)
	NFSv3 - 8 utas	545 MiB/sec (4,6 Gbps)	570 MiB/sec (4,8 Gbps)	240 MiB/sec (2,0 Gbps)

> **Note**
>
> Kinerja Anda mungkin bervariasi berdasarkan konfigurasi platform host dan bandwidth jaringan Anda. Kinerja throughput tulis menurun dengan ukuran file, dengan throughput tertinggi yang dapat dicapai untuk file kecil (kurang dari 32MiB) menjadi 16 file per detik.

Panduan kinerja untuk gateway dengan beberapa berbagi file

Amazon S3 File Gateway mendukung melampirkan hingga 50 file share ke satu alat Storage Gateway. Dengan menambahkan beberapa berbagi file per gateway, Anda dapat mendukung lebih banyak pengguna dan beban kerja sambil mengelola lebih sedikit gateway dan sumber daya perangkat keras virtual. Selain faktor lain, jumlah berbagi file yang dikelola oleh gateway dapat memengaruhi kinerja gateway tersebut. Bagian ini menjelaskan bagaimana kinerja gateway

diharapkan berubah tergantung pada jumlah berbagi file terlampir dan merekomendasikan konfigurasi perangkat keras virtual untuk mengoptimalkan kinerja gateway yang mengelola beberapa pembagian.

Secara umum, meningkatkan jumlah berbagi file yang dikelola oleh satu Storage Gateway dapat memiliki konsekuensi sebagai berikut:

- Peningkatan waktu yang diperlukan untuk me-restart gateway.
- Peningkatan pemanfaatan sumber daya perangkat keras virtual seperti vCPU dan RAM.
- Penurunan kinerja untuk operasi data dan metadata jika sumber daya perangkat keras virtual menjadi jenuh.

Tabel berikut mencantumkan konfigurasi perangkat keras virtual yang direkomendasikan untuk gateway yang mengelola beberapa pembagian file:

Berbagi File Per Gateway	Pengaturan Kapasitas Gateway yang Direkomendasikan	Cores vCPU yang Direkomendasikan	RAM yang direkomendasikan	Ukuran Disk Root yang Direkomendasikan			
1-10	Kecil	4 (tipe instans EC2 m4.xlarge atau lebih besar)	16 GiB	80 GiB			
10-20	Sedang	8 (tipe instans EC2 m4.2xlarge atau	32 GiB	160 GiB			

Berbagi File Per Gateway	Pengaturan Kapasitas Gateway yang Direkomendasikan	Cores vCPU yang Direkomendasikan	RAM yang direkomendasikan	Ukuran Disk Root yang Direkomendasikan			
		lebih besar)					
20+	Besar	16 (tipe instans EC2 m4.4xlarge atau lebih besar)	64 GiB	240 GiB			

Selain konfigurasi perangkat keras virtual yang direkomendasikan di atas, kami merekomendasikan praktik terbaik berikut untuk mengonfigurasi dan memelihara peralatan Storage Gateway yang mengelola beberapa berbagi file:

- Pertimbangkan bahwa hubungan antara jumlah pembagian file dan permintaan yang ditempatkan pada perangkat keras virtual gateway belum tentu linier. Beberapa berbagi file mungkin menghasilkan lebih banyak throughput, dan karenanya lebih banyak permintaan perangkat keras daripada yang lain. Rekomendasi dalam tabel sebelumnya didasarkan pada kapasitas perangkat keras maksimum dan berbagai tingkat throughput berbagi file.
- Jika Anda menemukan bahwa menambahkan beberapa pembagian file ke satu gateway mengurangi kinerja, pertimbangkan untuk memindahkan pembagian file yang paling aktif ke gateway lain. Secara khusus, jika berbagi file digunakan untuk very-high-throughput aplikasi, pertimbangkan untuk membuat gateway terpisah untuk berbagi file tersebut.
- Kami tidak menyarankan mengonfigurasi satu gateway untuk beberapa aplikasi throughput tinggi dan satu lagi untuk beberapa aplikasi throughput rendah. Sebagai gantinya, cobalah untuk menyebarkan berbagi file throughput tinggi dan rendah secara merata di seluruh gateway untuk menyeimbangkan saturasi perangkat keras. Untuk mengukur throughput berbagi file Anda,

gunakan `ReadBytes` dan `WriteBytes` metrik. Untuk informasi selengkapnya, lihat Memahami metrik berbagi file.

Memaksimalkan throughput Gateway File S3

Bagian berikut menjelaskan praktik terbaik untuk memaksimalkan throughput antara klien NFS dan SMB, Gateway File S3, dan Amazon S3. Panduan yang diberikan di setiap bagian berkontribusi secara bertahap untuk meningkatkan throughput secara keseluruhan. Meskipun tidak satu pun dari rekomendasi ini diperlukan, dan mereka tidak saling bergantung, mereka telah dipilih dan diurutkan dengan cara logis yang Dukungan digunakan untuk menguji dan menyetel implementasi S3 File Gateway. Saat Anda menerapkan dan menguji saran ini, ingatlah bahwa setiap penerapan S3 File Gateway adalah unik, sehingga hasil Anda dapat bervariasi.

S3 File Gateway menyediakan antarmuka file untuk menyimpan dan mengambil objek Amazon S3 menggunakan protokol file NFS atau SMB standar industri, dengan pemetaan asli 1:1 antara file dan objek. Anda menerapkan S3 File Gateway sebagai mesin virtual baik lokal di lingkungan VMware Microsoft Hyper-V, atau Linux KVM Anda, atau di cloud sebagai AWS instans Amazon EC2. S3 File Gateway tidak dirancang untuk bertindak sebagai pengganti NAS perusahaan penuh. S3 File Gateway mengemulasi sistem file, tetapi ini bukan sistem file. Menggunakan Amazon S3 sebagai penyimpanan backend yang tahan lama menciptakan overhead tambahan pada setiap I/O operasi, jadi mengevaluasi kinerja Gateway File S3 terhadap NAS atau server file yang ada bukanlah perbandingan yang setara.

Terapkan gateway Anda di lokasi yang sama dengan klien Anda

Sebaiknya gunakan alat virtual S3 File Gateway Anda di lokasi fisik dengan latensi jaringan sesedikit mungkin antara itu dan klien NFS atau SMB Anda. Saat memilih lokasi untuk gateway Anda, pertimbangkan hal berikut:

- Latensi jaringan yang lebih rendah ke gateway dapat membantu meningkatkan kinerja klien NFS atau SMB.
- S3 File Gateway dirancang untuk mentolerir latensi jaringan yang lebih tinggi antara gateway dan Amazon S3 daripada antara gateway dan klien.
- Untuk instans Gateway File S3 yang diterapkan di Amazon EC2, sebaiknya simpan gateway dan klien NFS atau SMB dalam grup penempatan yang sama. Untuk informasi selengkapnya, lihat Grup penempatan untuk instans Amazon EC2 Anda di Panduan Pengguna Amazon Elastic Compute Cloud.

Mengurangi kemacetan yang disebabkan oleh disk yang lambat

Kami merekomendasikan pemantauan `IoWaitPercent` CloudWatch metrik untuk mengidentifikasi kemacetan kinerja yang dapat dihasilkan dari disk penyimpanan yang lambat pada Gateway File S3 Anda. Saat mencoba mengoptimalkan masalah kinerja terkait disk, pertimbangkan hal berikut:

- `IoWaitPercent`melaporkan persentase waktu CPU menunggu respons dari disk root atau cache.
- Ketika `IoWaitPercent` lebih besar dari 5-10%, ini biasanya menunjukkan hambatan kinerja gateway yang disebabkan oleh disk yang berkinerja buruk. Metrik ini harus sedekat mungkin dengan 0% - artinya gateway tidak pernah menunggu di disk - yang membantu mengoptimalkan sumber daya CPU.
- Anda dapat memeriksa tab Monitoring **`IoWaitPercent`** pada konsol Storage Gateway, atau mengonfigurasi CloudWatch alarm yang disarankan untuk memberi tahu Anda secara otomatis jika metrik melonjak di atas ambang batas tertentu. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm yang direkomendasikan untuk gateway Anda.
- Sebaiknya gunakan salah satu NVMe atau SSD untuk disk root dan cache gateway Anda untuk meminimalkan`IoWaitPercent`.

Sesuaikan alokasi sumber daya mesin virtual untuk disk CPU, RAM, dan cache

Saat mencoba mengoptimalkan throughput untuk Gateway File S3 Anda, penting untuk mengalokasikan sumber daya yang cukup ke VM gateway, termasuk CPU, RAM, dan disk cache. Persyaratan sumber daya virtual minimum 4 CPUs, RAM 16GB, dan penyimpanan cache 150GB biasanya hanya cocok untuk beban kerja yang lebih kecil. Saat mengalokasikan sumber daya virtual untuk beban kerja yang lebih besar, kami merekomendasikan hal berikut:

- Tingkatkan jumlah yang dialokasikan CPUs menjadi antara 16 dan 48, tergantung pada penggunaan CPU khas yang dihasilkan oleh Gateway File S3 Anda. Anda dapat memantau penggunaan CPU menggunakan `UserCpuPercent` metrik. Untuk informasi selengkapnya, lihat Memahami metrik gateway.
- Tingkatkan RAM yang dialokasikan menjadi antara 32 dan 64 GB.

> **Note**
>
> S3 File Gateway tidak dapat menggunakan lebih dari 64 GB RAM.

- Gunakan NVMe atau SSD untuk disk root dan disk cache, dan ukuran disk cache Anda agar sejajar dengan kumpulan data kerja puncak yang Anda rencanakan untuk ditulis ke gateway. Untuk informasi selengkapnya, lihat praktik terbaik ukuran cache S3 File Gateway di saluran Amazon Web Services YouTube resmi.
- Tambahkan setidaknya 4 disk cache virtual ke gateway, daripada menggunakan satu disk besar. Beberapa disk virtual dapat meningkatkan kinerja bahkan jika mereka berbagi disk fisik dasar yang sama, tetapi perbaikan biasanya lebih besar ketika disk virtual terletak pada disk fisik dasar yang berbeda.

  Misalnya, jika Anda ingin menyebarkan cache 12TB, Anda dapat menggunakan salah satu konfigurasi berikut:

  - Disk cache 4 x 3 TB
  - Disk cache 8 x 1,5 TB
  - Disk cache 12 x 1 TB

  Selain kinerja, ini memungkinkan manajemen mesin virtual yang lebih efisien dari waktu ke waktu. Saat beban kerja Anda berubah, Anda dapat secara bertahap meningkatkan jumlah disk cache dan kapasitas cache Anda secara keseluruhan, sambil mempertahankan ukuran asli setiap disk virtual individu untuk menjaga integritas gateway.

  Untuk informasi selengkapnya, lihat Menentukan jumlah penyimpanan disk lokal.

Saat menerapkan S3 File Gateway sebagai instans Amazon EC2, pertimbangkan hal berikut:

- Jenis instans yang Anda pilih dapat memengaruhi kinerja gateway secara signifikan. Amazon EC2 memberikan fleksibilitas luas untuk menyesuaikan alokasi sumber daya untuk instans Gateway File S3 Anda.
- Untuk jenis instans Amazon EC2 yang direkomendasikan untuk Gateway File S3, lihat Persyaratan untuk jenis instans Amazon EC2.
- Anda dapat mengubah jenis instans Amazon EC2 yang menghosting Gateway File S3 aktif. Ini memungkinkan Anda untuk dengan mudah menyesuaikan pembuatan perangkat keras Amazon EC2 dan alokasi sumber daya untuk menemukan rasio yang ideal. price-to-performance Untuk mengubah jenis instans, gunakan prosedur berikut di konsol Amazon EC2:

  1. Hentikan instans Amazon EC2.
  2. Ubah jenis instans Amazon EC2.
  3. Nyalakan instans Amazon EC2.

> **Note**
>
> Menghentikan instance yang meng-host S3 File Gateway untuk sementara akan mengganggu akses berbagi file. Pastikan untuk menjadwalkan jendela pemeliharaan jika perlu.

- price-to-performanceRasio instans Amazon EC2 mengacu pada berapa banyak daya komputasi yang Anda dapatkan untuk harga yang Anda bayar. Biasanya, instans Amazon EC2 generasi yang lebih baru menawarkan rasio price-to-performance terbaik, dengan perangkat keras yang lebih baru dan peningkatan kinerja dengan biaya yang relatif lebih rendah dibandingkan dengan generasi yang lebih tua. Faktor-faktor seperti jenis instans, wilayah, dan pola penggunaan memengaruhi rasio ini, jadi penting untuk memilih instance yang tepat untuk beban kerja spesifik Anda guna mengoptimalkan efektivitas biaya.

Sesuaikan tingkat keamanan SMB

SMBv3 Protokol ini memungkinkan penandatanganan SMB dan enkripsi SMB, yang memiliki beberapa pertukaran dalam kinerja dan keamanan. Untuk mengoptimalkan throughput, Anda dapat menyesuaikan tingkat keamanan SMB gateway Anda untuk menentukan fitur keamanan mana yang diberlakukan untuk koneksi klien. Untuk informasi selengkapnya, lihat Menetapkan tingkat keamanan untuk gateway Anda.

Saat menyesuaikan tingkat keamanan SMB, pertimbangkan hal berikut:

- Tingkat keamanan default untuk S3 File Gateway adalah Enforce encryption. Pengaturan ini memberlakukan enkripsi dan penandatanganan untuk koneksi klien SMB ke berbagi file gateway, yang berarti bahwa semua lalu lintas dari klien ke gateway dienkripsi. Pengaturan ini tidak memengaruhi lalu lintas dari gateway ke AWS, yang selalu dienkripsi.

  Gateway membatasi setiap koneksi klien terenkripsi ke satu vCPU. Misalnya, jika Anda hanya memiliki 1 klien terenkripsi, maka klien itu akan dibatasi hanya 1 vCPU, bahkan jika 4 atau lebih v CPUs dialokasikan ke gateway. Karena itu, throughput untuk koneksi terenkripsi dari satu klien ke S3 File Gateway biasanya terhambat antara 40-60 MB/s.
- Jika persyaratan keamanan Anda memungkinkan postur yang lebih santai, Anda dapat mengubah tingkat keamanan ke Klien yang dinegosiasikan, yang akan menonaktifkan enkripsi SMB dan menegakkan penandatanganan SMB saja. Dengan pengaturan ini, koneksi klien ke gateway dapat memanfaatkan beberapa vCPUs, yang biasanya menghasilkan peningkatan kinerja throughput.

> **Note**
>
> Setelah Anda mengubah tingkat keamanan SMB untuk Gateway File S3 Anda, Anda harus menunggu status berbagi file berubah dari Memperbarui ke Tersedia di konsol Storage Gateway, lalu putuskan dan sambungkan kembali klien SMB Anda agar pengaturan baru diterapkan.

Gunakan beberapa utas dan klien untuk memparalelkan operasi penulisan

Sulit untuk mencapai kinerja throughput maksimum dengan S3 File Gateway yang hanya menggunakan satu klien NFS atau SMB untuk menulis satu file pada satu waktu, karena penulisan berurutan dari satu klien adalah operasi single-threaded. Sebagai gantinya, sebaiknya gunakan beberapa utas dari setiap klien NFS atau SMB untuk menulis beberapa file secara paralel, dan menggunakan beberapa klien NFS atau SMB secara bersamaan ke Gateway File S3 Anda untuk memaksimalkan throughput gateway.

Menggunakan beberapa utas dapat meningkatkan kinerja secara signifikan. Namun, menggunakan lebih banyak thread membutuhkan lebih banyak sumber daya sistem, yang dapat berdampak negatif pada kinerja jika gateway tidak berukuran untuk memenuhi peningkatan beban. Dalam penerapan tipikal, Anda dapat mengharapkan untuk mencapai kinerja throughput yang lebih baik saat Anda menambahkan lebih banyak utas dan klien, hingga Anda mencapai batasan perangkat keras dan bandwidth maksimum untuk gateway Anda. Sebaiknya bereksperimen dengan jumlah thread yang berbeda untuk menemukan keseimbangan optimal antara kecepatan dan penggunaan sumber daya sistem untuk konfigurasi perangkat keras dan jaringan spesifik Anda.

Pertimbangkan informasi berikut tentang alat umum yang dapat membantu Anda menguji utas dan konfigurasi klien Anda:

- Anda dapat menguji kinerja penulisan multithreaded dengan menggunakan alat seperti robocopy untuk menyalin satu set file ke berbagi file di gateway Anda. Secara default, robocopy menggunakan 8 utas saat menyalin file, tetapi Anda dapat menentukan hingga 128 utas.

  Untuk menggunakan beberapa utas dengan robocopy, tambahkan `/MT:`n sakelar ke perintah Anda, di mana n jumlah utas yang ingin Anda gunakan. Contoh:

  ```
  robocopy C:\source D:\destination /MT:64
  ```

Perintah ini akan menggunakan 64 utas untuk operasi penyalinan.

> **Note**
>
> Kami tidak menyarankan menggunakan Windows Explorer untuk menyeret dan melepaskan file saat menguji throughput maksimum, karena metode ini terbatas pada satu utas dan menyalin file secara berurutan.

Untuk informasi selengkapnya, lihat robocopy di situs web Microsoft Learn.

- Anda juga dapat melakukan tes menggunakan alat benchmarking penyimpanan umum seperti DISKSPD, atau FIO. Alat-alat ini memiliki opsi untuk menyesuaikan jumlah utas, kedalaman I/O, dan parameter lainnya agar sesuai dengan persyaratan beban kerja spesifik Anda.

  DiskSpd memungkinkan Anda untuk mengontrol jumlah utas menggunakan `-t` parameter. Contoh:

  ```
  diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
  ```

  Perintah contoh ini melakukan hal berikut:

  - Membuat file uji 10GB () `-c1G`
  - Berjalan selama 300 detik (`-d300`)
  - Melakukan I/O tes acak dengan 50% membaca 50% menulis (`-r -w50`)
  - Menggunakan 64 thread (`-t64`)
  - Menetapkan kedalaman antrian menjadi 32 per utas () `-o32`
  - Menggunakan ukuran blok 1MB () `-b1M`
  - Menonaktifkan cache perangkat keras dan perangkat lunak () `-h -L`

  Untuk informasi selengkapnya, lihat Menggunakan DISKSPD untuk menguji kinerja penyimpanan beban kerja di situs web Microsoft Learn.

- FIO menggunakan `numjobs` parameter untuk mengontrol jumlah thread paralel. Contoh:

  ```
  fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
  --size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
  group_reporting
  ```

  Perintah contoh ini melakukan hal berikut:

- Melakukan I/O tes acak (`--rw=randrw`)
- Melakukan 70% membaca dan 30% menulis (`--rwmixread=70`)
- Menggunakan ukuran blok 1MB () `--bs=1M`
- Menetapkan I/O kedalaman ke 64 (`--iodepth=64`)
- Tes pada file 10 GB (`--size=10G`)
- Berjalan selama 5 menit (`--runtime=300`)
- Menciptakan 64 pekerjaan paralel (thread) (`--numjobs=64`)
- Menggunakan mesin asinkron I/O () `--ioengine=libaio`
- Kelompokkan hasil untuk analisis yang lebih mudah (`--group_reporting`)

  Untuk informasi lebih lanjut, lihat halaman manual Fio Linux.

-

Matikan penyegaran cache otomatis

Fitur penyegaran cache otomatis memungkinkan Gateway File S3 Anda menyegarkan metadatanya secara otomatis, yang dapat membantu menangkap perubahan apa pun yang dilakukan pengguna atau aplikasi ke file Anda yang disetel dengan menulis ke bucket Amazon S3 secara langsung, bukan melalui gateway. Untuk informasi selengkapnya, lihat Menyegarkan cache objek bucket Amazon S3.

Untuk mengoptimalkan throughput gateway, kami sarankan untuk menonaktifkan fitur ini dalam penerapan di mana semua pembacaan dan penulisan ke bucket Amazon S3 akan dilakukan melalui Gateway File S3 Anda.

Saat mengonfigurasi penyegaran cache otomatis, pertimbangkan hal berikut:

- Jika Anda perlu menggunakan penyegaran cache otomatis karena pengguna atau aplikasi dalam penerapan Anda sesekali menulis ke Amazon S3 secara langsung, maka kami sarankan untuk mengonfigurasi interval waktu terpanjang antara penyegaran yang masih praktis untuk kebutuhan bisnis Anda. Interval penyegaran cache yang lebih lama membantu mengurangi jumlah operasi metadata yang perlu dilakukan gateway saat menjelajahi direktori atau memodifikasi file.

  Misalnya: atur penyegaran cache otomatis ke 24 jam, bukan 5 menit, jika itu dapat ditoleransi untuk beban kerja Anda.
- Interval waktu minimum adalah 5 menit. Interval maksimum adalah 30 hari.

- Jika Anda memilih untuk mengatur interval penyegaran cache yang sangat singkat, kami sarankan untuk menguji pengalaman penelusuran direktori untuk klien NFS dan SMB Anda. Waktu yang diperlukan untuk menyegarkan cache gateway dapat meningkat secara substansional tergantung pada jumlah file dan subdirektori di bucket Amazon S3 Anda.

Tingkatkan jumlah utas pengunggah Amazon S3

Secara default, S3 File Gateway membuka 8 utas untuk unggahan data Amazon S3, yang menyediakan kapasitas unggah yang cukup untuk sebagian besar penerapan umum. Namun, gateway dapat menerima data dari klien NFS dan SMB pada tingkat yang lebih tinggi daripada yang dapat diunggah ke Amazon S3 dengan kapasitas utas 8 standar, yang dapat menyebabkan cache lokal mencapai batas penyimpanannya.

Dalam keadaan tertentu, Dukungan dapat meningkatkan jumlah kumpulan thread upload Amazon S3 untuk gateway Anda dari 8 menjadi 40, yang memungkinkan lebih banyak data untuk diunggah secara paralel. Bergantung pada bandwidth dan faktor lain yang spesifik untuk penerapan Anda, ini dapat meningkatkan kinerja unggahan secara signifikan dan membantu mengurangi jumlah penyimpanan cache yang diperlukan untuk mendukung beban kerja Anda.

Sebaiknya gunakan `CachePercentDirty` CloudWatch metrik untuk memantau jumlah data yang disimpan di disk cache gateway lokal yang belum diunggah ke Amazon S3, dan Dukungan menghubungi untuk membantu menentukan apakah peningkatan jumlah kumpulan utas unggahan dapat meningkatkan throughput untuk Gateway File S3 Anda. Untuk informasi selengkapnya, lihat Memahami metrik gateway.

> **Note**
>
> Pengaturan ini menggunakan sumber daya CPU gateway tambahan. Kami merekomendasikan pemantauan penggunaan CPU gateway dan meningkatkan sumber daya CPU yang dialokasikan jika perlu.

Tingkatkan pengaturan batas waktu SMB

Ketika S3 File Gateway menyalin file besar ke berbagi file SMB, koneksi klien SMB dapat batas waktu setelah jangka waktu yang lama.

Kami merekomendasikan untuk memperpanjang pengaturan batas waktu sesi SMB untuk klien SMB Anda hingga 20 menit atau lebih, tergantung pada ukuran file dan kecepatan tulis gateway Anda. Defaultnya adalah 300 detik, atau 5 menit. Untuk informasi selengkapnya, lihat Pekerjaan pencadangan gateway Anda gagal atau ada kesalahan saat menulis ke gateway Anda.

Aktifkan penguncian oportunistik untuk aplikasi yang kompatibel

Penguncian oportunistik, atau “oplocks”, diaktifkan secara default untuk setiap Gateway File S3 baru. Saat menggunakan oplock dengan aplikasi yang kompatibel, klien mengumpulkan beberapa operasi yang lebih kecil menjadi yang lebih besar, yang lebih efisien untuk klien, gateway, dan jaringan. Sebaiknya aktifkan penguncian oportunistik jika Anda menggunakan aplikasi yang memanfaatkan caching lokal sisi klien, seperti Microsoft Office, Adobe Suite, dan banyak lainnya, karena dapat meningkatkan kinerja secara signifikan.

Jika Anda mematikan penguncian oportunistik, aplikasi yang mendukung oplock biasanya akan membuka file besar (50 MB atau lebih besar) jauh lebih lambat. Penundaan ini terjadi karena gateway mengirimkan data dalam 4 bagian KB, yang menghasilkan throughput tinggi I/O dan rendah.

Sesuaikan kapasitas gateway sesuai dengan ukuran set file kerja

Parameter kapasitas gateway menentukan jumlah maksimum file yang gateway Anda akan menyimpan metadata dalam cache lokalnya. Secara default, kapasitas gateway diatur ke Kecil, yang berarti gateway menyimpan metadata hingga 5 juta file. Pengaturan default berfungsi dengan baik untuk sebagian besar beban kerja, bahkan jika ada ratusan juta, atau bahkan miliaran objek di Amazon S3, karena hanya sebagian kecil file yang diakses secara aktif pada waktu tertentu dalam penerapan tipikal. Kelompok file ini disebut sebagai “set kerja”.

Jika beban kerja Anda secara teratur mengakses satu set file kerja yang lebih besar dari 5 juta, maka gateway Anda perlu melakukan penggusuran cache yang sering, yang merupakan operasi I/O kecil yang disimpan dalam RAM dan bertahan pada disk root. Ini dapat berdampak negatif pada kinerja gateway saat gateway mengambil data baru dari Amazon S3.

Anda dapat memantau `IndexEvictions` metrik untuk menentukan jumlah file yang metadatanya dikeluarkan dari cache untuk memberi ruang bagi entri baru. Untuk informasi selengkapnya, lihat Memahami metrik gateway.

Sebaiknya gunakan tindakan `UpdateGatewayInformation` API untuk meningkatkan kapasitas gateway agar sesuai dengan jumlah file dalam set kerja tipikal Anda. Untuk informasi selengkapnya, lihat UpdateGatewayInformation.

> **Note**
>
> Meningkatkan kapasitas gateway membutuhkan RAM tambahan dan kapasitas root disk.
>
> - Kecil (5 juta file) membutuhkan setidaknya 16 GB RAM dan 80 GB root disk.
> - Medium (10 juta file) membutuhkan setidaknya 32 GB RAM dan 160 GB root disk.
> - Besar (20 juta file) membutuhkan 64 GB RAM dan 240 GB root disk.

> **Important**
>
> Kapasitas gateway tidak dapat dikurangi.

Terapkan beberapa gateway untuk beban kerja yang lebih besar

Sebaiknya pisahkan beban kerja Anda di beberapa gateway bila memungkinkan, daripada mengkonsolidasikan banyak pembagian file pada satu gateway besar. Misalnya, Anda dapat mengisolasi satu berbagi file yang banyak digunakan pada satu gateway, sambil mengelompokkan berbagi file yang jarang digunakan bersama-sama di gateway lain.

Saat merencanakan penerapan dengan beberapa gateway dan berbagi file, pertimbangkan hal berikut:

- Jumlah maksimum berbagi file pada satu gateway adalah 50, tetapi jumlah berbagi file yang dikelola oleh gateway dapat memengaruhi kinerja gateway. Untuk informasi selengkapnya, lihat Panduan kinerja untuk gateway dengan beberapa berbagi file.
- Sumber daya pada setiap Gateway File S3 dibagikan di semua berbagi file, tanpa partisi.
- Berbagi file tunggal dengan penggunaan berat dapat memengaruhi kinerja berbagi file lain di gateway.

> **Note**
>
> Kami tidak menyarankan membuat beberapa berbagi file yang dipetakan ke lokasi Amazon S3 yang sama dari beberapa gateway, kecuali setidaknya satu di antaranya hanya-baca.

Menulis simultan ke file yang sama dari beberapa gateway dianggap sebagai skenario multi-penulis, yang dapat menyebabkan masalah integritas data.

Mengoptimalkan Gateway File S3 untuk backup database SQL Server

Pencadangan basis data adalah kasus penggunaan yang umum dan direkomendasikan untuk S3 File Gateway, yang menyediakan retensi jangka pendek dan jangka panjang yang hemat biaya dengan menyimpan cadangan basis data di Amazon S3, dengan kemampuan siklus hidup untuk menurunkan tingkat penyimpanan biaya sesuai kebutuhan. Dengan solusi ini, Anda dapat mengurangi kebutuhan akan aplikasi cadangan perusahaan menggunakan alat bawaan seperti SQL Server Management Studio dan Oracle RMAN.

Bagian berikut menjelaskan praktik terbaik untuk menyetel penerapan Gateway File S3 Anda untuk kinerja yang dioptimalkan dan dukungan hemat biaya untuk ratusan terabyte cadangan database SQL. Panduan yang diberikan di setiap bagian berkontribusi secara bertahap untuk meningkatkan throughput secara keseluruhan. Meskipun tidak satu pun dari rekomendasi ini diperlukan, dan mereka tidak saling bergantung, mereka telah dipilih dan diurutkan dengan cara logis yang Dukungan digunakan untuk menguji dan menyetel implementasi S3 File Gateway. Saat Anda menerapkan dan menguji saran ini, ingatlah bahwa setiap penerapan S3 File Gateway adalah unik, sehingga hasil Anda dapat bervariasi.

S3 File Gateway menyediakan antarmuka file untuk menyimpan dan mengambil objek Amazon S3 menggunakan protokol file NFS atau SMB standar industri, dengan pemetaan asli 1:1 antara file dan objek. Anda menerapkan S3 File Gateway sebagai mesin virtual baik lokal di lingkungan VMware Microsoft Hyper-V, atau Linux KVM Anda, atau di cloud sebagai AWS instans Amazon EC2. S3 File Gateway tidak dirancang untuk bertindak sebagai pengganti NAS perusahaan penuh. S3 File Gateway mengemulasi sistem file, tetapi ini bukan sistem file. Menggunakan Amazon S3 sebagai penyimpanan backend yang tahan lama menciptakan overhead tambahan pada setiap I/O operasi, jadi mengevaluasi kinerja Gateway File S3 terhadap NAS atau server file yang ada bukanlah perbandingan yang setara.

Menerapkan gateway Anda di lokasi yang sama dengan SQL Server

Sebaiknya gunakan alat virtual S3 File Gateway Anda di lokasi fisik dengan latensi jaringan sesedikit mungkin antara itu dan server SQL Anda. Saat memilih lokasi untuk gateway Anda, pertimbangkan hal berikut:

- Latensi jaringan yang lebih rendah ke gateway dapat membantu meningkatkan kinerja klien SMB, seperti server SQL.
- S3 File Gateway dirancang untuk mentolerir latensi jaringan yang lebih tinggi antara gateway dan Amazon S3 daripada antara gateway dan klien.
- Untuk instans Gateway File S3 yang diterapkan di Amazon EC2, sebaiknya simpan gateway dan server SQL dalam grup penempatan yang sama. Untuk informasi selengkapnya, lihat Grup penempatan untuk instans Amazon EC2 Anda di Panduan Pengguna Amazon Elastic Compute Cloud.

Mengurangi kemacetan yang disebabkan oleh disk yang lambat

Kami merekomendasikan pemantauan `IoWaitPercent` CloudWatch metrik untuk mengidentifikasi kemacetan kinerja yang dapat dihasilkan dari disk penyimpanan yang lambat pada Gateway File S3 Anda. Saat mencoba mengoptimalkan masalah kinerja terkait disk, pertimbangkan hal berikut:

- `IoWaitPercent`melaporkan persentase waktu CPU menunggu respons dari disk root atau cache.
- Ketika `IoWaitPercent` lebih besar dari 5-10%, ini biasanya menunjukkan hambatan kinerja gateway yang disebabkan oleh disk yang berkinerja buruk. Metrik ini harus sedekat mungkin dengan 0% - artinya gateway tidak pernah menunggu di disk - yang membantu mengoptimalkan sumber daya CPU.
- Anda dapat memeriksa tab Monitoring **`IoWaitPercent`** pada konsol Storage Gateway, atau mengonfigurasi CloudWatch alarm yang disarankan untuk memberi tahu Anda secara otomatis jika metrik melonjak di atas ambang batas tertentu. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm yang direkomendasikan untuk gateway Anda.
- Sebaiknya gunakan salah satu NVMe atau SSD untuk disk root dan cache gateway Anda untuk meminimalkan`IoWaitPercent`.

Sesuaikan alokasi sumber daya mesin virtual S3 File Gateway untuk disk CPU, RAM, dan cache

Saat mencoba mengoptimalkan throughput untuk Gateway File S3 Anda, penting untuk mengalokasikan sumber daya yang cukup ke VM gateway, termasuk CPU, RAM, dan disk cache. Persyaratan sumber daya virtual minimum 4 CPUs, RAM 16GB, dan penyimpanan cache 150GB biasanya hanya cocok untuk beban kerja yang lebih kecil. Saat mengalokasikan sumber daya virtual untuk beban kerja yang lebih besar, kami merekomendasikan hal berikut:

- Tingkatkan jumlah yang dialokasikan CPUs menjadi antara 16 dan 48, tergantung pada penggunaan CPU khas yang dihasilkan oleh Gateway File S3 Anda. Anda dapat memantau penggunaan CPU menggunakan `UserCpuPercent` metrik. Untuk informasi selengkapnya, lihat Memahami metrik gateway.
- Tingkatkan RAM yang dialokasikan menjadi antara 32 dan 64 GB.

> **Note**
>
> S3 File Gateway tidak dapat menggunakan lebih dari 64 GB RAM.

- Gunakan NVMe atau SSD untuk disk root dan disk cache, dan ukuran disk cache Anda agar sejajar dengan kumpulan data kerja puncak yang Anda rencanakan untuk ditulis ke gateway. Untuk informasi selengkapnya, lihat praktik terbaik ukuran cache S3 File Gateway di saluran Amazon Web Services YouTube resmi.
- Tambahkan setidaknya 4 disk cache virtual ke gateway, daripada menggunakan satu disk besar. Beberapa disk virtual dapat meningkatkan kinerja bahkan jika mereka berbagi disk fisik dasar yang sama, tetapi perbaikan biasanya lebih besar ketika disk virtual terletak pada disk fisik dasar yang berbeda.

  Misalnya, jika Anda ingin menyebarkan cache 12TB, Anda dapat menggunakan salah satu konfigurasi berikut:

  - Disk cache 4 x 3 TB
  - Disk cache 8 x 1,5 TB
  - Disk cache 12 x 1 TB

  Selain kinerja, ini memungkinkan manajemen mesin virtual yang lebih efisien dari waktu ke waktu. Saat beban kerja Anda berubah, Anda dapat secara bertahap meningkatkan jumlah disk cache dan kapasitas cache Anda secara keseluruhan, sambil mempertahankan ukuran asli setiap disk virtual individu untuk menjaga integritas gateway.

  Untuk informasi selengkapnya, lihat Menentukan jumlah penyimpanan disk lokal.

Saat menerapkan S3 File Gateway sebagai instans Amazon EC2, pertimbangkan hal berikut:

- Jenis instans yang Anda pilih dapat memengaruhi kinerja gateway secara signifikan. Amazon EC2 memberikan fleksibilitas luas untuk menyesuaikan alokasi sumber daya untuk instans Gateway File S3 Anda.

- Untuk jenis instans Amazon EC2 yang direkomendasikan untuk Gateway File S3, lihat Persyaratan untuk jenis instans Amazon EC2.
- Anda dapat mengubah jenis instans Amazon EC2 yang menghosting Gateway File S3 aktif. Ini memungkinkan Anda untuk dengan mudah menyesuaikan pembuatan perangkat keras Amazon EC2 dan alokasi sumber daya untuk menemukan rasio yang ideal. price-to-performance Untuk mengubah jenis instans, gunakan prosedur berikut di konsol Amazon EC2:

  1. Hentikan instans Amazon EC2.
  2. Ubah jenis instans Amazon EC2.
  3. Nyalakan instans Amazon EC2.

  > **Note**
  >
  > Menghentikan instance yang meng-host S3 File Gateway untuk sementara akan mengganggu akses berbagi file. Pastikan untuk menjadwalkan jendela pemeliharaan jika perlu.

- price-to-performanceRasio instans Amazon EC2 mengacu pada berapa banyak daya komputasi yang Anda dapatkan untuk harga yang Anda bayar. Biasanya, instans Amazon EC2 generasi yang lebih baru menawarkan rasio price-to-performance terbaik, dengan perangkat keras yang lebih baru dan peningkatan kinerja dengan biaya yang relatif lebih rendah dibandingkan dengan generasi yang lebih tua. Faktor-faktor seperti jenis instans, wilayah, dan pola penggunaan memengaruhi rasio ini, jadi penting untuk memilih instance yang tepat untuk beban kerja spesifik Anda guna mengoptimalkan efektivitas biaya.

Tingkatkan throughput klien SMB dengan menyesuaikan tingkat keamanan Gateway File S3 Anda

SMBv3 Protokol ini memungkinkan penandatanganan SMB dan enkripsi SMB, yang memiliki beberapa pertukaran dalam kinerja dan keamanan. Untuk mengoptimalkan throughput, Anda dapat menyesuaikan tingkat keamanan SMB gateway Anda untuk menentukan fitur keamanan mana yang diberlakukan untuk koneksi klien. Untuk informasi selengkapnya, lihat Menetapkan tingkat keamanan untuk gateway Anda.

Saat menyesuaikan tingkat keamanan SMB, pertimbangkan hal berikut:

- Tingkat keamanan default untuk S3 File Gateway adalah Enforce encryption. Pengaturan ini memberlakukan enkripsi dan penandatanganan untuk koneksi klien SMB ke berbagi file gateway, yang berarti bahwa semua lalu lintas dari klien ke gateway dienkripsi. Pengaturan ini tidak memengaruhi lalu lintas dari gateway ke AWS, yang selalu dienkripsi.

  Gateway membatasi setiap koneksi klien terenkripsi ke satu vCPU. Misalnya, jika Anda hanya memiliki 1 klien terenkripsi, maka klien itu akan dibatasi hanya 1 vCPU, bahkan jika 4 atau lebih v CPUs dialokasikan ke gateway. Karena itu, throughput untuk koneksi terenkripsi dari satu klien ke S3 File Gateway biasanya terhambat antara 40-60 MB/s.
- Jika persyaratan keamanan Anda memungkinkan postur yang lebih santai, Anda dapat mengubah tingkat keamanan ke Klien yang dinegosiasikan, yang akan menonaktifkan enkripsi SMB dan menegakkan penandatanganan SMB saja. Dengan pengaturan ini, koneksi klien ke gateway dapat memanfaatkan beberapa vCPUs, yang biasanya menghasilkan peningkatan kinerja throughput.

> **Note**
>
> Setelah Anda mengubah tingkat keamanan SMB untuk Gateway File S3 Anda, Anda harus menunggu status berbagi file berubah dari Memperbarui ke Tersedia di konsol Storage Gateway, lalu putuskan dan sambungkan kembali klien SMB Anda agar pengaturan baru diterapkan.

Tingkatkan throughput klien SMB dengan membagi cadangan SQL menjadi beberapa file

- Sulit untuk mencapai kinerja throughput maksimum dengan S3 File Gateway yang hanya satu server SQL menulis satu file pada satu waktu, karena penulisan berurutan dari server SQL tunggal adalah operasi single-threaded. Sebagai gantinya, sebaiknya gunakan beberapa thread dari setiap server SQL untuk menulis beberapa file secara paralel, dan menggunakan beberapa server SQL secara bersamaan ke S3 File Gateway Anda untuk memaksimalkan throughput gateway. Dengan cadangan SQL, membagi cadangan menjadi beberapa file memungkinkan setiap file menggunakan utas terpisah, yang akan menulis beberapa file secara bersamaan ke berbagi file S3 File Gateway. Semakin banyak thread yang Anda miliki, semakin banyak throughput yang dapat Anda capai, hingga batas gateway.
- SQL Server mendukung penulisan ke beberapa file pada saat yang sama selama operasi pencadangan tunggal. Misalnya, Anda dapat menentukan beberapa tujuan file menggunakan

perintah T-SQL atau SQL Server Management Studio (SSMS). Setiap file menggunakan thread terpisah untuk mengirim data dari server SQL ke berbagi file gateway. Pendekatan ini memungkinkan I/O throughput yang lebih baik, yang secara signifikan dapat meningkatkan kecepatan dan efisiensi cadangan.

Saat mengonfigurasi cadangan server SQL Anda, pertimbangkan hal berikut:

- Dengan membagi backup menjadi beberapa file, admin SQL Server dapat mengoptimalkan waktu backup dan mengelola backup database besar dengan lebih efektif.
- Jumlah file yang digunakan tergantung pada konfigurasi penyimpanan server dan persyaratan kinerja. Untuk database besar, kami sarankan untuk memecah cadangan menjadi beberapa file yang lebih kecil antara 10 GB dan 20 GB masing-masing.
- Tidak ada batasan ketat pada berapa banyak file SQL Server dapat menulis ke selama backup, tetapi pertimbangan praktis seperti arsitektur penyimpanan dan bandwidth jaringan harus memandu pilihan ini.

Untuk informasi lebih lanjut, lihat:

- Cadangkan SQL Server 43-67% lebih cepat dengan menulis ke beberapa file
- Simpan backup SQL Server Anda dengan mudah di Amazon S3 menggunakan File Gateway

Mencegah kegagalan salinan file besar dengan meningkatkan pengaturan batas waktu SMB

Ketika S3 File Gateway menyalin file cadangan SQL besar ke berbagi file SMB, koneksi klien SMB dapat batas waktu setelah jangka waktu yang lama. Sebaiknya perpanjang pengaturan batas waktu sesi SMB untuk klien SMB SQL server Anda hingga 20 menit atau lebih, tergantung pada ukuran file dan kecepatan tulis gateway Anda. Defaultnya adalah 300 detik, atau 5 menit. Untuk informasi selengkapnya, lihat Pekerjaan pencadangan gateway Anda gagal atau ada kesalahan saat menulis ke gateway Anda.

Tingkatkan jumlah utas pengunggah Amazon S3

Secara default, S3 File Gateway membuka 8 utas untuk unggahan data Amazon S3, yang menyediakan kapasitas unggah yang cukup untuk sebagian besar penerapan umum. Namun, gateway dapat menerima data dari server SQL dengan kecepatan yang lebih tinggi daripada yang

dapat diunggah ke Amazon S3 dengan kapasitas utas 8 standar, yang dapat menyebabkan cache lokal mencapai batas penyimpanannya.

Dalam keadaan tertentu, Dukungan dapat meningkatkan jumlah kumpulan thread upload Amazon S3 untuk gateway Anda dari 8 menjadi 40, yang memungkinkan lebih banyak data untuk diunggah secara paralel. Bergantung pada bandwidth dan faktor lain yang spesifik untuk penerapan Anda, ini dapat meningkatkan kinerja unggahan secara signifikan dan membantu mengurangi jumlah penyimpanan cache yang diperlukan untuk mendukung beban kerja Anda.

Sebaiknya gunakan `CachePercentDirty` CloudWatch metrik untuk memantau jumlah data yang disimpan di disk cache gateway lokal yang belum diunggah ke Amazon S3, dan Dukungan menghubungi untuk membantu menentukan apakah peningkatan jumlah kumpulan utas unggahan dapat meningkatkan throughput untuk Gateway File S3 Anda. Untuk informasi selengkapnya, lihat Memahami metrik gateway.

> **Note**
>
> Pengaturan ini menggunakan sumber daya CPU gateway tambahan. Kami merekomendasikan pemantauan penggunaan CPU gateway dan meningkatkan sumber daya CPU yang dialokasikan jika perlu.

Matikan penyegaran cache otomatis

Fitur penyegaran cache otomatis memungkinkan Gateway File S3 Anda menyegarkan metadatanya secara otomatis, yang dapat membantu menangkap perubahan apa pun yang dilakukan pengguna atau aplikasi ke file Anda yang disetel dengan menulis ke bucket Amazon S3 secara langsung, bukan melalui gateway. Untuk informasi selengkapnya, lihat Menyegarkan cache objek bucket Amazon S3.

Untuk mengoptimalkan throughput gateway, kami sarankan untuk menonaktifkan fitur ini dalam penerapan di mana semua pembacaan dan penulisan ke bucket Amazon S3 akan dilakukan melalui Gateway File S3 Anda.

Saat mengonfigurasi penyegaran cache otomatis, pertimbangkan hal berikut:

- Jika Anda perlu menggunakan penyegaran cache otomatis karena pengguna atau aplikasi dalam penerapan Anda sesekali menulis ke Amazon S3 secara langsung, maka kami sarankan untuk mengonfigurasi interval waktu terpanjang antara penyegaran yang masih praktis untuk kebutuhan

bisnis Anda. Interval penyegaran cache yang lebih lama membantu mengurangi jumlah operasi metadata yang perlu dilakukan gateway saat menjelajahi direktori atau memodifikasi file.

Misalnya: atur penyegaran cache otomatis ke 24 jam, bukan 5 menit, jika itu dapat ditoleransi untuk beban kerja Anda.

- Interval waktu minimum adalah 5 menit. Interval maksimum adalah 30 hari.
- Jika Anda memilih untuk mengatur interval penyegaran cache yang sangat singkat, kami sarankan untuk menguji pengalaman penelusuran direktori untuk server SQL Anda. Waktu yang diperlukan untuk menyegarkan cache gateway dapat meningkat secara substansional tergantung pada jumlah file dan subdirektori di bucket Amazon S3 Anda.

Terapkan beberapa gateway untuk mendukung beban kerja

Storage Gateway dapat mendukung backup SQL untuk lingkungan besar dengan ratusan database SQL, beberapa SQL Server, dan ratusan terabyte data cadangan dengan membagi beban kerja di beberapa gateway.

Saat merencanakan penyebaran dengan beberapa gateway dan server SQL, pertimbangkan hal berikut:

- Sebuah gateway tunggal biasanya dapat mengunggah hingga 20 TB per hari, dengan sumber daya perangkat keras dan bandwidth yang memadai. Anda dapat meningkatkan batas ini hingga 40 TB per hari dengan meningkatkan jumlah utas pengunggah Amazon S3.
- Sebaiknya lakukan proof-of-concept pengujian untuk mengukur kinerja dan memperhitungkan semua variabel dalam penerapan Anda. Setelah Anda menentukan throughput puncak beban kerja cadangan SQL Anda, Anda dapat menskalakan jumlah gateway untuk memenuhi kebutuhan Anda.
- Kami merekomendasikan merancang solusi Anda dengan mempertimbangkan pertumbuhan, karena jumlah database dan ukuran database dapat meningkat seiring waktu. Untuk terus meningkatkan skala dan mendukung peningkatan beban kerja, Anda dapat menerapkan gateway tambahan sesuai kebutuhan.

Sumber daya tambahan untuk beban kerja pencadangan basis data

- Simpan cadangan SQL Server di Amazon S3 menggunakan AWS Storage Gateway
- Simpan backup SQL Server Anda dengan mudah di Amazon S3 menggunakan File Gateway
- Menggunakan AWS Storage Gateway untuk menyimpan cadangan database Oracle di Amazon S3

- Mencadangkan database Oracle ke Amazon S3 dalam skala besar
- Integrasikan database SAP ASE ke Amazon S3 menggunakan AWS Storage Gateway
- Bagaimana satu AWS Pahlawan menggunakan AWS Storage Gateway untuk pencadangan di cloud
- Praktik terbaik ukuran cache S3 File Gateway

Keamanan di AWS Storage Gateway

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-partyauditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program Kepatuhan Program AWS Kepatuhan Program AWS . 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.

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. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data AWS . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

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 AWS sumber daya. 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 SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data menggunakan AWS KMS

Storage Gateway menggunakan SSL/TLS (Secure Socket Layers/Transport Layer Security) untuk mengenkripsi data yang ditransfer antara alat gateway dan AWS penyimpanan Anda. Secara default, Storage Gateway menggunakan kunci S3-Managed enkripsi Amazon (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 AWS Key Management Service kunci (). SSE-KMS

Mengenkripsi berbagi file

Anda dapat mengonfigurasi pembagian file di S3 File Gateway Anda untuk mengenkripsi objek yang disimpan dengan kunci yang AWS KMS dikelola dengan menggunakan atau. SSE-KMS DSSE-KMS Untuk informasi tentang metode enkripsi berbagi file yang didukung, lihat Mengenkripsi objek yang disimpan oleh File Gateway di Amazon S3.

Saat menggunakan AWS KMS untuk mengenkripsi data Anda, ingatlah hal berikut:

- Data Anda dienkripsi saat istirahat di cloud.
- 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.

> **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 .

Untuk informasi lebih lanjut tentang AWS KMS, lihat Apa itu AWS Key Management Service?

Identitas dan manajemen akses untuk AWS Storage Gateway

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya SGW. AWS IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan

- Bagaimana AWS Storage Gateway bekerja dengan IAM
- Identity-based contoh kebijakan untuk AWS Storage Gateway
- Pemecahan masalah AWS Identitas dan akses Storage Gateway
- Menggunakan tag untuk mengontrol akses ke gateway dan sumber daya Anda
- Menggunakan Windows ACL untuk membatasi akses berbagi file SMB

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Pemecahan masalah AWS Identitas dan akses Storage Gateway)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana AWS Storage Gateway bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Identity-based contoh kebijakan untuk AWS Storage Gateway)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensyal dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensyal. Google/ Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami

sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensyal dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensyal sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk 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. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. 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 AWS Storage Gateway

Fitur IAM	AWS Dukungan SGW
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak

Fitur IAM	AWS Dukungan SGW
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Service-linked peran	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.

Identity-based kebijakan untuk AWS SGW

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. 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. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk AWS SGW

Untuk melihat contoh kebijakan berbasis identitas AWS SGW, lihat. Identity-based contoh kebijakan untuk AWS Storage Gateway

Resource-based kebijakan dalam AWS SGW

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan 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 principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal 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 principal dalam kebijakan berbasis sumber daya. 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. 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. Identity-based contoh kebijakan untuk AWS 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. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar tipe resource AWS SGW dan ARNnya, lihat Resources Defined by AWS Storage Gateway di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh AWS Storage Gateway.

Untuk melihat contoh kebijakan berbasis identitas AWS SGW, lihat. Identity-based contoh kebijakan untuk AWS 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, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. 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. 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. Identity-based contoh kebijakan untuk AWS Storage Gateway

ACL di AWS SGW

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan AWS SGW

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

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 kredensyal sementara dengan AWS SGW

Mendukung kredensial sementara: Ya

Kredensyal sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensyal sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Teruskan sesi akses untuk AWS SGW

Mendukung sesi akses terusan (FAS): Ya

Sesi akses teruskan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

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.

Service-linked peran untuk AWS SGW

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran 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. Temukan layanan dalam tabel yang `Yes` menyertakan kolom Service-linked peran. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Identity-based contoh kebijakan untuk AWS Storage Gateway

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya AWS SGW. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

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 ARN untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk AWS Storage Gateway di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan AWS Konsol SGW
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Identity-based kebijakan 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 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 AWS Konsol 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": "*"
        }
    ]
}
```

Pemecahan masalah AWS Identitas dan akses Storage Gateway

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS SGW dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS SGW
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses saya AWS Sumber daya SGW

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.

> **Important**
>
> Storage Gateway dapat mengasumsikan peran layanan yang ada yang diteruskan menggunakan tindakan `iam:PassRole` kebijakan, tetapi tidak mendukung kebijakan IAM yang menggunakan kunci `iam:PassedToService` konteks untuk membatasi tindakan ke layanan tertentu.
> Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna AWS Identity and Access Management :
>
> - IAM: Lulus peran IAM ke layanan tertentu AWS
> - Memberikan izin pengguna untuk meneruskan peran ke layanan AWS
> - Kunci yang tersedia untuk IAM

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses saya AWS Sumber daya SGW

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 (ACL), 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.

Menggunakan tag untuk mengontrol akses ke gateway dan sumber daya Anda

Untuk mengontrol akses ke sumber daya dan tindakan gateway, Anda dapat menggunakan kebijakan AWS Identity and Access Management (IAM) berdasarkan tag. Anda dapat memberikan kontrol dengan dua cara:

1. Kontrol akses ke sumber daya gateway berdasarkan tag pada sumber daya tersebut.
2. Kontrol tag apa yang dapat diteruskan dalam kondisi permintaan IAM.

Untuk informasi tentang cara menggunakan tag untuk mengontrol akses, lihat Mengontrol Akses Menggunakan Tag.

Mengontrol Akses Berdasarkan Tag pada Sumber Daya

Untuk mengontrol tindakan apa yang dapat dilakukan pengguna atau peran pada sumber daya gateway, Anda dapat menggunakan tag pada sumber daya gateway. Misalnya, Anda mungkin ingin mengizinkan atau menolak operasi API tertentu pada sumber daya gateway file berdasarkan pasangan nilai kunci tag pada sumber daya.

Contoh berikut memungkinkan pengguna atau peran untuk melakukan`ListTagsForResource`,`ListFileShares`, dan `DescribeNFSFileShares` tindakan pada semua sumber daya. Kebijakan hanya berlaku jika tag pada sumber daya memiliki kunci yang disetel ke `allowListAndDescribe` dan nilai disetel ke`yes`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
}
```

Mengontrol Akses Berdasarkan Tag dalam Permintaan IAM

Untuk mengontrol apa yang dapat dilakukan pengguna pada sumber daya gateway, Anda dapat menggunakan kondisi dalam kebijakan IAM berdasarkan tag. Misalnya, Anda dapat menulis kebijakan yang memungkinkan atau menyangkal kemampuan pengguna untuk melakukan operasi API tertentu berdasarkan tag yang mereka berikan saat mereka membuat sumber daya.

Dalam contoh berikut, pernyataan pertama memungkinkan pengguna untuk membuat gateway hanya jika pasangan kunci-nilai dari tag yang mereka berikan saat membuat gateway adalah **`Department`** dan. **`Finance`** Saat menggunakan operasi API, Anda menambahkan tag ini ke permintaan aktivasi.

Pernyataan kedua memungkinkan pengguna untuk membuat file Network File System (NFS) atau Server Message Block (SMB) berbagi file pada gateway hanya jika pasangan kunci-nilai tag pada gateway cocok dan. **`Department`** **`Finance`** Selain itu, pengguna harus menambahkan tag ke berbagi file, dan pasangan nilai kunci tag harus **`Department`** dan. **`Finance`** Anda menambahkan tag ke berbagi file saat membuat berbagi file. Tidak ada izin untuk `RemoveTagsFromResource` operasi `AddTagsToResource` atau, sehingga pengguna tidak dapat melakukan operasi ini di gateway atau berbagi file.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
```

```
            ],
            "Resource":"*",
            "Condition":{
               "StringEquals":{
                  "aws:ResourceTag/Department":"Finance",
                  "aws:RequestTag/Department":"Finance"
               }
            }
         }
      ]
}
```

Menggunakan Windows ACL untuk membatasi akses berbagi file SMB

Gateway file Amazon S3 mendukung dua metode berbeda untuk mengontrol akses ke file dan direktori yang disimpan melalui berbagi file SMB: izin POSIX, atau Windows ACL.

Bagian ini menjelaskan cara menggunakan daftar kontrol akses Microsoft Windows (ACL) pada berbagi file SMB yang menggunakan Microsoft Active Directory (AD) untuk otentikasi. Dengan menggunakan Windows ACL, Anda dapat mengatur izin halus pada file dan folder di berbagi file SMB Anda.

Berikut ini adalah beberapa karakteristik penting dari Windows ACL pada berbagi file SMB:

- Windows ACL dipilih secara default untuk berbagi file SMB saat gateway file Anda digabungkan ke domain Active Directory.
- Saat ACL diaktifkan, informasi ACL disimpan di metadata objek Amazon S3.
- Gateway mempertahankan hingga 10 ACL per file atau folder.
- Saat Anda menggunakan berbagi file SMB dengan ACL yang diaktifkan untuk mengakses objek S3 yang dibuat di luar gateway Anda, objek mewarisi informasi ACL dari folder induk.

> **Note**
>
> Akar ACL default untuk berbagi file SMB memberikan akses penuh ke semua orang, tetapi Anda dapat mengubah izin ACL root. Anda dapat menggunakan ACL root untuk mengontrol akses ke berbagi file. Anda dapat mengatur siapa yang dapat memasang berbagi file (memetakan drive) dan izin apa yang didapat pengguna ke file dan folder secara rekursif

dalam berbagi file. Namun, kami menyarankan agar Anda menetapkan izin ini di folder tingkat atas di bucket S3 sehingga ACL Anda tetap ada.

Anda dapat mengaktifkan Windows ACL saat membuat berbagi file SMB baru dengan menggunakan operasi CreateSMBFileShareAPI. Atau Anda dapat mengaktifkan Windows ACL pada berbagi file SMB yang ada dengan menggunakan operasi UpdateSMBFileShareAPI.

Mengaktifkan Windows ACL pada Berbagi File SMB Baru

Ambil langkah-langkah berikut untuk mengaktifkan Windows ACL pada berbagi file SMB baru.

Untuk mengaktifkan Windows ACL saat membuat berbagi file SMB baru

1. Buat gateway file jika Anda belum memilikinya. Untuk informasi selengkapnya, lihat Membuat gateway Anda.
2. Jika gateway tidak bergabung ke domain, tambahkan ke domain. Untuk informasi selengkapnya, lihat Menggunakan Active Directory untuk mengautentikasi pengguna.
3. Buat berbagi file SMB. Untuk informasi selengkapnya, silakan lihat
4. Aktifkan Windows ACL pada file share dari konsol Storage Gateway.

   Untuk menggunakan Storage Gateway Console, lakukan hal berikut:

   a. Pilih berbagi file dan pilih Edit berbagi file.

   b. Untuk File/directory akses yang dikendalikan oleh opsi, pilih Daftar Kontrol Akses Windows.
5. (Opsional) Tambahkan pengguna admin ke AdminUsersList, jika Anda ingin pengguna admin memiliki hak istimewa untuk memperbarui ACL pada semua file dan folder dalam berbagi file.

> **Note**
>
> Jika Anda telah mengonfigurasi daftar Pengguna dan Grup yang Diizinkan dan Ditolak di setelan berbagi file SMB, ACL tidak akan memberikan akses apa pun yang menggantikan daftar tersebut.
> Daftar Pengguna dan Grup yang Diizinkan dan Ditolak dievaluasi sebelum ACL, dan mengontrol pengguna mana yang dapat memasang atau mengakses berbagi file. Jika ada pengguna atau grup yang ditempatkan pada daftar Diizinkan, daftar dianggap aktif, dan hanya pengguna tersebut yang dapat memasang berbagi file.

Setelah pengguna memasang file share, ACL kemudian memberikan perlindungan yang lebih terperinci yang mengontrol file atau folder tertentu yang dapat diakses pengguna.

6. Perbarui ACL untuk folder induk di bawah folder root. Untuk melakukan ini, gunakan Windows File Explorer untuk mengkonfigurasi ACL pada folder di berbagi file SMB.

   > **Note**
   >
   > Jika Anda mengonfigurasi ACL di root alih-alih folder induk di bawah root, izin ACL tidak akan tetap ada di Amazon S3.

   Sebaiknya atur ACL di folder tingkat atas di bawah root berbagi file Anda, alih-alih mengatur ACL langsung di root berbagi file. Pendekatan ini mempertahankan informasi sebagai metadata objek di Amazon S3.

7. Nyalakan warisan yang sesuai.

   > **Note**
   >
   > Anda dapat mengaktifkan warisan untuk berbagi file yang dibuat setelah 8 Mei 2019.

Jika Anda mengaktifkan pewarisan dan memperbarui izin secara rekursif, Storage Gateway memperbarui semua objek di bucket S3. Bergantung pada jumlah objek dalam ember, pembaruan dapat memakan waktu beberapa saat untuk diselesaikan.

Mengaktifkan Windows ACL pada Berbagi File SMB yang Ada

Ambil langkah-langkah berikut untuk mengaktifkan Windows ACL pada berbagi file SMB yang ada yang memiliki izin POSIX.

Untuk mengaktifkan Windows ACL pada berbagi file SMB yang ada menggunakan Storage Gateway Console

1. Pilih berbagi file dan pilih Edit berbagi file.
2. Untuk File/directory akses yang dikendalikan oleh opsi, pilih Daftar Kontrol Akses Windows.
3. Nyalakan warisan yang sesuai.

> **Note**
>
> Kami tidak menyarankan pengaturan ACL di tingkat root, karena jika Anda melakukan ini dan menghapus gateway Anda, Anda perlu mengatur ulang ACL lagi.

Jika Anda mengaktifkan pewarisan dan memperbarui izin secara rekursif, Storage Gateway memperbarui semua objek di bucket S3. Bergantung pada jumlah objek dalam ember, pembaruan dapat memakan waktu beberapa saat untuk diselesaikan.

Keterbatasan Saat Menggunakan Windows ACL

Ingatlah batasan berikut saat menggunakan Windows ACL untuk mengontrol akses ke berbagi file SMB:

- Windows ACL hanya didukung pada berbagi file yang menggunakan Active Directory untuk otentikasi ketika Anda menggunakan klien Windows SMB untuk mengakses berbagi file.
- Gateway file mendukung maksimal 10 entri ACL untuk setiap file dan direktori.
- Gateway file tidak mendukung `Audit` dan `Alarm` entri, yang merupakan entri daftar kontrol akses sistem (SACL). Dukungan `Allow` dan entri gateway file, yang merupakan `Deny` entri daftar kontrol akses diskresioner (DACL).
- Gateway file tidak mendukung izin Entri Kontrol Akses Lanjutan (ACE).
- Pengaturan ACL root dari berbagi file SMB hanya ada di gateway, dan pengaturan tetap ada di seluruh pembaruan gateway dan restart.

> **Note**
>
> Jika Anda mengonfigurasi ACL di root alih-alih folder induk di bawah root, izin ACL tidak akan tetap ada di Amazon S3.

Dengan kondisi ini, pastikan untuk melakukan hal berikut:

- Jika Anda mengonfigurasi beberapa gateway untuk mengakses bucket Amazon S3 yang sama, konfigurasikan ACL root di setiap gateway agar izin tetap konsisten.
- Jika Anda menghapus file share dan membuatnya kembali di bucket Amazon S3 yang sama, pastikan Anda menggunakan set ACL root yang sama.

Validasi kepatuhan untuk AWS Storage Gateway

Third-party Auditor menilai keamanan dan kepatuhan AWS Storage Gateway sebagai bagian dari beberapa program AWS kepatuhan. Ini termasuk SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5,, ENS High, OSPAR, dan HITRUST CSF. K-ISMS

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan . Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Storage Gateway ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan Panduan Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- Arsitektur untuk HIPAA Security and Compliance Whitepaper — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi. AWS HIPAA-compliant
- 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 CSPM— 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 AWS Storage Gateway

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 AZ yang terisolasi dan terpisah secara fisik 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 redundan, ultra-low-latency. Jika penerapan Anda memerlukan fokus pada ketersediaan tinggi, Anda dapat mengonfigurasi layanan dan sumber daya ke beberapa AZ untuk mencapai toleransi kesalahan yang lebih besar.

Wilayah AWS memenuhi tingkat keamanan infrastruktur, kepatuhan, dan perlindungan data tertinggi. Semua lalu lintas antara AZ akan dienkripsi. Kinerja jaringan cukup untuk mencapai replikasi sinkron antara AZ. AZ membuat layanan partisi dan sumber daya untuk ketersediaan tinggi menjadi mudah. Jika penyebaran Anda dipartisi di seluruh AZ, sumber daya Anda lebih terisolasi dan terlindungi dari masalah seperti pemadaman listrik, sambaran petir, tornado, gempa bumi, dan banyak lagi. AZ 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 mendukung VMware vSphere High Availability (VMware HA) untuk membantu melindungi beban kerja penyimpanan terhadap kegagalan perangkat keras, hypervisor, atau jaringan. Untuk informasi selengkapnya, lihat .

Keamanan infrastruktur di AWS Storage Gateway

Sebagai layanan terkelola, AWS Storage Gateway dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam Security Pillar - AWS Well-Architected Framework.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Storage Gateway melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.2. Klien juga harus mendukung cipher suite dengan perfect forward secrecy (PFS) seperti Ephemeral (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan principal 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 meninjau, menganalisis, dan memulihkan CVE 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 Mengelola pembaruan gateway menggunakan AWS Storage Gateway konsol .

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.

Penebangan dan pemantauan 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 AWS akun 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 acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun 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
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua tindakan Storage Gateway dicatat dan didokumentasikan dalam topik Tindakan. Misalnya, panggilan ke`ActivateGateway`,`ListGateways`, dan `ShutdownGateway` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan itu dibuat dengan kredensyal 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"
              }]
}
```

Memecahkan masalah dengan penerapan Storage Gateway

Berikut ini, Anda dapat menemukan informasi tentang praktik terbaik dan masalah pemecahan masalah yang terkait dengan gateway, platform host, berbagi file, ketersediaan tinggi, pemulihan data, dan keamanan. 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: Masalah Direktori Aktif- Pelajari apa yang harus dilakukan jika Anda menerima pesan galat seperti`NETWORK_ERROR`,`TIMEOUT`, atau `ACCESS_DENIED` ketika mencoba untuk bergabung dengan File Gateway Anda ke domain Microsoft Active Directory.
- Pemecahan masalah: masalah aktivasi gateway- Pelajari apa yang harus dilakukan jika Anda menerima pesan galat internal saat mencoba mengaktifkan Storage Gateway Anda.
- Pemecahan masalah: 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.
- Pemecahan masalah: Masalah penyiapan Microsoft Hyper-V- Pelajari tentang masalah umum yang mungkin Anda temui saat menerapkan Storage Gateway di platform Microsoft Hyper-V.
- Pemecahan masalah: Masalah gateway Amazon EC2- Temukan informasi tentang masalah umum yang mungkin Anda temui saat bekerja dengan gateway yang digunakan di Amazon EC2.
- Pemecahan masalah: masalah alat perangkat keras- Pelajari cara mengatasi masalah yang mungkin Anda temui dengan AWS Storage Gateway Hardware Appliance.
- Pemecahan masalah: Masalah File Gateway- Temukan informasi yang dapat membantu Anda memahami penyebab kesalahan dan pemberitahuan kesehatan yang muncul di CloudWatch log File Gateway Anda.
- Pemecahan masalah: masalah berbagi file- Pelajari tentang tindakan yang dapat Anda lakukan jika Anda mengalami masalah tak terduga dengan berbagi file Anda.
- Pemecahan masalah: masalah ketersediaan tinggi- Pelajari apa yang harus dilakukan jika Anda mengalami masalah dengan gateway yang digunakan di lingkungan HA. VMware

Pemecahan masalah: gateway offline di konsol Storage Gateway

Gunakan informasi pemecahan masalah berikut untuk menentukan apa yang harus dilakukan jika AWS Storage Gateway konsol menunjukkan bahwa gateway Anda sedang offline.

Gateway Anda mungkin ditampilkan sebagai offline karena satu atau beberapa alasan berikut:

- Gateway tidak dapat mencapai titik akhir layanan Storage Gateway.
- Pintu gerbang ditutup secara tak terduga.
- Disk cache yang terkait dengan gateway telah terputus atau dimodifikasi, atau gagal.

Untuk mengembalikan gateway Anda secara online, identifikasi dan selesaikan masalah yang menyebabkan gateway Anda offline.

Periksa firewall atau proxy terkait

Jika Anda mengonfigurasi gateway Anda untuk menggunakan proxy, atau Anda menempatkan gateway Anda di belakang firewall, maka tinjau aturan akses proxy atau firewall. Proxy atau firewall harus mengizinkan lalu lintas ke dan dari port jaringan dan titik akhir layanan yang diperlukan oleh Storage Gateway. Untuk informasi selengkapnya, lihat Persyaratan jaringan dan firewall Persyaratan .

Periksa SSL atau inspeksi paket mendalam yang sedang berlangsung dari lalu lintas gateway Anda

Jika inspeksi SSL atau deep-packet saat ini sedang dilakukan pada lalu lintas jaringan antara gateway Anda dan AWS, maka gateway Anda mungkin tidak dapat berkomunikasi dengan titik akhir layanan yang diperlukan. Untuk membawa gateway Anda kembali online, Anda harus menonaktifkan inspeksi.

Periksa metrik IOWait Persen setelah reboot atau pembaruan perangkat lunak

Setelah reboot atau pembaruan perangkat lunak, periksa untuk melihat apakah `IOWaitPercent` metrik untuk File Gateway Anda adalah 10 atau lebih besar. Ini mungkin menyebabkan gateway Anda lambat merespons saat membangun kembali cache indeks ke RAM. Untuk informasi

selengkapnya, lihat Pemecahan Masalah: Menggunakan CloudWatch metrik : Menggunakan metrik. CloudWatch

Periksa pemadaman listrik atau kegagalan perangkat keras pada host hypervisor

Pemadaman listrik atau kegagalan perangkat keras pada host hypervisor gateway Anda dapat menyebabkan gateway Anda mati secara tak terduga dan menjadi tidak terjangkau. Setelah Anda memulihkan daya dan konektivitas jaringan, gateway Anda akan dapat dijangkau lagi.

Setelah gateway Anda kembali online, pastikan untuk mengambil langkah-langkah untuk memulihkan data Anda. Untuk informasi selengkapnya, lihat Praktik terbaik: memulihkan data Anda .

Periksa masalah dengan disk cache terkait

Gateway Anda dapat offline jika setidaknya salah satu disk cache yang terkait dengan gateway Anda telah dihapus, diubah, atau diubah ukurannya, atau jika rusak.

Jika disk cache yang berfungsi dihapus dari host hypervisor:

1. Matikan pintu gerbangnya.
2. Tambahkan kembali disk.

> **Note**
>
> Pastikan Anda menambahkan disk ke node disk yang sama.

3. Mulai ulang gateway.

Jika disk cache rusak, diganti, atau diubah ukurannya:

- Ikuti prosedur Metode 2 yang dijelaskan dalam Mengganti Gateway File S3 yang ada dengan instance baru untuk menyiapkan gateway baru dan mengunduh ulang informasi disk cache dari cloud. AWS

Pemecahan masalah: masalah bergabung dengan gateway ke Active Directory

Gunakan informasi pemecahan masalah berikut untuk menentukan apa yang harus dilakukan jika Anda menerima pesan galat seperti `NETWORK_ERRORTIMEOUT`, atau `ACCESS_DENIED` saat mencoba menggabungkan Gateway File Anda ke domain Microsoft Active Directory.

Untuk mengatasi kesalahan ini, lakukan pemeriksaan dan konfigurasi berikut.

Konfirmasikan bahwa gateway dapat mencapai pengontrol domain dengan menjalankan tes nping

Untuk menjalankan tes nping:

1. Connect ke konsol lokal gateway menggunakan perangkat lunak manajemen hypervisor (VMware, Hyper-V, atau KVM) untuk gateway lokal, atau menggunakan ssh untuk gateway Amazon EC2.
2. Masukkan angka yang sesuai untuk memilih Gateway Console, lalu masukkan h untuk mencantumkan semua perintah yang tersedia. Untuk menguji konektivitas antara mesin virtual Storage Gateway dan domain, jalankan perintah berikut:

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > Ganti `corp.domain.com` dengan nama DNS domain Active Directory Anda dan ganti `389` dengan port LDAP untuk lingkungan Anda.
   > Verifikasi bahwa Anda telah membuka port yang diperlukan dalam firewall Anda.

Berikut ini adalah contoh tes nping yang berhasil di mana gateway dapat mencapai pengontrol domain:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
```

```
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>

Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

Berikut ini adalah contoh tes nping di mana tidak ada konektivitas atau respons dari `corp.domain.com` tujuan:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Periksa opsi DHCP yang ditetapkan untuk VPC instans gateway Amazon EC2 Anda

Jika File Gateway berjalan pada instans Amazon EC2, maka Anda harus memastikan set opsi DHCP dikonfigurasi dengan benar dan dilampirkan ke Amazon Virtual Private Cloud (VPC) yang berisi instance gateway. Untuk informasi selengkapnya, lihat set opsi DHCP di Amazon VPC.

Konfirmasikan bahwa gateway dapat menyelesaikan domain dengan menjalankan kueri penggalian

Jika domain tidak dapat diselesaikan oleh gateway, maka gateway tidak dapat bergabung dengan domain.

Untuk menjalankan kueri penggalian:

1. Connect ke konsol lokal gateway menggunakan perangkat lunak manajemen hypervisor (VMware, Hyper-V, atau KVM) untuk gateway lokal, atau menggunakan ssh untuk gateway Amazon EC2.

2. Masukkan angka yang sesuai untuk memilih Gateway Console, lalu masukkan h untuk mencantumkan semua perintah yang tersedia. Untuk menguji apakah gateway dapat menyelesaikan domain, jalankan perintah berikut:

   ```
   dig -d corp.domain.com
   ```

   > **Note**
   >
   > Ganti `corp.domain.com` dengan nama DNS domain Active Directory Anda.

Berikut ini adalah contoh respons yang berhasil:

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

Periksa pengaturan dan peran pengontrol domain

Verifikasi bahwa pengontrol domain tidak disetel ke hanya-baca, dan bahwa pengontrol domain memiliki peran yang cukup bagi komputer untuk bergabung. Untuk menguji ini, coba gabungkan server lain dari subnet VPC yang sama dengan VM gateway ke domain.

Periksa apakah gateway bergabung dengan pengontrol domain terdekat

Sebagai praktik terbaik, kami sarankan untuk bergabung dengan gateway Anda ke pengontrol domain yang secara geografis dekat dengan alat gateway. Jika alat gateway tidak dapat berkomunikasi dengan pengontrol domain dalam waktu 20 detik karena latensi jaringan, maka proses penggabungan domain dapat habis. Misalnya, proses mungkin habis jika alat gateway berada di AS Timur (Virginia N.) Wilayah AWS dan pengontrol domain berada di Asia Pasifik (Singapura). Wilayah AWS

> **Note**
>
> Untuk meningkatkan nilai batas waktu default 20 detik, Anda dapat menjalankan perintah join-domain di AWS Command Line Interface (AWS CLI) dan menyertakan `--timeout-in-seconds` opsi untuk menambah waktu. Anda juga dapat menggunakan panggilan JoinDomain API dan menyertakan `TimeoutInSeconds` parameter untuk menambah waktu. Nilai batas waktu maksimum adalah 3.600 detik.
> Jika Anda menerima kesalahan saat menjalankan AWS CLI perintah, pastikan Anda menggunakan AWS CLI versi terbaru.

Konfirmasikan bahwa Active Directory membuat objek komputer baru di unit organisasi default (OU)

Pastikan Microsoft Active Directory tidak memiliki Objek Kebijakan Grup yang membuat objek komputer baru di lokasi apa pun selain OU default. Sebelum Anda dapat bergabung dengan gateway Anda ke domain Active Directory, objek komputer baru harus ada di OU default. Beberapa lingkungan Active Directory disesuaikan agar berbeda OUs untuk objek yang baru dibuat. Untuk menjamin bahwa objek komputer baru untuk VM gateway ada di OU default, coba buat objek komputer secara manual pada pengontrol domain Anda sebelum Anda bergabung dengan gateway ke domain. Anda juga dapat menjalankan perintah join-domain menggunakan file. AWS CLI Kemudian, tentukan opsi untuk`--organizational-unit`.

> **Note**
>
> Proses pembuatan objek komputer disebut pra-pementasan.

Periksa log peristiwa pengontrol domain Anda

Jika Anda tidak dapat bergabung dengan gateway ke domain setelah mencoba semua pemeriksaan dan konfigurasi lain yang dijelaskan di bagian sebelumnya, sebaiknya periksa log peristiwa pengontrol domain Anda. Periksa kesalahan apa pun di penampil acara pengontrol domain. Verifikasi bahwa kueri gateway telah mencapai pengontrol domain.

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 instans Amazon EC2, periksa apakah port terbuka di grup keamanan instans. Untuk mengonfirmasi bahwa port terbuka, jalankan perintah telnet pada titik akhir publik dari server. Server ini harus berada di subnet yang sama dengan gateway. Misalnya, perintah telnet berikut menguji koneksi ke port 443:

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

Untuk mengonfirmasi bahwa gateway itu sendiri dapat mencapai titik akhir, akses konsol VM lokal gateway (untuk gateway yang digunakan di lokasi). Atau, Anda dapat SSH ke instance gateway (untuk gateway yang digunakan di Amazon EC2). Kemudian, jalankan tes konektivitas jaringan. Konfirmasikan bahwa tes kembali`[PASSED]`. Untuk informasi selengkapnya, lihat Menguji konektivitas jaringan gateway Anda Menguji konektivitas .

> **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.

Opsi Manajemen Waktu Sistem tidak tersedia di gateway yang di-host di instans Amazon EC2. Untuk memastikan gateway Amazon EC2 dapat menyinkronkan waktu dengan benar, konfirmasikan bahwa instans Amazon EC2 dapat terhubung ke daftar kumpulan server NTP berikut melalui port UDP dan TCP 123:

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Mengatasi kesalahan saat mengaktifkan gateway menggunakan endpoint Amazon VPC

Untuk mengatasi kesalahan aktivasi saat mengaktifkan gateway menggunakan titik akhir Amazon Virtual Private Cloud (Amazon VPC), lakukan pemeriksaan dan konfigurasi berikut.

Periksa port yang diperlukan

Pastikan port yang diperlukan dalam firewall lokal Anda (untuk gateway yang digunakan di lokasi) atau grup keamanan (untuk gateway yang digunakan di Amazon EC2) terbuka. Port yang diperlukan untuk menghubungkan gateway ke titik akhir VPC Storage Gateway berbeda dari yang diperlukan saat menghubungkan gateway ke titik akhir publik. Port berikut diperlukan untuk menghubungkan ke titik akhir VPC Storage Gateway:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Selain itu, periksa grup keamanan yang dilampirkan ke titik akhir VPC Storage Gateway Anda. Grup keamanan default yang dilampirkan ke titik akhir mungkin tidak mengizinkan port yang diperlukan. Buat grup keamanan baru yang memungkinkan lalu lintas dari rentang alamat IP gateway Anda melalui port yang diperlukan. Kemudian, lampirkan grup keamanan itu ke titik akhir VPC.

> **Note**
>
> Gunakan konsol VPC Amazon untuk memverifikasi grup keamanan yang dilampirkan ke titik akhir VPC. Lihat titik akhir VPC Storage Gateway Anda dari konsol, lalu pilih tab Grup Keamanan.

Untuk mengonfirmasi bahwa port yang diperlukan terbuka, Anda dapat menjalankan perintah telnet pada Storage Gateway VPC Endpoint. Anda harus menjalankan perintah ini dari server yang berada di subnet yang sama dengan gateway. Anda dapat menjalankan pengujian pada nama DNS pertama yang tidak menentukan Availability Zone. Misalnya, perintah telnet berikut menguji koneksi port yang diperlukan menggunakan nama DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
```

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Pastikan keamanan firewall tidak mengubah paket yang dikirim dari gateway ke titik akhir Storage Gateway Amazon VPC

Inspeksi SSL, inspeksi paket mendalam, atau bentuk keamanan firewall lainnya dapat mengganggu paket yang dikirim dari gateway. Jabat tangan SSL gagal jika sertifikat SSL dimodifikasi dari apa yang diharapkan titik akhir aktivasi. Untuk mengonfirmasi bahwa tidak ada pemeriksaan SSL yang sedang berlangsung, jalankan perintah OpenSSL di titik akhir VPC Storage Gateway Anda. Anda harus menjalankan perintah ini dari mesin yang berada di subnet yang sama dengan gateway. Jalankan perintah untuk setiap port yang diperlukan:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Jika tidak ada inspeksi SSL yang sedang berlangsung, maka perintah mengembalikan respons yang mirip dengan berikut ini:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, 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.

Opsi Manajemen Waktu Sistem tidak tersedia di gateway yang di-host di instans Amazon EC2. Untuk memastikan gateway Amazon EC2 dapat menyinkronkan waktu dengan benar, konfirmasikan bahwa instans Amazon EC2 dapat terhubung ke daftar kumpulan server NTP berikut melalui port UDP dan TCP 123:

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

Periksa proxy HTTP dan konfirmasikan pengaturan grup keamanan terkait

Sebelum aktivasi, periksa apakah Anda memiliki proxy HTTP di Amazon EC2 yang dikonfigurasi di VM gateway lokal sebagai proxy Squid di port 3128. Dalam hal ini, 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 VPC Amazon EC2 harus memiliki aturan masuk. Aturan masuk ini harus mengizinkan lalu lintas pada port 1026-1028, 1031, 2222, dan 443 dari alamat IP proxy HTTP di Amazon EC2.

Mengatasi kesalahan saat mengaktifkan gateway Anda menggunakan titik akhir publik dan ada titik akhir VPC Storage Gateway di VPC yang sama

Untuk mengatasi kesalahan saat mengaktifkan gateway menggunakan titik akhir publik saat ada 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.

Pemecahan masalah: masalah gateway lokal

Anda dapat menemukan informasi berikut tentang masalah umum yang mungkin Anda temui saat bekerja dengan gateway lokal, dan cara mengizinkan untuk terhubung Dukungan ke gateway untuk membantu pemecahan masalah.

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.

Isu	Tindakan yang Harus Dilakukan
	• 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. • 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.

Isu	Tindakan yang Harus Dilakukan
Aktivasi gateway Anda gagal ketika Anda mengklik tombol Lanjutkan ke Aktivasi di Storage Gateway Management Console.	• Periksa apakah VM gateway dapat diakses dengan melakukan ping VM dari klien Anda. • Periksa apakah VM Anda memiliki konektivitas jaringan ke internet. Jika tidak, Anda harus mengonfigurasi proxy SOCKS. Untuk informasi selengkapnya tentang cara melakukannya, lihat Menguji konektivitas jaringan gateway 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. Mengkonfigurasi server Network Time Protocol (NTP) untuk gateway Anda • Setelah melakukan langkah-langkah ini, Anda dapat mencoba kembali penerapan gateway menggunakan konsol Storage Gateway dan wizard Setup and Activate Gateway. • Periksa apakah VM Anda memiliki setidaknya 16 GB RAM. Alokasi gateway gagal jika ada kurang dari 16 GB RAM. Untuk informasi selengkapnya, lihat Persyaratan pengaturan File Gateway.
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 menghindari pertengkaran bandwidth, terutama selama pemulihan snapshot. Untuk kebutuhan beban kerja throughput tinggi, Anda dapat menggunakannya 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, lihatKinerja dan optimasi. 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 konektivitas jaringan gateway Anda.
	• Periksa konfigurasi adaptor jaringan gateway Anda di klien manajemen hypervisor Anda dan pastikan bahwa semua antarmuka yang ingin Anda gunakan untuk gateway diaktifkan.
	• Periksa konfigurasi adaptor jaringan gateway Anda di konsol lokal gateway. Untuk petunjuk, lihat Mengonfigurasi pengaturan 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 ke AWS, lihatKinerja dan optimasi.

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

Pemecahan masalah: Pemindaian keamanan menunjukkan port NFS terbuka

Port NFS tertentu diaktifkan secara default, bahkan pada gateway yang hanya Anda gunakan dengan berbagi file SMB. Jika Anda menggunakan perangkat lunak keamanan pihak ketiga seperti Qualys untuk memindai jaringan tempat File Gateway Anda digunakan, hasil pemindaian mungkin melaporkan port NFS terbuka ini sebagai potensi kerentanan keamanan. Jika Anda hanya menggunakan gateway Anda dengan berbagi file SMB dan Anda ingin menonaktifkan port NFS yang tidak digunakan untuk alasan keamanan, gunakan prosedur berikut:

Untuk menonaktifkan port NFS pada File Gateway:

1. Akses prompt perintah konsol lokal gateway menggunakan prosedur yang diuraikan dalamMenjalankan perintah Storage Gateway di konsol lokal.
2. Masukkan perintah berikut untuk menonaktifkan lalu lintas NFS:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ```

```
ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. Masukkan perintah berikut untuk mengonfirmasi bahwa port NFS yang diblokir muncul di tabel IP:

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

Mengaktifkan Dukungan akses untuk membantu memecahkan masalah gateway yang dihosting di lokasi

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

- Jika gateway Anda menggunakan titik akhir publik, di jendela AVAILABLE COMMANDS, masukkan **`open-support-channel`** untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.
- Jika gateway Anda menggunakan titik akhir VPC, di jendela AVAILABLE COMMANDS, masukkan. **`open-support-channel`** Jika gateway Anda tidak diaktifkan, berikan titik akhir VPC atau alamat IP untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.

> **Note**
>
> Nomor saluran bukan nomor port Transmission 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 Storage Gateway.
8. Ikuti petunjuk untuk keluar dari konsol lokal.

Pemecahan 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 ini dapat terjadi karena alasan berikut:

Isu	Tindakan yang Harus Dilakukan
“Kesalahan server terjadi saat mencoba mengimpor mesin virtual. Impor gagal. Tidak dapat menemukan file impor mesin virtual di bawah lokasi [...]. Anda dapat mengimpor mesin virtual hanya jika Anda menggunakan Hyper-V untuk membuat dan mengekspornya.	• 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` . Contoh: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • 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-Storage-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 pengaturan File 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 pengaturan File 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 Mengkonfigurasi server Network Time Protocol (NTP) untuk gateway Anda.
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 kredensil 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 solusi, lihat dokumentasi Microsoft, lihat Kinerja jaringan yang buruk pada mesin virtual pada host Windows Server 2012 Hyper-V jika VMQ diaktifkan.

Pemecahan masalah: 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 host Amazon EC2 default untuk S3 File Gateway

Untuk informasi tentang penggunaan penyimpanan sementara, lihat. Menggunakan penyimpanan singkat dengan gateway EC2

Topik

- Aktivasi gateway Anda tidak terjadi setelah beberapa saat
- Anda tidak dapat menemukan instans gateway EC2 di daftar instans
- Anda ingin terhubung ke instans gateway menggunakan konsol serial Amazon EC2
- Anda Dukungan ingin membantu memecahkan masalah gateway Amazon EC2

Aktivasi gateway Anda tidak terjadi setelah beberapa saat

Periksa hal berikut di konsol Amazon EC2:

- Port 80 terbuka di grup keamanan yang Anda kaitkan dengan instans. Untuk informasi selengkapnya tentang menambahkan aturan grup keamanan, lihat Menambahkan aturan grup keamanan di Panduan Pengguna Amazon EC2.
- Instance gateway ditandai sebagai berjalan. Di konsol Amazon EC2, nilai Status untuk instance harus RUNNING.

- Pastikan jenis instans Amazon EC2 Anda memenuhi persyaratan minimum, seperti yang dijelaskan dalam. Persyaratan penyimpanan

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

Anda tidak dapat menemukan instans gateway EC2 di daftar instans

Jika Anda tidak memberikan tag sumber daya pada instans Anda dan memiliki banyak instance yang berjalan, mungkin sulit untuk mengetahui instance mana yang Anda luncurkan. Dalam hal ini, Anda dapat mengambil tindakan berikut untuk menemukan instance gateway:

- Periksa nama Amazon Machine Image (AMI) pada tab Deskripsi instance. Sebuah instance berdasarkan Storage Gateway AMI harus dimulai dengan teks**`aws-storage-gateway-ami`**.
- Jika Anda memiliki beberapa instance berdasarkan Storage Gateway AMI, periksa waktu peluncuran instans untuk menemukan instance yang benar.

Anda ingin terhubung ke instans gateway menggunakan konsol serial Amazon EC2

Anda dapat menggunakan konsol serial Amazon EC2 untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya. Untuk petunjuk dan tips pemecahan masalah, lihat Konsol Serial Amazon EC2 di Panduan Pengguna Amazon Elastic Compute Cloud.

Anda Dukungan ingin membantu memecahkan masalah gateway Amazon EC2

Storage Gateway menyediakan konsol lokal yang dapat Anda gunakan untuk melakukan beberapa tugas pemeliharaan, termasuk memungkinkan Dukungan untuk mengakses gateway Anda untuk membantu Anda mengatasi masalah gateway. Secara default, Dukungan akses ke gateway Anda dimatikan. Anda mengaktifkan akses ini melalui konsol lokal Amazon EC2. Anda masuk ke konsol lokal Amazon EC2 melalui Secure Shell (SSH). Untuk berhasil masuk melalui SSH, grup keamanan instans Anda harus memiliki aturan yang membuka port TCP 22.

> **Note**
>
> Jika Anda menambahkan aturan baru ke grup keamanan yang sudah ada, aturan baru berlaku untuk semua instans yang menggunakan grup keamanan tersebut. Untuk informasi selengkapnya tentang grup keamanan dan cara menambahkan aturan grup keamanan, lihat Grup keamanan Amazon EC2 di Panduan Pengguna Amazon EC2.

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

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

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

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

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

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

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

   - Jika gateway Anda menggunakan titik akhir publik, di jendela AVAILABLE COMMANDS, masukkan **`open-support-channel`** untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat

Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.

- Jika gateway Anda menggunakan titik akhir VPC, di jendela AVAILABLE COMMANDS, masukkan. **`open-support-channel`** Jika gateway Anda tidak diaktifkan, berikan titik akhir VPC atau alamat IP untuk terhubung ke dukungan pelanggan untuk Storage Gateway. Izinkan port TCP 22 sehingga Anda dapat membuka saluran dukungan. AWS Saat Anda terhubung ke dukungan pelanggan, Storage Gateway memberi Anda nomor dukungan. Catat nomor dukungan Anda.

> **Note**
>
> Nomor saluran bukan nomor port Transmission 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 Storage Gateway.
8. Ikuti menu konsol untuk keluar dari instance Storage Gateway.

Pemecahan masalah: masalah 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.

Topik berikut membahas masalah yang mungkin Anda temui dengan AWS Storage Gateway Hardware Appliance, dan saran tentang pemecahan masalah ini.

Topik

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 AWS 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 AWS 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 waktu 30 detik jika tidak ada konektivitas jaringan atau masalah firewall. Contoh:

Status: Buka di port 19599

3. Perhatikan nomor port dan berikan ke Dukungan.

Pemecahan masalah: Masalah File Gateway

Anda dapat mengonfigurasi File Gateway Anda untuk menulis entri log ke grup CloudWatch log Amazon. Jika ya, Anda menerima pemberitahuan tentang status kesehatan gateway dan tentang kesalahan apa pun yang ditemui gateway. Anda dapat menemukan informasi tentang kesalahan dan pemberitahuan kesehatan ini di CloudWatch Log.

Di bagian berikut, Anda dapat menemukan informasi yang dapat membantu Anda memahami penyebab setiap kesalahan dan pemberitahuan kesehatan serta cara memperbaiki masalah.

Topik

Kesalahan: 1344 (0x00000540)

Saat memigrasikan file ke Amazon S3, Anda mungkin menemukan `ERROR 1344 (0x00000540)` jika Anda mencoba menyalin file dengan lebih dari 10 Entri Kontrol Akses ACEs () ke Amazon S3. Entri Kontrol Akses tercantum dalam Daftar Kontrol Akses (ACL).

Amazon S3 File Gateway hanya dapat menyimpan 10 entri ACE per file atau folder tertentu.

Untuk mengatasi Kesalahan 1344: Menyalin Keamanan NTFS ke Direktori Tujuan.

Kurangi jumlah entri dalam Izin Windows untuk file atau folder yang berisi lebih dari 10 entri. Pendekatan umum adalah membuat grup yang berisi daftar lengkap entri, kemudian mengganti daftar entri dengan grup tunggal itu. Setelah jumlah entri kurang dari 10, Anda dapat mencoba lagi menyalin file atau folder ke gateway.

Kesalahan: GatewayClockOutOfSync

Anda bisa mendapatkan `GatewayClockOutOfSync` kesalahan ketika gateway mendeteksi perbedaan 5 menit atau lebih antara waktu sistem lokal dan waktu yang dilaporkan oleh server AWS Storage Gateway. Masalah sinkronisasi jam dapat berdampak negatif pada konektivitas antara gateway dan AWS. Jika jam gateway tidak sinkron, kesalahan I/O mungkin terjadi untuk koneksi NFS dan SMB, dan pengguna SMB mungkin mengalami kesalahan otentikasi.

Untuk mengatasi GatewayClockOutOfSync kesalahan

- Periksa konfigurasi jaringan antara gateway dan server NTP. Untuk informasi selengkapnya tentang sinkronisasi waktu VM gateway dan memperbarui konfigurasi server NTP, lihat Mengonfigurasi server Network Time Protocol (NTP) untuk gateway Anda (NTP) untuk gateway Anda.

Kesalahan: InaccessibleStorageClass

Anda bisa mendapatkan `InaccessibleStorageClass` kesalahan ketika objek telah pindah dari kelas penyimpanan Standar Amazon S3.

Gateway File Anda biasanya mengalami kesalahan ini ketika mencoba mengunggah objek ke atau membaca objek dari bucket Amazon S3. Umumnya, kesalahan ini berarti objek telah pindah ke Amazon Glacier dan berada di kelas penyimpanan S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive.

Gateway File S3 Anda dapat menghasilkan laporan cache yang mencantumkan semua file di cache gateway yang saat ini gagal diunggah ke Amazon S3 karena kesalahan ini. Informasi dalam laporan ini dapat membantu Anda mengatasi masalah Dukungan dengan konfigurasi gateway, Amazon S3, atau IAM Anda. Untuk informasi selengkapnya, lihat Membuat laporan cache.

Untuk mengatasi InaccessibleStorageClass kesalahan

- Kembalikan objek dari kelas penyimpanan S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive kembali ke kelas penyimpanan aslinya di S3.

  Jika Anda mengembalikan objek ke bucket S3 untuk memperbaiki kesalahan unggahan, file tersebut akhirnya diunggah. Jika Anda mengembalikan objek untuk memperbaiki kesalahan baca, klien SMB atau NFS File Gateway kemudian dapat membaca file tersebut.

Kesalahan: InvalidObjectState

Anda bisa mendapatkan `InvalidObjectState` kesalahan saat penulis selain Gateway File yang ditentukan memodifikasi file yang ditentukan di bucket Amazon S3 yang ditentukan. Akibatnya, status file untuk File Gateway tidak cocok dengan statusnya di Amazon S3. Setiap unggahan file berikutnya ke Amazon S3 atau pengambilan file dari Amazon S3 gagal.

Gateway File S3 Anda dapat menghasilkan laporan cache yang mencantumkan semua file di cache gateway yang saat ini gagal diunggah ke Amazon S3 karena kesalahan ini. Informasi dalam laporan ini dapat membantu Anda mengatasi masalah Dukungan dengan konfigurasi gateway, Amazon S3, atau IAM Anda. Untuk informasi selengkapnya, lihat Membuat laporan cache.

Untuk mengatasi InvalidObjectState kesalahan

Jika operasi yang memodifikasi file adalah `S3Upload` atau`S3GetObject`, lakukan hal berikut:

1. Simpan salinan file terbaru ke sistem file lokal klien SMB atau NFS Anda (Anda memerlukan salinan file ini pada langkah 4). Jika versi file di Amazon S3 adalah yang terbaru, unduh versi itu. Anda dapat melakukan ini menggunakan Konsol Manajemen AWS atau AWS CLI.
2. Hapus file di Amazon S3 menggunakan atau. Konsol Manajemen AWS AWS CLI
3. Hapus file dari File Gateway menggunakan klien SMB atau NFS Anda.
4. Salin versi terbaru file yang Anda simpan di langkah 1 ke Amazon S3 menggunakan klien SMB atau NFS Anda. Lakukan ini melalui File Gateway Anda.

Kesalahan: ObjectMissing

Anda bisa mendapatkan `ObjectMissing` kesalahan ketika penulis selain Gateway File yang ditentukan menghapus file yang ditentukan dari bucket S3. Setiap unggahan berikutnya ke Amazon S3 atau pengambilan dari Amazon S3 untuk objek gagal.

Gateway File S3 Anda dapat menghasilkan laporan cache yang mencantumkan semua file di cache gateway yang saat ini gagal diunggah ke Amazon S3 karena kesalahan ini. Informasi dalam laporan ini dapat membantu Anda mengatasi masalah Dukungan dengan konfigurasi gateway, Amazon S3, atau IAM Anda. Untuk informasi selengkapnya, lihat Membuat laporan cache.

Untuk mengatasi ObjectMissing kesalahan

Jika operasi yang memodifikasi file adalah `S3Upload` atau`S3GetObject`, lakukan hal berikut:

1. Simpan salinan file terbaru ke sistem file lokal klien SMB atau NFS Anda (Anda memerlukan salinan file ini pada langkah 3).
2. Hapus file dari File Gateway menggunakan klien SMB atau NFS Anda.
3. Salin versi terbaru dari file yang Anda simpan di langkah 1 menggunakan klien SMB atau NFS Anda. Lakukan ini melalui File Gateway Anda.

Kesalahan: RoleTrustRelationshipInvalid

Anda mendapatkan kesalahan ini ketika peran IAM untuk berbagi file memiliki hubungan kepercayaan IAM yang salah dikonfigurasi (yaitu, peran IAM tidak mempercayai nama utama Storage Gateway). `storagegateway.amazonaws.com` Akibatnya, File Gateway tidak akan bisa mendapatkan kredensil untuk menjalankan operasi apa pun pada bucket S3 yang mendukung pembagian file.

Untuk mengatasi RoleTrustRelationshipInvalid kesalahan

- Gunakan konsol IAM atau IAM API untuk disertakan `storagegateway.amazonaws.com` sebagai prinsipal yang dipercaya oleh file share Anda. IAMrole Untuk informasi tentang peran IAM, lihat Tutorial: mendelegasikan akses di seluruh AWS akun menggunakan peran IAM.

Kesalahan: S3 AccessDenied

Anda bisa mendapatkan `S3AccessDenied` kesalahan untuk peran Amazon S3 bucket access AWS Identity and Access Management (IAM) berbagi file. Dalam hal ini, peran IAM akses bucket S3 yang ditentukan oleh `roleArn` dalam kesalahan tidak mengizinkan operasi yang terlibat. Operasi tidak diizinkan karena izin untuk objek dalam direktori yang ditentukan oleh awalan Amazon S3.

Gateway File S3 Anda dapat menghasilkan laporan cache yang mencantumkan semua file di cache gateway yang saat ini gagal diunggah ke Amazon S3 karena kesalahan ini. Informasi dalam laporan

ini dapat membantu Anda mengatasi masalah Dukungan dengan konfigurasi gateway, Amazon S3, atau IAM Anda. Untuk informasi selengkapnya, lihat Membuat laporan cache.

Untuk mengatasi kesalahan S3 AccessDenied

- Ubah kebijakan akses Amazon S3 yang dilampirkan `roleArn` di log kesehatan File Gateway untuk mengizinkan izin operasi Amazon S3. Pastikan bahwa kebijakan akses mengizinkan izin untuk operasi yang menyebabkan kesalahan. Juga, izinkan izin untuk direktori yang ditentukan dalam log untuk`prefix`. Untuk informasi tentang izin Amazon S3, lihat Menentukan izin dalam kebijakan di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

  Operasi ini dapat menyebabkan `S3AccessDenied` kesalahan terjadi:

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

Kesalahan: DroppedNotifications

Anda mungkin melihat `DroppedNotifications` kesalahan alih-alih jenis entri CloudWatch log lain yang diharapkan ketika ruang penyimpanan kosong pada disk root gateway Anda kurang dari 1 GB, atau jika lebih dari 100 pemberitahuan kesehatan dihasilkan dalam interval 1 menit. Dalam keadaan ini, gateway berhenti menghasilkan pemberitahuan CloudWatch log terperinci sebagai tindakan pencegahan.

Untuk mengatasi DroppedNotifications kesalahan

1. Periksa `Root Disk Usage` metrik pada tab Monitoring untuk gateway Anda di konsol Storage Gateway untuk menentukan apakah ruang disk root yang tersedia hampir habis.
2. Tingkatkan ukuran disk penyimpanan root gateway jika ruang yang tersedia kurang dari 1 GB. Lihat dokumentasi hypervisor mesin virtual Anda untuk instruksi.

   Untuk meningkatkan ukuran disk root untuk gateway Amazon EC2, lihat Meminta modifikasi pada volume EBS Anda di Panduan Pengguna Amazon Elastic Compute Cloud.

> **Note**
>
> Tidak mungkin untuk meningkatkan ukuran disk root untuk AWS Storage Gateway Hardware Appliance.

3. Mulai ulang gateway Anda.

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 menyebabkan peristiwa ini.

Saat gateway Anda berjalan di lingkungan seperti itu, periksa keberadaan `HealthCheckFailure` notifikasi dan lihat log VMware peristiwa untuk VM.

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.

Jika waktu reboot dalam 10 menit dari waktu mulai pemeliharaan gateway yang dikonfigurasi, reboot ini mungkin merupakan kejadian normal dan bukan tanda masalah apa pun. Jika reboot terjadi secara signifikan di luar jendela pemeliharaan, periksa apakah gateway dimulai ulang secara manual.

Pemecahan masalah: Pemindaian keamanan menunjukkan port NFS terbuka

Port NFS tertentu diaktifkan secara default, bahkan pada gateway yang hanya Anda gunakan dengan berbagi file SMB. Jika Anda menggunakan perangkat lunak keamanan pihak ketiga seperti Qualys untuk memindai jaringan tempat File Gateway Anda digunakan, hasil pemindaian mungkin melaporkan port NFS terbuka ini sebagai potensi kerentanan keamanan. Jika Anda hanya menggunakan gateway Anda dengan berbagi file SMB dan Anda ingin menonaktifkan port NFS yang tidak digunakan untuk alasan keamanan, gunakan prosedur berikut:

Untuk menonaktifkan port NFS pada File Gateway:

1. Akses prompt perintah konsol lokal gateway menggunakan prosedur yang diuraikan dalamMenjalankan perintah Storage Gateway di konsol lokal.
2. Masukkan perintah berikut untuk menonaktifkan lalu lintas NFS:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

3. Masukkan perintah berikut untuk mengonfirmasi bahwa port NFS yang diblokir muncul di tabel IP:

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

Pemecahan masalah: Menggunakan metrik CloudWatch

Anda dapat menemukan informasi berikut tentang tindakan untuk mengatasi masalah menggunakan CloudWatch metrik Amazon dengan Storage Gateway.

Topik

Gateway Anda bereaksi lambat saat menjelajah direktori

Jika File Gateway bereaksi lambat saat menjalankan ls perintah atau menelusuri direktori, periksa `IndexFetch` dan `IndexEviction` CloudWatch metrik:

- Jika `IndexFetch` metrik lebih besar dari 0 saat Anda menjalankan `ls` perintah atau menelusuri direktori, File Gateway Anda dimulai tanpa informasi tentang isi direktori yang terpengaruh dan harus mengakses Amazon FSx File Server. Upaya selanjutnya untuk membuat daftar isi direktori itu harus berjalan lebih cepat.
- Jika `IndexEviction` metrik lebih besar dari 0, itu berarti File Gateway Anda telah mencapai batas dari apa yang dapat dikelola dalam cache pada saat itu. Dalam hal ini, File Gateway Anda harus membebaskan beberapa ruang penyimpanan dari direktori yang paling tidak baru diakses untuk mencantumkan direktori baru. Jika ini sering terjadi dan ada dampak kinerja, hubungi Dukungan.

  Dukungan Diskusikan dengan isi bucket S3 terkait dan rekomendasi untuk meningkatkan kinerja berdasarkan kasus penggunaan Anda.

Gateway Anda tidak merespons

Jika File Gateway Anda tidak merespons, lakukan hal berikut:

- Jika ada pembaruan reboot atau perangkat lunak baru-baru ini, maka periksa `IOWaitPercent` metriknya. Metrik ini menunjukkan persentase waktu CPU menganggur ketika ada I/O permintaan disk yang luar biasa. Dalam beberapa kasus, ini mungkin tinggi (10 atau lebih) dan mungkin meningkat setelah server di-boot ulang atau diperbarui. Dalam kasus ini, maka File Gateway Anda mungkin terhambat oleh disk root yang lambat karena membangun kembali cache indeks ke RAM.

Anda dapat mengatasi masalah ini dengan menggunakan disk fisik yang lebih cepat untuk disk root.

- Jika `MemUsedBytes` metrik berada pada atau hampir sama dengan `MemTotalBytes` metrik, maka File Gateway Anda kehabisan RAM yang tersedia. Pastikan bahwa File Gateway Anda memiliki setidaknya RAM minimum yang diperlukan. Jika sudah, pertimbangkan untuk menambahkan lebih banyak RAM ke File Gateway Anda berdasarkan beban kerja dan kasus penggunaan Anda.

  Jika berbagi file adalah SMB, masalahnya mungkin juga disebabkan oleh jumlah klien SMB yang terhubung ke berbagi file. Untuk melihat jumlah klien yang terhubung pada waktu tertentu, periksa `SMBV(1/2/3)Sessions` metriknya. Jika ada banyak klien yang terhubung, Anda mungkin perlu menambahkan lebih banyak RAM ke File Gateway Anda.

Gateway Anda lambat mentransfer data ke Amazon S3

Jika File Gateway Anda lambat mentransfer data ke Amazon S3, lakukan hal berikut:

- Jika `CachePercentDirty` metriknya 80 atau lebih besar, File Gateway Anda menulis data lebih cepat ke disk daripada mengunggah data ke Amazon S3. Pertimbangkan untuk meningkatkan bandwidth untuk diunggah dari File Gateway Anda, menambahkan satu atau lebih disk cache, atau memperlambat penulisan klien.
- Jika `CachePercentDirty` metriknya rendah, periksa `IoWaitPercent` metriknya. Jika `IoWaitPercent` lebih besar dari 10, File Gateway Anda mungkin terhambat oleh kecepatan disk cache lokal. Kami merekomendasikan disk solid state drive (SSD) lokal untuk cache Anda, lebih disukai NVM Express (). NVMe Jika disk tersebut tidak tersedia, coba gunakan beberapa disk cache dari disk fisik terpisah untuk peningkatan kinerja.
- Jika `S3PutObjectRequestTimeS3UploadPartRequestTime`,, atau `S3GetObjectRequestTime` tinggi, mungkin ada hambatan jaringan. Coba analisis jaringan Anda untuk memverifikasi bahwa gateway memiliki bandwidth yang diharapkan.

Gateway Anda melakukan lebih banyak operasi Amazon S3 dari yang diharapkan

Jika File Gateway Anda melakukan lebih banyak operasi Amazon S3 dari yang diharapkan, periksa metriknya. `FilesRenamed` Operasi ganti nama mahal untuk dijalankan di Amazon S3. Optimalkan alur kerja Anda untuk meminimalkan jumlah operasi ganti nama.

Anda tidak melihat file di bucket Amazon S3 Anda

Jika Anda melihat bahwa file di gateway tidak tercermin di bucket Amazon S3, periksa metriknya. `FilesFailingUpload` Jika metrik melaporkan bahwa beberapa file gagal diunggah, periksa pemberitahuan kesehatan Anda. Ketika file gagal diunggah, gateway menghasilkan pemberitahuan kesehatan yang berisi detail lebih lanjut tentang masalah tersebut.

Pekerjaan pencadangan gateway Anda gagal atau ada kesalahan saat menulis ke gateway Anda

Jika pekerjaan pencadangan File Gateway Anda gagal atau ada kesalahan saat menulis ke File Gateway Anda, lakukan hal berikut:

- Jika `CachePercentDirty` metriknya 90 persen atau lebih besar, File Gateway Anda tidak dapat menerima penulisan baru ke disk karena tidak ada cukup ruang yang tersedia pada disk cache. Untuk melihat seberapa cepat File Gateway Anda mengunggah ke Amazon FSx Server, lihat `CloudBytesUploaded` metrik. Bandingkan metrik itu dengan `WriteBytes` metrik, yang menunjukkan seberapa cepat klien menulis file ke File Gateway Anda. Jika klien SMB menulis ke File Gateway Anda lebih cepat daripada yang dapat diunggah ke Amazon FSx Server, tambahkan lebih banyak disk cache untuk menutupi ukuran pekerjaan cadangan minimal. Atau, tingkatkan bandwidth unggahan.
- Jika salinan file besar seperti pekerjaan cadangan gagal tetapi `CachePercentDirty` metriknya kurang dari 80 persen, File Gateway Anda mungkin mencapai batas waktu sesi sisi klien. Untuk SMB, Anda dapat meningkatkan batas waktu ini menggunakan perintah. PowerShell `Set-SmbClientConfiguration -SessionTimeout 300` Menjalankan perintah ini menetapkan batas waktu menjadi 300 detik.

  Untuk NFS, pastikan klien dipasang menggunakan hard mount alih-alih soft mount.

Pemecahan masalah: masalah berbagi file

Anda dapat menemukan informasi berikut tentang tindakan yang harus diambil jika Anda mengalami masalah tak terduga dengan berbagi file Anda.

Topik

- Berbagi file macet dalam keadaan MEMBUAT, MEMPERBARUI, atau MENGHAPUS
- Anda tidak dapat membuat berbagi file

- Berbagi file SMB tidak mengizinkan beberapa metode akses yang berbeda
- Beberapa berbagi file tidak dapat menulis ke bucket S3 yang dipetakan
- Pemberitahuan untuk grup log yang dihapus saat menggunakan log audit
- Tidak dapat mengunggah file ke bucket S3 Anda
- Tidak dapat mengubah enkripsi default untuk menggunakan SSE-KMS untuk mengenkripsi objek yang disimpan di bucket S3 saya
- Perubahan yang dilakukan langsung di bucket S3 dengan versi objek diaktifkan dapat memengaruhi apa yang Anda lihat di berbagi file
- Saat menulis ke bucket S3 dengan versi diaktifkan, Amazon S3 File Gateway dapat membuat beberapa versi objek Amazon S3
- Perubahan pada bucket S3 tidak tercermin di Storage Gateway
- Izin ACL tidak berfungsi seperti yang diharapkan
- Performa gateway Anda menurun setelah Anda melakukan operasi rekursif

Berbagi file macet dalam keadaan MEMBUAT, MEMPERBARUI, atau MENGHAPUS

Status berbagi file merangkum kesehatan berbagi file Anda. Jika berbagi file S3 File Gateway macet di`CREATING`,`UPDATING`, atau `DELETING` status, gunakan langkah pemecahan masalah berikut untuk mengidentifikasi dan menyelesaikan masalah.

Konfirmasikan izin peran IAM dan hubungan kepercayaan

Peran AWS Identity and Access Management (IAM) yang terkait dengan berbagi file Anda harus memiliki izin yang cukup untuk mengakses bucket Amazon S3. Selain itu, kebijakan kepercayaan peran harus memberikan izin layanan Storage Gateway untuk mengambil peran tersebut.

Untuk memverifikasi izin peran IAM:

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran.
3. Pilih peran IAM yang terkait dengan berbagi file Anda.
4. Pilih tab Trust relationship.

5. Konfirmasikan bahwa Storage Gateway terdaftar sebagai entitas tepercaya. Jika Storage Gateway bukan entitas tepercaya, pilih Edit hubungan kepercayaan, lalu tambahkan kebijakan berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Verifikasi bahwa peran IAM memiliki izin yang benar dan bucket Amazon S3 terdaftar sebagai sumber daya dalam kebijakan IAM. Untuk informasi selengkapnya, lihat Memberikan akses ke bucket Amazon S3.

> **Note**
>
> Untuk menghindari masalah pencegahan wakil yang membingungkan lintas layanan, gunakan kebijakan hubungan kepercayaan yang mencakup kunci konteks kondisi. Untuk informasi selengkapnya, lihat the section called “Pencegahan "confused deputy" lintas layanan”.

Verifikasi AWS STS diaktifkan di Wilayah Anda

Berbagi file dapat macet di `UPDATING` negara bagian `CREATING` atau jika AWS Security Token Service (AWS STS) dinonaktifkan di AWS Wilayah Anda.

Untuk memverifikasi status AWS STS:

1. Buka AWS Identity and Access Management konsol di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengaturan akun.

3. Di bagian Security Token Service (STS), verifikasi bahwa Status Aktif untuk AWS Wilayah tempat Anda ingin membuat berbagi file.
4. Jika statusnya Tidak Aktif, pilih Aktifkan untuk mengaktifkan AWS STS di Wilayah tersebut.

Verifikasi bucket S3 ada dan ikuti aturan penamaan

Berbagi file Anda memerlukan bucket Amazon S3 yang valid yang mengikuti konvensi penamaan Amazon S3.

Untuk memverifikasi bucket S3 Anda:

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Konfirmasikan bahwa bucket Amazon S3 yang dipetakan ke berbagi file Anda sudah ada. Jika ember tidak ada, buatlah. Setelah Anda membuat bucket, status berbagi file akan berubah menjadi`AVAILABLE`. Untuk informasi selengkapnya, lihat Membuat bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
3. Pastikan nama bucket Anda mematuhi aturan penamaan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

> **Note**
>
> S3 File Gateway tidak mendukung bucket Amazon S3 dengan period `.` () dalam nama bucket.

Hapus paksa file share yang macet dalam status DELETING

Saat Anda menghapus file share, gateway akan menghapus share dari bucket Amazon S3 terkait. Namun, data yang saat ini diunggah terus diunggah sebelum penghapusan selesai. Selama proses ini, berbagi file menunjukkan `DELETING` status.

> **Important**
>
> Periksa CloudWatch metrik Amazon `CachePercentDirty` untuk gateway Anda untuk menentukan berapa banyak data yang tertunda upload. Untuk informasi selengkapnya tentang metrik Storage Gateway, lihatthe section called “Memantau Gateway File Gateway S3 Anda”.

Jika Anda tidak ingin menunggu semua unggahan yang sedang berlangsung selesai, Anda dapat menghapus file share secara paksa.

Untuk menghapus paksa berbagi file:

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/.
2. Di panel navigasi, pilih Berbagi file.
3. Pilih file share yang ingin Anda hapus.
4. Pilih tab Detail, dan tinjau pesan Berbagi file ini sedang dihapus.
5. Verifikasi ID berbagi file dalam pesan, lalu pilih kotak konfirmasi.

> **Note**
>
> Anda tidak dapat membatalkan operasi penghapusan paksa.

6. Pilih Paksa hapus sekarang.

Atau, Anda dapat menggunakan AWS CLI delete-file-shareperintah dengan `--force-delete` parameter yang disetel ke`true`.

> **Important**
>
> Sebelum menghapus file share secara paksa, konfirmasikan bahwa gateway Anda tidak dalam `OFFLINE` status. Jika gateway sedang offline, pertama-tama selesaikan masalah offline. Untuk informasi selengkapnya, lihat the section called “Pemecahan masalah: masalah offline gateway”.

Jika gateway virtual machine (VM) sudah dihapus, Anda harus menghapus gateway dari konsol Storage Gateway untuk menghapus semua berbagi file terkait, termasuk yang terjebak dalam `DELETING` status. Untuk informasi selengkapnya, lihat the section called “Menghapus gateway Anda dan menghapus sumber daya”.

Memecahkan masalah konektivitas jaringan

Masalah jaringan dapat mencegah berbagi file Anda dari transisi keluar dari`CREATING`,`UPDATING`, atau `DELETING` status. Masalah jaringan umum meliputi:

- Gateway Anda sedang offline atau gateway VM dihapus.
- Akses jaringan antara Storage Gateway dan endpoint layanan Amazon S3 diblokir.
- Titik akhir Amazon S3 Amazon VPC yang digunakan gateway untuk berkomunikasi dengan Amazon S3 telah dihapus.
- Port jaringan yang diperlukan tidak terbuka atau perutean jaringan tidak dikonfigurasi dengan benar.

Uji konektivitas S3 dari konsol lokal gateway

Untuk menguji konektivitas S3:

1. Masuk ke konsol lokal gateway Anda. Untuk informasi selengkapnya, lihat the section called "Masuk ke konsol lokal File Gateway".
2. Di menu utama Storage Gateway - Configuration, masukkan nomor yang sesuai dengan Test S3 Connectivity.
3. Pilih jenis endpoint Amazon S3:
   - Untuk lalu lintas Amazon S3 yang mengalir melalui Gateway Internet, Gateway NAT, Gateway Transit, atau titik akhir Amazon S3 Gateway Amazon VPC, pilih Publik.
   - Untuk lalu lintas Amazon S3 yang mengalir melalui antarmuka Amazon S3 titik akhir Amazon VPC, pilih VPC (). PrivateLink
   - Untuk titik akhir FIPS, pilih opsi FIPS.
4. Masuk ke Wilayah bucket Amazon S3.
5. Jika menggunakan titik akhir Amazon VPC, masukkan nama DNS titik akhir Amazon S3 Amazon VPC (misalnya,). `vpce-0329c2790456f2d01-0at85l34`

Gateway secara otomatis melakukan tes konektivitas yang memvalidasi koneksi jaringan dan koneksi SSL. Jika tes gagal:

- Kegagalan Uji Jaringan - Biasanya disebabkan oleh aturan firewall, konfigurasi grup keamanan, atau perutean jaringan yang tidak tepat. Verifikasi bahwa port yang diperlukan terbuka dan perutean jaringan dikonfigurasi dengan benar.
- Kegagalan Uji SSL - Menunjukkan bahwa inspeksi SSL atau inspeksi paket mendalam terjadi antara titik akhir layanan VM gateway dan Amazon S3 Anda. Nonaktifkan SSL dan inspeksi paket mendalam untuk lalu lintas Storage Gateway.

Verifikasi konfigurasi proxy

Jika gateway Anda menggunakan server proxy, verifikasi bahwa proxy tidak memblokir komunikasi jaringan.

Untuk memeriksa konfigurasi proxy:

1. Di menu utama Storage Gateway - Configuration, masukkan nomor yang sesuai dengan HTTP/SOCKS Proxy Configuration.
2. Pilih opsi untuk melihat konfigurasi proxy jaringan saat ini.
3. Jika proxy dikonfigurasi, verifikasi bahwa lalu lintas Amazon S3 dapat mengalir dari Storage Gateway ke server proxy melalui port 3128 (atau port listener yang dikonfigurasi), lalu ke endpoint Amazon S3 melalui port 443.
4. Konfirmasikan bahwa proxy atau firewall memungkinkan lalu lintas ke dan dari port jaringan dan titik akhir layanan yang diperlukan oleh Storage Gateway. Untuk informasi selengkapnya, lihat port jaringan yang diperlukan.

Jika masalah berlanjut, Anda dapat menghapus sementara konfigurasi proxy untuk menentukan apakah proxy menyebabkan masalah.

Verifikasi grup keamanan dan perutean jaringan

- Untuk gateway di Amazon EC2 - Konfirmasikan bahwa grup keamanan memiliki port 443 terbuka ke titik akhir Amazon S3. Verifikasi bahwa tabel rute subnet Amazon EC2 dengan benar merutekan lalu lintas Amazon S3 ke titik akhir Amazon S3. Untuk informasi selengkapnya, lihat port jaringan yang diperlukan.
- Untuk gateway lokal - Konfirmasikan bahwa aturan firewall mengizinkan port yang diperlukan dan tabel rute lokal merutekan lalu lintas Amazon S3 dengan benar ke titik akhir Amazon S3. Untuk informasi selengkapnya, lihat port jaringan yang diperlukan.
- Titik akhir VPC - Verifikasi bahwa titik akhir VPC Amazon S3 Amazon yang digunakan oleh gateway belum dihapus. Jika titik akhir VPC Amazon dihapus dan gateway tidak memiliki alamat IP publik, gateway tidak dapat berkomunikasi dengan Amazon S3.

Anda tidak dapat membuat berbagi file

1. Jika Anda tidak dapat membuat berbagi file karena berbagi file macet dalam status CREATING, verifikasi bahwa bucket S3 tempat Anda memetakan file share sudah ada. Untuk informasi tentang

cara melakukannya, lihatBerbagi file macet dalam keadaan MEMBUAT, MEMPERBARUI, atau MENGHAPUS, sebelumnya.

2. Jika bucket S3 ada, maka verifikasi yang AWS Security Token Service diaktifkan di wilayah tempat Anda membuat file share. Jika token keamanan tidak aktif, Anda harus mengaktifkannya. Untuk informasi tentang cara mengaktifkan token menggunakan AWS Security Token Service, lihat Mengaktifkan dan menonaktifkan AWS STS di AWS Wilayah dalam Panduan Pengguna IAM.

Berbagi file SMB tidak mengizinkan beberapa metode akses yang berbeda

Berbagi file SMB memiliki batasan sebagai berikut:

1. Ketika klien yang sama mencoba memasang file SMB Active Directory dan akses Tamu, pesan kesalahan berikut akan ditampilkan: `Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Pengguna Windows tidak dapat tetap terhubung ke dua berbagi file SMB Akses Tamu, dan mungkin terputus saat koneksi Akses Tamu baru dibuat.
3. Klien Windows tidak dapat memasang akses tamu dan berbagi file SMB Direktori Aktif yang diekspor oleh gateway yang sama.

Beberapa berbagi file tidak dapat menulis ke bucket S3 yang dipetakan

Kami tidak menyarankan mengonfigurasi bucket S3 Anda untuk memungkinkan beberapa pembagian file ditulis ke satu bucket S3. Pendekatan ini dapat menyebabkan hasil yang tidak terduga.

Sebagai gantinya, kami menyarankan Anda hanya mengizinkan satu file share untuk menulis ke setiap bucket S3. Anda membuat kebijakan bucket untuk mengizinkan hanya peran yang terkait dengan berbagi file Anda untuk menulis ke bucket. Untuk informasi selengkapnya, lihat Praktik Terbaik untuk Gateway File.

Pemberitahuan untuk grup log yang dihapus saat menggunakan log audit

Jika grup log tidak ada, pengguna dapat memilih tautan grup log di bawah pesan tersebut untuk membuat grup log baru atau menggunakan grup log yang ada untuk digunakan sebagai target log audit

Tidak dapat mengunggah file ke bucket S3 Anda

Jika Anda tidak dapat mengunggah file ke bucket S3, lakukan hal berikut:

1. Pastikan Anda telah memberikan akses yang diperlukan untuk Amazon S3 File Gateway untuk mengunggah file ke bucket S3 Anda. Untuk informasi selengkapnya, lihat Memberikan akses ke bucket Amazon S3.
2. Pastikan peran yang membuat bucket memiliki izin untuk menulis ke bucket S3. Untuk informasi selengkapnya, lihat Praktik Terbaik untuk Gateway File.
3. Jika File Gateway Anda menggunakan SSE-KMS atau DSSE-KMS untuk enkripsi, pastikan peran IAM yang terkait dengan berbagi file mencakup izin KMS:Encrypt, KMS:Decrypt, kms: *, kms:, dan kms:. ReEncrypt GenerateDataKey DescribeKey Untuk informasi selengkapnya, lihat Menggunakan Kebijakan Berbasis Identitas (Kebijakan IAM) untuk Storage Gateway.

Tidak dapat mengubah enkripsi default untuk menggunakan SSE-KMS untuk mengenkripsi objek yang disimpan di bucket S3 saya

Jika Anda mengubah enkripsi default dan menjadikan SSE-KMS (enkripsi sisi server dengan kunci yang AWS KMS dikelola) sebagai default untuk bucket S3, objek yang disimpan oleh Amazon S3 File Gateway dalam bucket tidak dienkripsi dengan SSE-KMS. Secara default, Gateway File S3 menggunakan enkripsi sisi server yang dikelola dengan Amazon S3 (SSE-S3) saat menulis data ke bucket S3. Mengubah default tidak akan secara otomatis mengubah enkripsi Anda.

Untuk mengubah enkripsi untuk menggunakan SSE-KMS dengan AWS KMS kunci Anda sendiri, Anda harus mengaktifkan enkripsi SSE-KMS. Untuk melakukannya, Anda memberikan Nama Sumber Daya Amazon (ARN) dari kunci KMS saat Anda membuat berbagi file. Anda juga dapat memperbarui pengaturan KMS untuk berbagi file Anda dengan menggunakan operasi `UpdateNFSFileShare` atau `UpdateSMBFileShare` API. Pembaruan ini berlaku untuk objek yang disimpan dalam bucket S3 setelah pembaruan. Untuk informasi selengkapnya, lihat Enkripsi data menggunakan AWS KMS.

Perubahan yang dilakukan langsung di bucket S3 dengan versi objek diaktifkan dapat memengaruhi apa yang Anda lihat di berbagi file

Jika bucket S3 Anda memiliki objek yang ditulis oleh klien lain, tampilan bucket S3 Anda mungkin bukan up-to-date karena pembuatan versi objek bucket S3. Anda harus selalu menyegarkan cache Anda sebelum memeriksa file yang menarik.

Pembuatan versi objek adalah fitur bucket S3 opsional yang membantu melindungi data dengan menyimpan banyak salinan objek dengan nama yang sama. Setiap salinan memiliki nilai ID terpisah, misalnya`file1.jpg`: `ID="xxx"` dan`file1.jpg`:`ID="yyy"`. Jumlah objek yang diberi nama identik dan masa pakainya dikendalikan oleh kebijakan siklus hidup Amazon S3. Untuk detail selengkapnya tentang konsep Amazon S3 ini, lihat Menggunakan pembuatan versi dan manajemen siklus hidup Objek di Panduan Pengembang Amazon S3.

Saat Anda menghapus objek berversi, objek tersebut ditandai dengan penanda hapus tetapi dipertahankan. Hanya pemilik bucket S3 yang dapat menghapus objek secara permanen dengan versi diaktifkan.

Di S3 File Gateway Anda, file yang ditampilkan adalah versi objek terbaru dalam bucket S3 pada saat objek diambil atau cache di-refresh. S3 File Gateways mengabaikan versi lama atau objek apa pun yang ditandai untuk dihapus. Saat membaca file, Anda membaca data dari versi terbaru. Saat Anda menulis file di berbagi file, Gateway File S3 Anda membuat versi baru dari objek bernama dengan perubahan Anda, dan versi itu menjadi versi terbaru.

Gateway File S3 Anda terus membaca dari versi sebelumnya, dan pembaruan yang Anda buat didasarkan pada versi sebelumnya jika versi baru ditambahkan ke bucket S3 di luar aplikasi Anda. Untuk membaca versi terbaru objek, gunakan tindakan RefreshCacheAPI atau refresh dari konsol seperti yang dijelaskan dalamMenyegarkan cache objek bucket Amazon S3.

> **Important**
>
> Kami tidak menyarankan objek atau file ditulis ke bucket S3 File Gateway S3 Anda dari luar berbagi file.

Saat menulis ke bucket S3 dengan versi diaktifkan, Amazon S3 File Gateway dapat membuat beberapa versi objek Amazon S3

Dengan versi objek diaktifkan, Anda mungkin memiliki beberapa versi objek yang dibuat di Amazon S3 pada setiap pembaruan ke file dari klien NFS atau SMB Anda. Berikut adalah skenario yang dapat menghasilkan beberapa versi objek yang dibuat di bucket S3 Anda:

- Saat file dimodifikasi di Amazon S3 File Gateway oleh klien NFS atau SMB setelah diunggah ke Amazon S3, Gateway File S3 mengunggah data baru atau yang dimodifikasi alih-alih mengunggah seluruh file. Modifikasi file menghasilkan versi baru objek Amazon S3 yang sedang dibuat.

- Saat file ditulis ke Gateway File S3 oleh klien NFS atau SMB, Gateway File S3 mengunggah data file ke Amazon S3 diikuti oleh metadatanya, (kepemilikan, cap waktu, dll.). Mengunggah data file akan membuat objek Amazon S3, dan mengunggah metadata untuk file akan memperbarui metadata untuk objek Amazon S3. Proses ini menciptakan versi lain dari objek, menghasilkan dua versi objek.
- Saat S3 File Gateway mengunggah file yang lebih besar, mungkin perlu mengunggah potongan file yang lebih kecil sebelum klien selesai menulis ke File Gateway. Beberapa alasan untuk ini termasuk untuk membebaskan ruang cache atau tingkat penulisan yang tinggi ke file. Ini dapat menghasilkan beberapa versi objek di bucket S3.

Anda harus memantau bucket S3 untuk menentukan berapa banyak versi objek yang ada sebelum menyiapkan kebijakan siklus hidup untuk memindahkan objek ke kelas penyimpanan yang berbeda. Anda harus mengonfigurasi kedaluwarsa siklus hidup untuk versi sebelumnya untuk meminimalkan jumlah versi yang Anda miliki untuk objek di bucket S3 Anda. Penggunaan replikasi Same-Region (SRR) atau replikasi Cross-Region (CRR) antara bucket S3 akan meningkatkan penyimpanan yang digunakan. Untuk informasi lebih lanjut tentang replikasi, lihat Replikasi.

> **Important**
>
> Jangan mengonfigurasi replikasi antara bucket S3 sampai Anda memahami berapa banyak penyimpanan yang digunakan saat pembuatan versi objek dihidupkan.

Penggunaan bucket S3 berversi dapat sangat meningkatkan jumlah penyimpanan di Amazon S3 karena setiap modifikasi pada file membuat versi baru dari objek S3. Secara default, Amazon S3 terus menyimpan semua versi ini kecuali Anda secara khusus membuat kebijakan untuk mengganti perilaku ini dan membatasi jumlah versi yang disimpan. Jika Anda melihat penggunaan penyimpanan yang luar biasa besar dengan versi objek diaktifkan, periksa apakah kebijakan penyimpanan Anda ditetapkan dengan tepat. Peningkatan jumlah `HTTP 503-slow down` tanggapan untuk permintaan browser juga dapat menjadi hasil dari masalah dengan versi objek.

Jika Anda mengaktifkan versi objek setelah menginstal Gateway File S3, semua objek unik dipertahankan (`ID="NULL"`) dan Anda dapat melihat semuanya di sistem file. Versi baru objek diberi ID unik (versi lama dipertahankan). Berdasarkan stempel waktu objek, hanya objek berversi terbaru yang dapat dilihat di sistem file NFS.

Setelah Anda mengaktifkan versi objek, bucket S3 Anda tidak dapat dikembalikan ke status nonversioned. Namun, Anda dapat menangguhkan pembuatan versi. Saat Anda menangguhkan pembuatan versi, objek baru diberi ID. Jika objek bernama yang sama ada dengan `ID=”NULL”` nilai, versi yang lebih lama akan ditimpa. Namun, versi apa pun yang berisi `NULL` non-ID dipertahankan. Stempel waktu mengidentifikasi objek baru sebagai yang sekarang, dan itulah yang muncul di sistem file NFS.

Perubahan pada bucket S3 tidak tercermin di Storage Gateway

Storage Gateway memperbarui cache berbagi file secara otomatis ketika Anda menulis file ke cache secara lokal menggunakan berbagi file. Namun, Storage Gateway tidak secara otomatis memperbarui cache saat Anda mengunggah file langsung ke Amazon S3. Ketika Anda melakukan ini, Anda harus melakukan `RefreshCache` operasi untuk melihat perubahan pada berbagi file. Jika Anda memiliki lebih dari satu file share, maka Anda harus menjalankan `RefreshCache` operasi pada setiap file share.

Anda dapat menyegarkan cache menggunakan konsol Storage Gateway dan AWS Command Line Interface (AWS CLI):

- Untuk menyegarkan cache menggunakan konsol Storage Gateway, lihat Menyegarkan objek di bucket Amazon S3.
- Untuk me-refresh cache menggunakan AWS CLI:
  1. Jalankan perintah `aws storagegateway list-file-shares`
  2. Salin Amazon Resource Number (ARN) dari file berbagi dengan cache yang ingin Anda refresh.
  3. Jalankan `refresh-cache` perintah dengan ARN Anda sebagai nilai untuk: `--file-share-arn`

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

Untuk mengotomatiskan `RefreshCache` operasi, lihat Bagaimana cara mengotomatiskan RefreshCache operasi di Storage Gateway?

Izin ACL tidak berfungsi seperti yang diharapkan

Jika izin daftar kontrol akses (ACL) tidak berfungsi seperti yang Anda harapkan dengan berbagi file SMB, Anda dapat melakukan pengujian.

Untuk melakukan ini, pertama-tama uji izin pada server file Microsoft Windows atau berbagi file Windows lokal. Kemudian bandingkan perilaku tersebut dengan berbagi file gateway Anda.

Performa gateway Anda menurun setelah Anda melakukan operasi rekursif

Dalam beberapa kasus, Anda mungkin melakukan operasi rekursif, seperti mengganti nama direktori atau mengaktifkan pewarisan untuk ACL, dan memaksanya turun ke pohon. Jika Anda melakukan ini, Gateway File S3 Anda secara rekursif menerapkan operasi ke semua objek dalam berbagi file.

Misalnya, Anda menerapkan pewarisan ke objek yang ada di bucket S3. Gateway File S3 Anda secara rekursif menerapkan pewarisan ke semua objek di bucket. Operasi semacam itu dapat menyebabkan kinerja gateway Anda menurun.

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, lihatPemecahan masalah: masalah ketersediaan tinggi.

Pemecahan masalah: masalah ketersediaan tinggi

Anda dapat menemukan informasi berikut tentang tindakan yang harus diambil jika Anda mengalami masalah ketersediaan.

Topik

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: HealthCheckFailure
- Pemberitahuan: AvailabilityMonitorTest

Pemberitahuan: Reboot

Anda bisa mendapatkan notifikasi reboot saat gateway VM dimulai ulang. Anda dapat memulai ulang VM gateway dengan menggunakan konsol VM Hypervisor Management atau konsol Storage Gateway. Anda juga dapat memulai ulang dengan menggunakan perangkat lunak gateway selama siklus pemeliharaan gateway.

Tindakan yang Harus Diambil

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 menyebabkan peristiwa ini.

Tindakan yang Harus Diambil

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 yang Harus Diambil

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-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 File Gateway

Bagian ini berisi topik-topik berikut, yang memberikan informasi tentang praktik terbaik untuk bekerja dengan gateway, berbagi file, bucket, 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. Memecahkan masalah dengan penerapan Storage 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 EC2 Amazon Machine Image (AMI). Jika VM gateway Anda tidak berfungsi, aktifkan gateway baru dan pulihkan data Anda ke gateway itu menggunakan instruksi berikut.

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 konektivitas jaringan gateway Anda.

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.

Memulihkan data Anda dari pusat data yang tidak dapat diakses

Jika gateway atau pusat data Anda menjadi tidak dapat diakses karena alasan tertentu, Anda dapat memulihkan data Anda ke gateway lain di pusat data yang berbeda atau memulihkan ke gateway yang dihosting pada instans Amazon EC2. Jika Anda tidak memiliki akses ke pusat data lain, sebaiknya buat gateway pada instans Amazon EC2. Langkah-langkah yang Anda ikuti tergantung pada jenis gateway tempat Anda meliput datanya.

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

Untuk File Gateway, Anda memetakan baru ke bucket Amazon S3 FSx yang berisi data yang ingin Anda pulihkan.

1. Buat dan aktifkan File Gateway baru di host Amazon EC2. Untuk informasi selengkapnya, lihat Menerapkan host Amazon EC2 default untuk S3 File Gateway.
2. Buat baru di gateway EC2 yang Anda buat. Untuk informasi selengkapnya, lihat Membuat berbagi file .
3. Pasang Anda pada klien Anda dan petakan ke bucket S3 FSx yang berisi data yang ingin Anda pulihkan. Untuk informasi selengkapnya, lihat Mount dan gunakan file share Anda .

Praktik terbaik: mengelola unggahan multipart

Saat mentransfer file besar, S3 File Gateway menggunakan fitur unggahan multipart Amazon S3 untuk membagi file menjadi bagian-bagian yang lebih kecil dan mentransfernya secara paralel untuk meningkatkan efisiensi. Untuk informasi selengkapnya tentang unggahan multibagian, lihat Mengunggah dan menyalin objek menggunakan unggahan multibagian di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Jika unggahan multibagian tidak berhasil diselesaikan karena alasan apa pun, gateway biasanya menghentikan transfer, menghapus bagian file yang ditransfer sebagian dari Amazon S3, dan mencoba transfer lagi. Dalam kasus yang jarang terjadi, seperti ketika kegagalan perangkat keras atau jaringan mencegah gateway dibersihkan setelah unggahan multibagian yang gagal, potongan file yang ditransfer sebagian mungkin tetap ada di Amazon S3 di mana mereka dapat dikenakan biaya penyimpanan.

Sebagai praktik terbaik untuk meminimalkan biaya penyimpanan Amazon S3 dari unggahan multibagian yang tidak lengkap, sebaiknya konfigurasi aturan siklus hidup bucket Amazon S3 yang menggunakan `AbortIncompleteMultipartUpload` tindakan API untuk secara otomatis menghentikan transfer yang gagal dan menghapus bagian file terkait setelah beberapa hari yang ditentukan. Untuk petunjuknya, lihat Mengonfigurasi konfigurasi siklus hidup bucket untuk menghapus unggahan multibagian yang tidak lengkap di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Praktik terbaik: Buka zip file terkompresi secara lokal sebelum menyalin ke gateway

Jika Anda mencoba membuka zip arsip terkompresi yang berisi ribuan file saat disimpan di gateway Anda, Anda mungkin mengalami penundaan terkait kinerja yang signifikan. Proses membuka ritsleting arsip yang berisi sejumlah besar file pada semua jenis berbagi file jaringan secara inheren melibatkan volume input/output operasi yang tinggi, manipulasi cache metadata, overhead jaringan, dan latensi. Selain itu, Storage Gateway tidak dapat menentukan kapan setiap file dari arsip telah selesai membuka ritsleting, dan dapat mulai mengunggah file sebelum proses selesai, yang selanjutnya berdampak pada kinerja. Masalah-masalah ini diperparah ketika file di dalam arsip banyak, tetapi ukurannya kecil.

Sebagai praktik terbaik, kami sarankan untuk mentransfer arsip terkompresi dari gateway Anda ke mesin lokal Anda terlebih dahulu, sebelum Anda membuka ritsletingnya. Kemudian, jika perlu, Anda

dapat menggunakan alat seperti robocopy atau rsync untuk mentransfer file yang tidak di-zip kembali ke gateway.

Pertahankan atribut file saat menyalin data dari Windows Server

Dimungkinkan untuk menyalin file ke File Gateway Anda menggunakan `copy` perintah dasar pada Microsoft Windows, tetapi perintah ini hanya menyalin data file secara default - menghilangkan atribut file tertentu seperti deskriptor keamanan. Jika file disalin ke gateway tanpa batasan keamanan yang sesuai dan informasi Daftar Kontrol Akses Discretionary (DACL), ada kemungkinan bahwa mereka dapat diakses oleh pengguna yang tidak sah.

Sebagai praktik terbaik untuk melestarikan semua atribut file dan informasi keamanan saat menyalin file ke gateway Anda di Microsoft Windows Server, sebaiknya gunakan `xcopy` perintah `robocopy` atau, dengan `/o` tanda `/copy:DS` atau, masing-masing. Untuk informasi selengkapnya, lihat robocopy dan xcopy di dokumentasi referensi perintah Microsoft Windows Server.

Praktik terbaik: Ukuran disk cache yang tepat

Untuk kinerja terbaik, ukuran cache disk total harus cukup besar untuk menutupi ukuran set kerja aktif Anda. Untuk read/write beban kerja yang berat baca dan campuran, ini memastikan bahwa Anda dapat mencapai persentase klik cache yang tinggi pada pembacaan, yang diinginkan. Anda dapat memantau ini melalui `CacheHitPercent` metrik untuk Gateway File S3 Anda.

Untuk beban kerja berat tulis (misalnya untuk pencadangan dan pengarsipan), S3 File Gateway buffer penulisan yang masuk di cache disk sebelum menyalin data ini secara asinkron ke Amazon S3. Anda harus memastikan bahwa Anda memiliki kapasitas cache yang cukup untuk menyangga data tertulis. `CachePercentDirty`Metrik memberikan indikasi persentase cache disk yang belum bertahan AWS.

Nilai rendah diinginkan. `CachePercentDirty` Nilai yang secara konsisten mendekati 100% menunjukkan bahwa S3 File Gateway tidak dapat mengikuti tingkat lalu lintas tulis yang masuk. Anda dapat menghindari hal ini dengan meningkatkan kapasitas cache disk yang disediakan, atau meningkatkan bandwidth jaringan khusus yang tersedia dari S3 File Gateway ke Amazon S3, atau keduanya.

Untuk informasi selengkapnya tentang ukuran disk cache, lihat praktik terbaik ukuran cache Amazon S3 File Gateway di saluran Amazon Web Services resmi. YouTube

Bekerja dengan beberapa berbagi file dan bucket Amazon S3

Saat Anda mengonfigurasi satu bucket Amazon S3 untuk mengizinkan beberapa gateway atau berbagi file untuk ditulis, hasilnya tidak dapat diprediksi. Anda dapat mengonfigurasi bucket Anda dengan salah satu dari dua cara untuk menghindari hasil yang tidak terduga. Pilih metode konfigurasi yang paling sesuai dengan kasus penggunaan Anda dari opsi berikut:

- Konfigurasikan bucket S3 Anda sehingga hanya satu file share yang dapat menulis ke setiap bucket. Gunakan berbagi file yang berbeda untuk menulis ke setiap bucket.

  Untuk melakukannya, buat kebijakan bucket S3 yang menyangkal semua peran kecuali peran yang digunakan untuk berbagi file tertentu untuk menempatkan atau menghapus objek di bucket. Lampirkan kebijakan serupa ke setiap bucket, dengan menentukan pembagian file yang berbeda untuk ditulis ke setiap bucket.

  Contoh kebijakan berikut menolak izin penulisan bucket S3 ke semua peran kecuali peran yang membuat bucket. Tindakan `s3:DeleteObject` dan `s3:PutObject` tindakan ditolak untuk semua peran kecuali`"TestUser"`. Kebijakan ini berlaku untuk semua objek dalam `"arn:aws:s3:::amzn-s3-demo-bucket/*"` ember.

  JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
```

```
}
```

- Jika Anda ingin beberapa berbagi file ditulis ke bucket Amazon S3 yang sama, Anda harus mencegah berbagi file mencoba menulis ke objek yang sama secara bersamaan.

  Untuk melakukan ini, konfigurasikan awalan objek unik yang terpisah untuk setiap berbagi file. Ini berarti bahwa setiap berbagi file hanya menulis ke objek dengan awalan yang sesuai, dan tidak menulis ke objek yang terkait dengan berbagi file lain dalam penerapan Anda. Anda mengonfigurasi awalan objek di bidang nama awalan S3 saat Anda membuat berbagi file baru.

Bersihkan sumber daya yang tidak perlu

Sebagai praktik terbaik, kami merekomendasikan untuk membersihkan sumber daya Storage Gateway untuk menghindari biaya yang tidak terduga atau tidak perlu. Misalnya, jika Anda membuat gateway sebagai latihan demonstrasi atau pengujian, pertimbangkan untuk menghapusnya dan alat virtualnya dari penerapan Anda. Gunakan prosedur berikut untuk membersihkan sumber daya.

Untuk membersihkan sumber daya yang tidak Anda butuhkan

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

Sumber daya Storage Gateway tambahan

Bagian ini berisi topik-topik berikut, yang memberikan informasi dan sumber daya tambahan yang terkait dengan pengaturan dan penggunaan AWS Storage Gateway:

Topik

- Pengaturan tuan rumah- Pelajari cara menerapkan dan mengonfigurasi host mesin virtual untuk gateway Anda.
- Menggunakan Storage Gateway dengan VMware HA- Pelajari cara mengatur Storage Gateway untuk bekerja dengan fitur ketersediaan tinggi VMware vSphere.
- Mendapatkan kunci aktivasi- Pelajari di mana menemukan kunci aktivasi yang perlu Anda berikan saat Anda menerapkan gateway baru.
- Dukungan atribut file- Pelajari bagaimana gateway Anda menangani atribut file DOS dan Windows.
- Menggunakan Direct Connect- Pelajari cara membuat koneksi jaringan khusus antara gateway lokal dan AWS cloud.
- Izin Direktori Aktif- Pelajari izin mana yang harus dimiliki akun layanan Anda untuk dapat bergabung dengan gateway Anda ke domain Direktori Aktif Anda.
- 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 ID sumber daya- Pelajari cara AWS mengidentifikasi sumber daya dan subresource yang dibuat oleh Storage Gateway.
- Memberi tag ke sumber daya Anda- Pelajari cara menggunakan tag metadata untuk mengkategorikan sumber daya Anda dan membuatnya lebih mudah dikelola.
- Komponen-komponen Open-source- Pelajari tentang alat dan lisensi pihak ketiga yang digunakan untuk memberikan fungsionalitas Storage Gateway.
- Kuota- Pelajari tentang batas dan kuota untuk File Gateway, termasuk batasan minimum dan maksimum untuk berbagi file dan disk cache lokal.
- Menggunakan kelas penyimpanan- Pelajari tentang kelas penyimpanan Amazon S3 yang didukung File Gateway, dan apa yang harus dipertimbangkan saat memilih kelas penyimpanan.
- Menggunakan driver Kubernetes CSI- Pelajari cara menginstal dan mengkonfigurasi driver Container Storage Interface (CSI) untuk memungkinkan instance Kubernetes menggunakan File Gateway untuk penyimpanan.

- Terraform modul- Pelajari cara menggunakan Terraform untuk menyebarkan File Gateway sebagai mesin virtual.

Menyebarkan dan mengonfigurasi host VM gateway

Topik berikut memberikan informasi tentang pengaturan platform host mesin virtual untuk gateway Anda.

Topik

- Menerapkan host Amazon EC2 default untuk S3 File Gateway
- Menerapkan host Amazon EC2 yang disesuaikan untuk S3 File Gateway
- Ubah opsi metadata instans Amazon EC2
- Sinkronisasi waktu VM dengan Hyper-V atau waktu host Linux KVM
- Sinkronisasi waktu VM dengan waktu host VMware
- Mengkonfigurasi adapter jaringan untuk gateway Anda
- Menggunakan VMware vSphere Ketersediaan Tinggi dengan Storage Gateway

Menerapkan host Amazon EC2 default untuk S3 File Gateway

Topik ini mencantumkan langkah-langkah untuk menerapkan host Amazon EC2 menggunakan spesifikasi default.

Anda dapat menerapkan dan mengaktifkan Amazon S3 File Gateway Amazon FSx File Gateway Elastic Compute Cloud (Amazon EC2). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai komunitas AMI.

> **Note**
>
> AMI komunitas Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.

1. Untuk menyiapkan instans Amazon EC2, pilih Amazon EC2 sebagai platform Host di bagian Opsi platform pada alur kerja. Untuk petunjuk cara mengonfigurasi instans Amazon EC2, lihat Menerapkan instans Amazon EC2 untuk meng-host Gateway File Amazon S3 Menerapkan instans Amazon Anda.

2. Pilih Launch instance untuk membuka template AWS Storage Gateway AMI di konsol Amazon EC2 dan sesuaikan pengaturan tambahan seperti tipe Instans, Pengaturan jaringan, dan Konfigurasi penyimpanan.
3. Secara opsional, Anda dapat memilih Gunakan pengaturan default di konsol Storage Gateway untuk menerapkan instans Amazon EC2 dengan konfigurasi default.

   Instans Amazon EC2 yang dibuat menggunakan pengaturan default memiliki spesifikasi default berikut:

   - Jenis contoh - m5.xlarge
   - Pengaturan Jaringan
     - Untuk VPC, pilih VPC yang Anda inginkan untuk menjalankan instans EC2 Anda.
     - Untuk Subnet, tentukan subnet tempat instans EC2 Anda harus diluncurkan.

     > **Note**
     >
     > Subnet VPC akan muncul di drop-down hanya jika mereka mengaktifkan pengaturan alamat IP publik yang ditetapkan secara otomatis dari konsol manajemen VPC.

     - Auto-assign IP Publik - Diaktifkan
     - Grup keamanan EC2 dibuat dan dikaitkan dengan Instans EC2. Grup keamanan memiliki aturan port masuk berikut:

     > **Note**
     >
     > Anda akan membutuhkan Port 80 terbuka selama aktivasi gateway. Port ditutup segera setelah aktivasi. Setelah itu, instans EC2 Anda hanya dapat diakses melalui port lain dari VPC yang dipilih.
     > Berbagi file di gateway Anda hanya dapat diakses dari host di VPC yang sama dengan gateway. Jika berbagi file perlu diakses dari host di luar VPC, Anda harus memperbarui aturan grup keamanan yang sesuai.
     > Anda dapat mengedit grup keamanan kapan saja dengan menavigasi ke halaman detail instans Amazon EC2, memilih Keamanan, menavigasi ke detail grup Keamanan, dan memilih ID grup keamanan.

Port	Protokol	Protokol Sistem File				
80	TCP	Akses HTTP untuk aktivasi				
111	TCP, UDP	NFSv3				
139	TCP, UDP	SMB				
445	TCP	SMB				
2049	TCP, UDP	NFS				
20048	TCP, UDP	NFSv3				

- Konfigurasikan penyimpanan

Pengaturan Default	Volume Akar AMI	Volume 2 Cache				
Nama perangkat		'/dev/sdb'				
Size	80 Gib	165 GiB				
Jenis Volume	gp3	gp3				
IOPS	3000	3000				

Pengaturan Default	Volume Akar AMI	Volume 2 Cache				
Hapus saat pengakhiran	Ya	Ya				
Dienkripsi	Tidak	Tidak				
Throughput	125	125				

Menerapkan host Amazon EC2 yang disesuaikan untuk S3 File Gateway

Anda dapat menerapkan dan mengaktifkan Amazon S3 File Gateway Amazon FSx File Gateway Elastic Compute Cloud (Amazon EC2). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai komunitas AMI.

> **Note**
>
> AMI komunitas Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.
> S3 File Gateway Gateway AMI menggunakan konvensi penamaan berikut. Nomor versi yang ditambahkan ke nama AMI berubah dengan setiap rilis versi.
> `aws-storage-gateway-FILE_S3-1.25.0`

Untuk menerapkan instans Amazon EC2 untuk meng-host Gateway File Amazon S3 Anda

1. Mulai menyiapkan gateway baru menggunakan konsol Storage Gateway. Untuk petunjuk, lihat Menyiapkan Gateway File Amazon S3 Mengatur Gateway File . Saat Anda mencapai bagian Opsi platform, pilih Amazon EC2 sebagai platform Host, lalu gunakan langkah-langkah berikut untuk meluncurkan instans Amazon EC2 yang akan meng-host File Gateway Anda.
2. Pilih Launch instance untuk membuka template AWS Storage Gateway AMI di konsol Amazon EC2, tempat Anda dapat mengonfigurasi pengaturan tambahan.

   Gunakan Quicklaunch untuk meluncurkan instans Amazon EC2 dengan pengaturan default.

3. Untuk Nama, masukkan nama untuk instans Amazon EC2. Setelah instance di-deploy, Anda dapat mencari nama ini untuk menemukan instance Anda di halaman daftar di konsol Amazon EC2.
4. Di bagian Jenis instans, untuk tipe Instance, pilih konfigurasi perangkat keras untuk instans Anda. Konfigurasi perangkat keras harus memenuhi persyaratan minimum tertentu untuk mendukung gateway Anda. Sebaiknya mulai dengan tipe instans m5.xlarge, yang memenuhi persyaratan perangkat keras minimum agar gateway Anda berfungsi dengan baik. Untuk informasi selengkapnya, lihat Persyaratan untuk jenis instans Amazon EC2.

   Anda dapat mengubah ukuran instans Anda setelah meluncurkan, jika perlu. Untuk informasi selengkapnya, lihat Mengubah ukuran instans Anda di Panduan Pengguna Amazon EC2.

   > **Note**
   >
   > Jenis instans tertentu, terutama i3 EC2, menggunakan disk SSD NVMe. Ini dapat menyebabkan masalah ketika Anda memulai atau menghentikan File 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 EC2 Anda. Untuk informasi selengkapnya, lihat Cara kerja Amazon VPC di Panduan Pengguna Amazon Virtual Private Cloud.

   b. (Opsional) Untuk Subnet, pilih subnet tempat Anda ingin meluncurkan instans Amazon EC2 Anda.

   c. Untuk IP Auto-assign Publik, pilih Aktifkan.
7. Di subbagian Firewall (grup keamanan), tinjau pengaturan yang telah dikonfigurasi sebelumnya. Anda dapat mengubah nama default dan deskripsi grup keamanan baru yang akan dibuat untuk

instans Amazon EC2 Anda jika Anda mau, atau memilih untuk menerapkan aturan firewall dari grup keamanan yang ada.

8. Dalam subbagian aturan grup keamanan masuk, tambahkan aturan firewall untuk membuka port yang akan digunakan klien untuk terhubung ke instans Anda. Untuk informasi selengkapnya tentang menambahkan aturan firewall, lihat Aturan grup keamanan di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

> **Note**
>
> Amazon S3 File Gateway mengharuskan port TCP 80 terbuka untuk lalu lintas masuk dan akses HTTP satu kali selama aktivasi gateway. Setelah aktivasi, Anda dapat menutup port ini.
> Jika Anda berencana untuk membuat berbagi file NFS, Anda harus membuka TCP/UDP port 2049 untuk akses NFS, port 111 untuk akses NFSv3, dan TCP/UDP port 20048 untuk akses NFSv3. TCP/UDP
> Jika Anda berencana untuk membuat berbagi file SMB, Anda harus membuka port TCP 445 untuk akses SMB.

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 150 GiB kapasitas untuk penyimpanan cache selain volume Root yang telah dikonfigurasi sebelumnya. Untuk meningkatkan kinerja, kami sarankan mengalokasikan beberapa volume EBS untuk penyimpanan cache dengan masing-masing setidaknya 150 GiB.

11. Di bagian Detail lanjutan, tinjau pengaturan yang telah dikonfigurasi sebelumnya dan buat perubahan jika perlu.
12. Pilih Luncurkan instans untuk meluncurkan instans gateway Amazon EC2 baru Anda dengan pengaturan yang dikonfigurasi.
13. Untuk memverifikasi bahwa instans baru berhasil diluncurkan, buka halaman Instans di konsol Amazon EC2 dan cari instans baru berdasarkan nama. Pastikan bahwa status Instance

menampilkan Berjalan dengan tanda centang hijau, dan pemeriksaan Status selesai, dan menunjukkan tanda centang hijau.

14. Pilih contoh Anda dari halaman detail. Salin alamat IP Publik dari bagian Ringkasan instans, lalu kembali ke halaman Mengatur gateway di konsol Storage Gateway untuk melanjutkan pengaturan Amazon S3 File Gateway Amazon File Gateway.

Anda dapat menentukan ID AMI yang akan digunakan untuk meluncurkan File Gateway 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 Menyiapkan Gateway File Amazon S3 Mengatur Gateway File . Saat Anda mencapai bagian Opsi platform, pilih Amazon EC2 sebagai platform Host, lalu pilih Launch instance untuk membuka template AWS Storage Gateway AMI di konsol Amazon EC2.

  Anda diarahkan ke halaman AMI komunitas EC2, di mana Anda dapat melihat ID AMI untuk AWS Wilayah Anda di URL.
- Kueri penyimpanan parameter Systems Manager. Anda dapat menggunakan AWS CLI atau Storage Gateway API untuk menanyakan parameter publik Systems Manager di bawah namespace `/aws/service/storagegateway/ami/FILE_S3/latest`. Misalnya, menggunakan perintah CLI berikut mengembalikan ID AMI saat ini di yang Wilayah AWS Anda tentukan.

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  FILE_S3/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/
  FILE_S3/latest",
          "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
          "Value": "ami-123c45dd67d891000"
  ```

```
    }
}
```

Ubah opsi metadata instans Amazon EC2

Layanan metadata instance (IMDS) adalah komponen on-instance yang menyediakan akses aman ke metadata instans Amazon EC2. Sebuah instance dapat dikonfigurasi untuk menerima permintaan metadata masuk yang menggunakan IMDS Versi 1 (IMDSv1) atau mengharuskan semua permintaan metadata menggunakan IMDS Versi 2 (IMDSv2). IMDSv2 menggunakan permintaan berorientasi sesi dan mengurangi beberapa jenis kerentanan yang dapat digunakan untuk mencoba mengakses IMDS. Untuk informasi tentang IMDSv2, lihat Cara Kerja Layanan Metadata Instans Versi 2 di Panduan Pengguna Amazon Elastic Compute Cloud.

Sebaiknya Anda memerlukan IMDSv2 untuk semua instans Amazon EC2 yang menghosting Storage Gateway. IMDSv2 diperlukan secara default pada semua instance gateway yang baru diluncurkan. Jika Anda memiliki instans yang masih dikonfigurasi untuk menerima permintaan metadata IMDSv1, lihat Memerlukan penggunaan IMDSv2 di Panduan Pengguna Amazon Elastic Compute Cloud untuk petunjuk mengubah opsi metadata instans Anda agar memerlukan penggunaan IMDSv2. Menerapkan perubahan ini tidak memerlukan reboot instance.

Sinkronisasi waktu VM dengan Hyper-V atau waktu host Linux KVM

Untuk gateway yang digunakan pada 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 Hyper-V lokal Microsoft, lihatAkses 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 Alat VMware 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 adapter jaringan untuk gateway Anda

Storage Gateway menggunakan adaptor jaringan VMXNET3 (10 GbE) tunggal secara default, tetapi Anda dapat mengonfigurasi gateway Anda untuk menggunakan lebih dari satu adaptor jaringan sehingga dapat diakses oleh beberapa 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 berbagi file dan inisiator yang terhubung ke mereka dalam jaringan yang terisolasi. Jaringan ini berbeda dari jaringan tempat gateway berkomunikasi AWS.

Dalam kasus penggunaan multi-adaptor yang khas, satu adaptor dikonfigurasi sebagai rute yang digunakan gateway untuk berkomunikasi AWS (yaitu, sebagai gateway default). Kecuali untuk adaptor yang satu ini, inisiator harus berada di subnet yang sama dengan adaptor yang berisi berbagi file yang mereka sambungkan. Jika tidak, komunikasi dengan target yang dituju mungkin tidak mungkin dilakukan. Jika target dikonfigurasi pada adaptor yang sama yang digunakan untuk komunikasi dengan AWS, lalu lintas berbagi file untuk target dan AWS lalu lintas mengalir melalui adaptor yang sama.

Dalam beberapa kasus, Anda mungkin mengonfigurasi satu adaptor untuk terhubung ke konsol Storage Gateway dan kemudian menambahkan adaptor kedua. Dalam kasus seperti itu, Storage Gateway secara otomatis mengkonfigurasi tabel rute untuk menggunakan adaptor kedua sebagai rute pilihan. Untuk petunjuk tentang cara mengkonfigurasi beberapa adaptor, lihat topik berikut:

Topik

- Mengkonfigurasi Gateway Anda untuk Beberapa NIC pada Host VMware ESXi
- Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Microsoft Host Hyper-V

Mengkonfigurasi Gateway Anda untuk Beberapa NIC pada Host VMware ESXi

Prosedur berikut mengasumsikan bahwa VM gateway Anda sudah memiliki satu adaptor jaringan yang ditentukan, dan menjelaskan cara menambahkan adaptor pada VMware ESXi.

Untuk mengkonfigurasi gateway Anda untuk menggunakan adaptor jaringan tambahan di host VMware ESXi

1. Matikan pintu gerbangnya.
2. Di klien VMware vSphere, pilih VM gateway Anda.

VM dapat tetap dihidupkan untuk prosedur ini.

3. Di klien, buka menu konteks (klik kanan) untuk VM gateway Anda, dan pilih Edit Pengaturan.
4. Pada tab Hardware pada kotak dialog Virtual Machine Properties, pilih Tambah untuk menambahkan perangkat.
5. Ikuti panduan Add Hardware untuk menambahkan adaptor jaringan.

   a. Di panel Jenis Perangkat, pilih Adaptor Ethernet untuk menambahkan adaptor, lalu pilih Berikutnya.

   b. Di panel Network Type, pastikan Connect at power on dipilih untuk Type, lalu pilih Next.

      Kami menyarankan Anda menggunakan adaptor jaringan VMXNET3 dengan Storage Gateway. Untuk informasi selengkapnya tentang jenis adaptor yang mungkin muncul di daftar adaptor, lihat Jenis Adaptor Jaringan di Dokumentasi Server ESXi dan vCenter.

   c. Di panel Siap Selesai, tinjau informasinya, lalu pilih Selesai.
6. Pilih tab Ringkasan untuk VM, dan pilih Lihat Semua di sebelah kotak Alamat IP. Jendela Alamat IP Mesin Virtual menampilkan semua alamat IP yang dapat Anda gunakan untuk mengakses gateway. Konfirmasikan bahwa alamat IP kedua terdaftar untuk gateway.

   > **Note**
   >
   > Mungkin perlu beberapa saat agar perubahan adaptor diterapkan dan informasi ringkasan VM disegarkan.

7. Di konsol Storage Gateway, nyalakan gateway.
8. Di panel Navigasi konsol Storage Gateway, pilih Gateways dan pilih gateway tempat Anda menambahkan adaptor. Konfirmasikan bahwa alamat IP kedua tercantum di tab Detail.

   > **Note**
   >
   > Contoh perintah pemasangan yang disediakan pada halaman info untuk berbagi file di konsol Storage Gateway akan selalu menyertakan alamat IP adaptor jaringan yang terbaru ditambahkan ke gateway terkait berbagi file.

Untuk informasi tentang tugas konsol lokal yang umum untuk VMware,, dan host KVM Hyper-V, lihat Melakukan tugas pada konsol lokal mesin virtual

Mengkonfigurasi Gateway Anda untuk Beberapa NIC di Microsoft Host 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 Hyper-V host Microsoft.

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. Right-click nama gateway VM 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.

> **Note**
>
> Contoh perintah pemasangan yang disediakan pada halaman info untuk berbagi file di konsol Storage Gateway akan selalu menyertakan alamat IP adaptor jaringan yang terbaru ditambahkan ke gateway terkait berbagi file.

Untuk informasi tentang tugas konsol lokal yang umum untuk VMware,, dan host KVM Hyper-V, lihat Melakukan tugas pada konsol lokal mesin virtual

Menggunakan VMware vSphere Ketersediaan Tinggi dengan Storage Gateway

Storage Gateway menyediakan ketersediaan tinggi pada VMware melalui serangkaian pemeriksaan kesehatan tingkat aplikasi yang terintegrasi dengan VMware vSphere High Availability (VMware HA). Pendekatan ini membantu melindungi beban kerja penyimpanan terhadap kegagalan perangkat keras, hypervisor, atau jaringan. Ini juga membantu melindungi terhadap kesalahan perangkat lunak, seperti batas waktu koneksi dan berbagi file atau tidak tersedianya volume.

Dengan integrasi ini, gateway yang digunakan di lingkungan VMware lokal atau di VMware Cloud AWS secara otomatis pulih dari sebagian besar gangguan layanan. Hal ini umumnya dilakukan dalam waktu kurang dari 60 detik tanpa kehilangan data.

> **Note**
>
> Sebaiknya lakukan hal-hal berikut jika Anda menerapkan Storage Gateway di cluster VMware HA:
>
> - Menerapkan paket download VMware ESX .ova yang berisi VM Storage Gateway hanya pada satu host dalam sebuah cluster.
> - Saat menerapkan paket.ova, 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.
> - Dengan pengelompokan, jika Anda menerapkan paket.ova 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 cluster VMware HA:

Topik

- Aktifkan Gateway Anda
- Uji Konfigurasi Ketersediaan Tinggi VMware Anda

Konfigurasikan Cluster VSphere VMware HA Anda

Pertama, jika Anda belum membuat cluster VMware, buat satu. Untuk informasi tentang cara membuat cluster VMware, lihat Membuat Cluster VSphere HA di dokumentasi VMware.

Selanjutnya, konfigurasikan cluster VMware Anda untuk bekerja dengan Storage Gateway.

Untuk mengkonfigurasi cluster VMware Anda

1. Pada halaman Edit Pengaturan Cluster di VMware vSphere, pastikan bahwa pemantauan VM dikonfigurasi untuk VM dan pemantauan aplikasi. Untuk melakukannya, atur nilai berikut untuk setiap opsi:

   - Respon Kegagalan Host: Mulai Ulang VM
   - Respons untuk Isolasi Host: Matikan dan restart VM
   - Datastore dengan PDL: Dinonaktifkan
   - Datastore dengan APD: Dinonaktifkan
   - Pemantauan VM: VM dan Pemantauan Aplikasi
2. Fine-tune sensitivitas cluster dengan menyesuaikan nilai-nilai berikut:

   - Interval kegagalan — Setelah interval ini, VM dimulai ulang jika detak jantung VM tidak diterima.
   - Waktu aktif minimum - Cluster menunggu selama ini setelah VM mulai memantau detak jantung alat VM.
   - Reset per-VM maksimum - Cluster me-restart VM maksimal ini berkali-kali dalam jendela waktu reset maksimum.
   - Jendela waktu reset maksimum — Jendela waktu untuk menghitung reset maksimum per VM reset.

   Jika Anda tidak yakin nilai apa yang akan ditetapkan, gunakan contoh pengaturan ini:

   - Interval kegagalan: **30** detik
   - Waktu aktif minimum: detik **120**

- Reset per-VM maksimum: **3**
- Jendela waktu reset maksimum: jam **1**

Jika Anda memiliki VM lain yang berjalan di cluster, Anda mungkin ingin menetapkan nilai-nilai ini secara khusus untuk VM Anda. Anda tidak dapat melakukan ini sampai Anda menerapkan VM dari .ova. Untuk informasi selengkapnya tentang menyetel nilai-nilai ini, lihat(Opsional) Tambahkan Opsi Override untuk VM Lain di Cluster Anda.

Siapkan Jenis Gateway Anda

Gunakan prosedur berikut untuk mengatur gateway

Untuk mengunduh gambar.ova untuk jenis gateway Anda

- Unduh gambar.ova untuk jenis gateway Anda dari salah satu dari berikut ini:
  - Gerbang Berkas — Membuat dan mengaktifkan Gateway File Amazon S3

Menyebarkan Gateway

Di cluster Anda yang dikonfigurasi, terapkan gambar.ova ke salah satu host cluster. Untuk petunjuk, lihat Menerapkan Template OVF atau OVA di dokumentasi online VMware vSphere.

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.

(Opsional) Tambahkan Opsi Override untuk VM Lain di Cluster Anda

Jika Anda memiliki VM lain yang berjalan di cluster Anda, Anda mungkin ingin mengatur nilai cluster secara khusus untuk setiap VM. Untuk petunjuk, lihat Menyesuaikan Mesin Virtual Individu dalam dokumentasi online VMware vSphere.

Untuk menambahkan opsi penggantian untuk VM lain 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 di-deploy di lingkungan VMware Anda, aktifkan gateway Anda menggunakan konsol Storage Gateway. Untuk petunjuknya, lihat Meninjau pengaturan dan mengaktifkan pengaturan Tinjauan Gateway File Amazon S3 Anda.

Uji Konfigurasi Ketersediaan Tinggi VMware Anda

Setelah Anda mengaktifkan gateway Anda, uji konfigurasi Anda.

Untuk menguji konfigurasi HA VMware Anda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.
2. Pada panel navigasi, pilih Gateways, lalu pilih gateway yang ingin Anda uji untuk VMware HA.
3. Untuk Tindakan, pilih Verifikasi VMware HA.
4. Di kotak Verifikasi Konfigurasi Ketersediaan Tinggi VMware yang muncul, pilih OK.

> **Note**
>
> Menguji konfigurasi VMware HA Anda me-reboot VM gateway Anda dan mengganggu konektivitas ke gateway Anda. Tes mungkin memakan waktu beberapa menit untuk menyelesaikannya.

Jika tes berhasil, status Verified muncul di tab detail gateway di konsol.

5. Pilih Keluar.

Anda dapat menemukan informasi tentang peristiwa VMware HA di grup CloudWatch log Amazon. Untuk informasi selengkapnya, lihat Mendapatkan log kesehatan S3 FSx File Gateway dengan grup CloudWatch log.

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**
>
> AWS Storage Gateway Hardware Appliance, template gambar VM, dan Amazon EC2 Amazon Machine Images (AMI) telah dikonfigurasi sebelumnya dengan layanan HTTP yang diperlukan untuk menerima dan menanggapi permintaan web yang dijelaskan di halaman ini. Tidak diperlukan atau disarankan untuk menginstal layanan tambahan apa pun di gateway Anda.

Topik

Linux (ikal)

Contoh berikut menunjukkan cara mendapatkan kunci aktivasi menggunakan Linux (curl).

> **Note**
>
> Ganti variabel yang disorot dengan nilai aktual untuk gateway Anda. Nilai yang dapat diterima adalah sebagai berikut:
>
> - *`gateway_ip_address`*- Alamat IPv4 gateway Anda, misalnya `172.31.29.201`
> - *`gateway_type`*- Jenis gateway yang ingin Anda aktifkan, seperti`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. `us-east-1`
> - *`vpc_endpoint`*- Nama titik akhir VPC untuk gateway Anda, misalnya. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Titik akhir publik

Untuk mendapatkan kunci aktivasi untuk titik akhir publik, gunakan salah satu perintah berikut:

Titik akhir standar

Untuk mendapatkan kunci aktivasi untuk titik akhir standar:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Dual-stack titik akhir

Untuk mendapatkan kunci aktivasi untuk titik akhir dual-stack:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

Titik akhir FIPS

Untuk mendapatkan kunci aktivasi untuk titik akhir FIPS:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

Titik akhir VPC

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.

Gateway berbasis Amazon Linux 2 (AL2)

Anda dapat memilih titik akhir standar atau FIPS untuk gateway berdasarkan AL2.

> **Note**
>
> Titik akhir FIPS tidak tersedia di semua. Wilayah AWS Untuk informasi selengkapnya, lihat Titik Akhir FIPS menurut Layanan.

Untuk mendapatkan kunci aktivasi untuk AL2-based gateway Anda dari konsol lokal Anda

1. Masuk ke konsol lokal Anda sebagai admin.
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, pilih `0` untuk memilih Dapatkan tombol aktivasi.
3. Pilih Storage Gateway untuk opsi keluarga gateway.
4. Masukkan AWS Wilayah tempat Anda ingin mengaktifkan gateway Anda.
5. Untuk jenis jaringan, masukkan 1 untuk Publik atau 2 untuk VPC.
6. Untuk tipe endpoint, masukkan 1 Standard atau 2 Federal Information Processing Standard (FIPS).

Gateway berbasis Amazon Linux 2023 (AL2023)

Untuk gateway berdasarkan AL2023, titik akhir berikut tersedia:

- Titik akhir standar (hanya mendukung IPv4)
- Titik akhir FIPS (hanya mendukung IPv4)
- Dual-stack titik akhir (mendukung IPv4 dan IPv6)
- Dual-stack Titik akhir FIPS (mendukung IPv4 dan IPv6)

Untuk informasi selengkapnya, lihat Jenis titik akhir.

Untuk mendapatkan kunci aktivasi untuk AL2023-based gateway Anda dari konsol lokal Anda

1. Masuk ke konsol lokal Anda. Jika Anda terhubung ke instans Amazon EC2 dari komputer Windows, masuk sebagai admin.
2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, pilih `0` untuk memilih Dapatkan tombol aktivasi.
3. Pilih Storage Gateway untuk opsi keluarga gateway.
4. Masukkan AWS Wilayah tempat Anda ingin mengaktifkan gateway Anda.
5. Untuk jenis jaringan, masukkan 1 untuk Publik atau 2 untuk titik akhir VPC.
6. Untuk Pilih tipe titik akhir, Aktifkan FIPS? , masukkan Y untuk mengaktifkan FIPS atau menggunakan titik N akhir non-FIPS.
7. Untuk tipe endpoint, masukkan 1 untuk endpoint standar atau 2 untuk dual-stack endpoint.

    - Untuk titik akhir dual-stack, untuk versi Select IP atau exit:, masukkan 1 untuk IPv4 atau IPv6. 2

Support untuk atribut file di Amazon S3 File Gateway

Amazon S3 File Gateway mendukung atribut file DOS atau Windows secara default. Menggunakan S3 File Gateway, Anda dapat menyimpan data file dan metadata serta memperbarui setelan — seperti menandai item sebagai diarsipkan saat ditempatkan di Amazon S3. Untuk informasi selengkapnya tentang atribut file DOS dan Windows, lihat artikel Konstanta Atribut File di situs web dokumentasi pengembangan aplikasi Windows.

S3 File Gateway mendukung atribut berikut:

- ReadOnly— Gateway File S3 mencegah perubahan pada file yang memiliki ReadOnly atribut yang ditetapkan.
- Arsip — Gateway File S3 menetapkan atribut ini ketika file pertama kali ditambahkan ke gateway.

> **Note**
>
> Aplikasi Backup biasanya backup file yang memiliki bit Archive diatur dan kemudian menghapus bit setelah backup berhasil.

- Tersembunyi - Server Message Block (SMB) klien menyembunyikan file yang menggunakan bit set ini.

- Sistem - Atribut ini tetap ada setelah Anda mengaturnya.

Saat Anda menyalin file ke S3 File Gateway dengan atribut yang disetel, atribut DOS atau Windows file disimpan di S3 File Gateway dan di Amazon S3. Anda dapat memperbarui atribut ini untuk file di gateway, dan pembaruan tersebut juga berlaku untuk objek di Amazon S3. Jika file dikeluarkan dari gateway, gateway akan menarik file, metadatanya, dan atribut persistennya dari Amazon S3 saat Anda meminta.

> **Note**
>
> Atribut DOS hanya didukung pada saham SMB dan jika akses dikendalikan oleh Daftar Kontrol Akses Windows.

Penggunaan Direct Connect dengan Storage Gateway

Direct Connect menghubungkan jaringan internal Anda ke Amazon Web Services Cloud. 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 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 Direct Connect lokasi, atau dapat berada di AWS Wilayah yang berbeda.

Ilustrasi berikut menunjukkan contoh cara 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 menggunakan 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 Direct Connect di Panduan Direct Connect Pengguna.
2. Hubungkan alat Storage Gateway lokal Anda ke Direct Connect router.

3. Buat antarmuka virtual publik, dan konfigurasikan router lokal Anda sesuai dengan itu. Untuk informasi selengkapnya, lihat Membuat Antarmuka Virtual di Panduan Direct Connect Pengguna.

Untuk detailnya Direct Connect, lihat Apa itu Direct Connect? dalam Direct Connect User Guide.

Persyaratan izin akun layanan Active Directory

Jika Anda berencana untuk menggunakan direktori Microsoft Active untuk memberikan akses terautentikasi pengguna ke di Anda AWS Storage Gateway, Anda perlu memastikan bahwa Anda memiliki akun layanan Direktori Aktif, dan bahwa akun layanan telah mendelegasikan izin untuk bergabung dengan komputer ke domain Anda. Akun layanan adalah akun pengguna Active Directory yang telah didelegasikan izin untuk melakukan tugas-tugas tertentu. Anda memberikan kredensi nama pengguna dan kata sandi untuk akun ini saat Anda bergabung dengan Storage Gateway ke domain Active Directory Anda.

Akun layanan Active Directory harus didelegasikan izin berikut di OU tempat Anda bergabung dengan gateway Anda:

- Kemampuan untuk membuat dan menghapus objek komputer
- Kemampuan untuk mengatur ulang kata sandi
- Kemampuan untuk memodifikasi izin
- Kemampuan untuk membatasi akun dari membaca dan menulis data
- Kemampuan tervalidasi untuk membaca dan menulis Pembatasan Akun
- Kemampuan tervalidasi untuk menulis ke nama prinsipal layanan
- Kemampuan tervalidasi untuk menulis ke nama host DNS

Ini mewakili serangkaian izin minimum yang diperlukan untuk menggabungkan objek komputer ke Direktori Aktif Anda. Untuk informasi selengkapnya, lihat topik dokumentasi Microsoft Windows Server Galat: Akses ditolak ketika pengguna non-administrator yang telah didelegasikan kontrol mencoba untuk menggabungkan komputer ke kontroler domain.

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 gateway Amazon EC2, Anda juga bisa mendapatkan alamat IP instans Amazon EC2 dari Amazon EC2 Management Console. Untuk mengetahui cara mendapatkan alamat IP gateway Anda, lihat salah satu dari berikut ini:

- Host VMware: Mengakses Konsol Lokal Gateway dengan VMware ESXi
- Host HyperV: Akses Konsol Lokal Gateway dengan Microsoft Hyper-V
- Host Mesin Kernel-based Virtual Linux (KVM): Mengakses Konsol Lokal Gateway dengan Linux KVM
- Tuan rumah EC2: Mendapatkan Alamat IP dari Host Amazon EC2

Ketika Anda menemukan alamat IP, perhatikan itu. Kemudian kembali ke konsol Storage Gateway dan ketik alamat IP ke konsol.

Mendapatkan Alamat IP dari Host Amazon EC2

Untuk mendapatkan alamat IP instans Amazon EC2 gateway Anda digunakan, masuk ke konsol lokal instans EC2. Kemudian dapatkan alamat IP dari bagian atas halaman konsol. Untuk petunjuk, lihat .

Anda juga bisa mendapatkan alamat IP dari Amazon EC2 Management Console. Kami merekomendasikan menggunakan alamat IP publik untuk aktivasi. Untuk mendapatkan alamat IP publik, gunakan prosedur 1. Jika Anda memilih untuk menggunakan alamat IP elastis sebagai gantinya, lihat prosedur 2.

Prosedur 1: Untuk terhubung ke gateway Anda menggunakan alamat IP publik

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih instans EC2 tempat gateway Anda digunakan.
3. Pilih tab Deskripsi di bagian bawah, lalu catat IP publik. Anda menggunakan alamat IP ini untuk terhubung ke gateway. Kembali ke konsol Storage Gateway dan ketik alamat IP.

Jika Anda ingin menggunakan alamat IP elastis untuk aktivasi, gunakan prosedur berikut.

Prosedur 2: Untuk terhubung ke gateway Anda menggunakan alamat IP elastis

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih instans EC2 tempat gateway Anda digunakan.
3. Pilih tab Deskripsi di bagian bawah, dan kemudian perhatikan nilai IP Elastis. Anda menggunakan alamat IP elastis ini untuk terhubung ke gateway. Kembali ke konsol Storage Gateway dan ketik alamat IP elastis.

Dukungan IPv6

Dukungan IPv6 hanya tersedia pada perangkat gateway versi 2.x atau lebih tinggi. Gateway appliance versi 1.x tidak dapat diperbarui ke versi 2.x. Anda harus memigrasi atau mengganti alat gateway versi 1.x untuk mendapatkan dukungan IPv6.

Titik akhir dual-stack berikut diperlukan untuk IPv6.

```
storagegateway.region.api.aws:443
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
s3.dualstack.region.amazonaws.com
```

Memahami sumber daya Storage Gateway dan ID sumber daya

Di Storage Gateway, sumber daya utama adalah gateway tetapi jenis sumber daya lainnya adalah berbagi file. Berbagi file disebut sebagai subresource dan mereka tidak ada kecuali mereka terkait dengan gateway.

Sumber daya dan subsumber daya ini memiliki Nama Sumber Daya Amazon (ARN) unik yang terkait dengannya seperti yang ditunjukkan dalam tabel ini.

Jenis Sumber Daya	Format ARN
Gerbang ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`*` :gateway/` *`gateway-id`*

Jenis Sumber Daya	Format ARN
Berbagi File ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

Bekerja dengan ID Sumber Daya

Saat Anda membuat sumber daya, Storage Gateway menetapkan sumber daya ID sumber daya unik. ID sumber daya ini adalah bagian dari sumber daya ARN. ID sumber daya mengambil bentuk pengenal sumber daya, diikuti oleh tanda hubung, dan kombinasi unik dari delapan huruf dan angka. Misalnya, ID gateway adalah bentuk `sgw-12A3456B` di mana `sgw` adalah pengenal sumber daya untuk gateway.

ID sumber daya Storage Gateway berada dalam huruf besar. Namun, jika Anda menggunakan ID sumber daya ini dengan Amazon EC2 API, Amazon EC2 mengharapkan ID sumber daya dalam huruf kecil. Anda harus mengubah ID sumber daya Anda menjadi huruf kecil untuk menggunakannya dengan EC2 API. Misalnya, di Storage Gateway ID untuk gateway mungkin`sgw-12A3456B`. Jika Anda menggunakan ID ini dengan EC2 API, Anda harus mengubahnya menjadi`sgw-12a3456b`. Jika tidak, API EC2 mungkin tidak berperilaku seperti yang diharapkan.

Menandai sumber daya Storage Gateway

Di Storage Gateway, Anda dapat menggunakan tag untuk mengelola sumber daya Anda. Tanda memungkinkan Anda menambahkan metadata ke sumber daya Anda dan mengategorikan sumber daya Anda untuk membuatnya 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 kaset 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.

Untuk File Gateway, Anda dapat menggunakan tag untuk mengontrol akses ke sumber daya. Untuk informasi tentang cara melakukan ini, lihat Menggunakan tag untuk mengontrol akses ke gateway dan sumber daya Anda.

Tag tidak memiliki arti semantik melainkan ditafsirkan sebagai string karakter.

Batasan berikut ini berlaku untuk tag:

- Kunci dan nilai tag peka terhadap huruf besar dan kecil.
- Jumlah maksimum tag untuk setiap sumber daya adalah 50.
- Kunci tag tidak dapat dimulai dengan`aws:`. Awalan ini dicadangkan untuk penggunaan AWS .
- Karakter yang valid untuk properti kunci adalah UTF-8 huruf dan angka, spasi, dan karakter khusus + - =. _:/dan @.

Bekerja dengan tag

Anda dapat bekerja dengan tag dengan menggunakan konsol Storage Gateway, Storage Gateway API, atau Storage Gateway Command Line Interface (CLI). Prosedur berikut menunjukkan cara menambahkan, mengedit, dan menghapus tag di konsol.

Untuk menambahkan tag

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.
2. Di panel navigasi, pilih sumber daya yang ingin Anda tag.

   Misalnya, untuk menandai gateway, pilih Gateway, lalu pilih gateway yang ingin Anda tag dari daftar gateway.
3. Pilih Tag, lalu pilih Add/edittag.
4. Di kotak dialog Add/edit tag, pilih Buat tag.
5. Ketik kunci untuk Key dan nilai untuk Value. Misalnya, Anda dapat mengetik **`Department`** kunci dan **`Accounting`** nilainya.

> **Note**
>
> Anda dapat membiarkan kotak Nilai kosong.

6. Pilih Buat Tag untuk menambahkan lebih banyak tag. Anda dapat menambahkan beberapa tag ke sumber daya.
7. Setelah selesai menambahkan tag, pilih Simpan.

Untuk mengedit tag

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.
2. Pilih sumber daya yang tagnya ingin Anda edit.
3. Pilih Tag untuk membuka kotak dialog Add/edittag.
4. Pilih ikon pensil di sebelah tag yang ingin Anda edit, lalu edit tag.
5. Setelah selesai mengedit tag, pilih Simpan.

Untuk menghapus tanda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/home.
2. Pilih sumber daya yang tagnya ingin Anda hapus.
3. Pilih Tag, lalu pilih Add/edittag untuk membuka kotak dialog Add/edit tag.
4. Pilih ikon X di sebelah tag yang ingin Anda hapus, lalu pilih Simpan.

Bekerja dengan komponen sumber terbuka untuk AWS Storage Gateway

Bagian ini menjelaskan alat dan lisensi pihak ketiga yang kami andalkan untuk memberikan AWS Storage Gateway fungsionalitas.

Topik

- Open-source komponen untuk Storage Gateway
- Open-source komponen untuk Amazon S3 File Gateway

Open-source komponen untuk Storage Gateway

Beberapa alat dan lisensi pihak ketiga digunakan untuk memberikan fungsionalitas untuk Volume Gateway, Tape Gateway, dan Amazon S3 File Gateway.

Gunakan tautan berikut untuk mengunduh kode sumber untuk komponen perangkat lunak sumber terbuka tertentu yang disertakan dengan AWS Storage Gateway perangkat lunak:

- Untuk peralatan Storage Gateway yang digunakan di VMware ESXi: sources.tar
- Untuk peralatan Storage Gateway yang digunakan di Microsoft Hyper-V: sources_hyperv.tar
- Untuk peralatan Storage Gateway yang digunakan di Linux Kernel-based Virtual Machine (KVM): sumber_ 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 Third-Party Lisensi.

Open-source komponen untuk Amazon S3 File Gateway

Beberapa alat dan lisensi pihak ketiga digunakan untuk memberikan fungsionalitas Amazon S3 File Gateway (S3 File Gateway).

Gunakan tautan berikut untuk mengunduh kode sumber untuk komponen perangkat lunak sumber terbuka tertentu yang disertakan dengan perangkat lunak S3 File Gateway:

- Untuk Gerbang File Amazon S3: sgw-file-s3-open-source.tgz

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 Third-Party Lisensi.

Batas dan kuota untuk Gateway File Amazon S3

Kuota untuk berbagi file

Tabel berikut mencantumkan kuota untuk berbagi file.

Deskripsi	Kuota
Jumlah maksimum pembagian file per gateway **Note** Setiap berbagi file hanya dapat terhubung ke satu bucket S3, tetapi beberapa berbagi file dapat terhubung ke bucket yang sama. Jika Anda menghubungkan lebih dari satu file share ke bucket yang sama, Anda harus mengonfigurasi setiap file share untuk menggunakan nama awalan yang unik dan tidak tumpang tindih untuk mencegah konflik. read/write Jumlah berbagi file yang dikelola oleh gateway dapat memengaruhi kinerja gateway. Untuk informasi selengkap nya, lihat Panduan kinerja untuk gateway dengan beberapa berbagi file.	50
Jumlah maksimum file yang gateway dapat secara bersamaan cache metadata **Note** Karena S3 File Gateway didukung oleh Amazon S3, tidak ada ukuran folder maksimum atau batasan jumlah file yang dapat Anda simpan atau akses menggunakan gateway. Setiap gateway memiliki batas yang dapat dikonfigurasi yang menentukan jumlah file yang dapat secara bersamaan cache metadata. Anda dapat menggunak	Kapasitas gerbang: Kecil - file 5M Sedang - File 10M Besar - File 20M

Deskripsi	Kuota
an tindakan UpdateGatewayInformationAPI untuk menyetel GatewayCapacitykeSmall,Medium, atauLarge. Pengaturan ini memengaruhi kinerja gateway dan rekomendasi perangkat keras. Untuk informasi selengkapnya, lihat Panduan kinerja untuk gateway dengan beberapa berbagi file.	
Ukuran maksimum file individual **Note** Jika Anda mencoba menulis file yang lebih besar dari batas ukuran sepotong demi sepotong, hanya 5 TiB pertama yang akan diunggah. Jika Anda mencoba menulis file yang lebih besar dari batas ukuran sekaligus, pada klien Windows tidak ada file yang dibuat dan pada klien Linux file ukuran nol dibuat.	5 TiB

Deskripsi	Kuota
Panjang jalur maksimum **Note** Klien tidak diizinkan untuk membuat jalur yang melebihi panjang ini, dan hal itu menghasilkan kesalahan. Batas ini berlaku untuk kedua protokol yang didukung oleh File Gateways, NFS dan SMB. Panjang jalur dalam byte dihitung dari nilai bit karakter dalam UTF-8 pengkodean.	1024 byte
Panjang nama file maksimum **Note** File Gateway tidak mendukung nama file yang melebihi panjang ini. Panjang nama file dalam byte dihitung dari nilai bit karakter dalam UTF-8 pengkodean.	255 bita

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)
Gerbang File S3	150 GiB	64 TiB

> **Note**
>
> Anda dapat mengkonfigurasi satu atau lebih drive lokal untuk cache Anda hingga kapasitas maksimum.
> Saat menambahkan cache 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.

Menggunakan kelas penyimpanan

Amazon S3 File Gateway mendukung kelas penyimpanan Standar Amazon S3, Akses Amazon S3, Amazon S3 Zone-Infrequent One Standard-Infrequent Access, Amazon S3, dan kelas penyimpanan Intelligent-Tiering Amazon Glacier. Untuk informasi selengkapnya tentang kelas penyimpanan, lihat kelas penyimpanan Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

> **Note**
>
> S3 File Gateway saat ini tidak mendukung kelas penyimpanan Amazon S3 Glacier Instant Retrieval.

Topik

- Menggunakan kelas penyimpanan dengan File Gateway
- Menggunakan kelas penyimpanan GLACIER dengan File Gateway

Menggunakan kelas penyimpanan dengan File Gateway

Saat membuat atau memperbarui file share, Anda memiliki opsi untuk memilih kelas penyimpanan untuk objek Anda. Anda dapat memilih kelas penyimpanan Standar Amazon S3, atau salah satu kelas penyimpanan S3, S3 One Standard-IA Zone-IA, atau S3. Intelligent-Tiering Objek yang disimpan di salah satu kelas penyimpanan ini dapat dialihkan ke GLACIER menggunakan kebijakan siklus hidup.

Kelas penyimpanan Amazon S3	Pertimbangan-pertimbangan
Standar	Pilih Standar untuk menyimpan file yang sering diakses secara berlebihan di beberapa Availability Zone yang dipisahkan secara geografis. Ini adalah kelas penyimpanan default. Lihat harga Amazon S3 untuk detail selengkapnya.
S3 Intelligent-Tiering	Pilih Intelligent-Tiering untuk mengoptimalkan biaya penyimpanan dengan memindahkan data secara otomatis ke tingkat akses penyimpanan yang paling hemat biaya. Objek yang lebih kecil dari 128 KB tidak memenuhi syarat untuk tiering otomatis di kelas Intelligent-Tiering penyimpanan. Objek ini dibebankan pada tarif tingkat akses yang sering, dan tidak dikenakan biaya pemantauan yang dibebankan untuk objek berjenjang otomatis. S3 Intelligent-Tiering sekarang mendukung tingkat Akses Arsip dan tingkat Akses Arsip Dalam. S3 Intelligent-Tiering secara otomatis memindahkan objek yang belum diakses selama 90 hari ke tingkat Akses Arsip, dan setelah 180 hari tanpa diakses, ke tingkat Akses Arsip Dalam. Setiap kali objek di salah satu tingkatan akses arsip dipulihkan, objek pindah ke tingkat Akses Sering dalam beberapa jam dan siap untuk diambil. Ini menciptakan kesalahan batas waktu untuk pengguna atau aplikasi yang mencoba mengakses file melalui berbagi file jika objek hanya ada di salah satu dari dua tingkatan arsip. Jangan gunakan tingkatan arsip dengan S3 Intelligent-Tiering jika aplikasi Anda

Kelas penyimpanan Amazon S3	Pertimbangan-pertimbangan
	mengakses file melalui berbagi file yang disajikan oleh File Gateway. Ketika operasi file yang memperbarui metadata (seperti pemilik, stempel waktu, izin, dan ACL) dilakukan terhadap file yang dikelola oleh File Gateway, objek yang ada dihapus dan versi baru objek dibuat di kelas penyimpanan Amazon S3 ini. Validasi bagaimana operasi file memengaruhi pembuatan objek sebelum menggunakan kelas penyimpanan ini dalam produksi. Lihat harga Amazon S3 untuk detail selengkapnya.

Kelas penyimpanan Amazon S3	Pertimbangan-pertimbangan
S3 Standard-IA	Pilih Standard-IA untuk menyimpan file Anda yang jarang diakses secara berlebihan di beberapa Availability Zone yang terpisah secara geografis. Objek yang disimpan di kelas Standard-IA penyimpanan dapat dikenakan biaya tambahan untuk menimpa, menghapus, meminta, mengambil, atau mentransisikan objek antar kelas penyimpanan dalam waktu 30 hari. Ada durasi penyimpanan minimum 30 hari. Objek yang dihapus sebelum 30 hari dikenakan biaya pro-rated sama dengan biaya penyimpanan untuk hari-hari yang tersisa. Pertimbangkan seberapa sering objek ini berubah, berapa lama Anda berencana untuk menyimpan objek ini, dan seberapa sering Anda perlu mengaksesnya. Objek yang lebih kecil dari 128 KB dikenakan biaya 128 KB dan biaya penghapusan awal berlaku. Ketika operasi file yang memperbarui metadata (seperti pemilik, stempel waktu, izin, dan ACL) dilakukan terhadap file yang dikelola oleh File Gateway, objek yang ada dihapus dan versi baru objek dibuat di kelas penyimpan an Amazon S3 ini. Anda harus memvalida si bagaimana operasi file memengaruhi pembuatan objek sebelum menggunakan kelas penyimpanan ini dalam produksi karena biaya penghapusan awal berlaku. Lihat harga Amazon S3 untuk detail selengkapnya.

Kelas penyimpanan Amazon S3	Pertimbangan-pertimbangan
S3 Satu Zone-IA	Pilih Satu Zone-IA untuk menyimpan file yang jarang Anda akses dalam satu Availability Zone. Objek yang disimpan dalam kelas Satu Zone-IA penyimpanan dapat dikenakan biaya tambahan untuk menimpa, menghapus, meminta, mengambil, atau mentransisikan objek antara kelas penyimpanan dalam waktu 30 hari. Ada durasi penyimpanan minimum 30 hari, dan objek yang dihapus sebelum 30 hari dikenakan biaya pro-rated sama dengan biaya penyimpan an untuk hari-hari yang tersisa. Pertimbangkan seberapa sering objek ini berubah, berapa lama Anda berencana untuk menyimpan objek ini, dan seberapa sering Anda perlu mengaksesnya. Objek yang lebih kecil dari 128 KB dikenakan biaya 128 KB dan biaya penghapusan awal berlaku. Ketika operasi file yang memperbarui metadata (seperti pemilik, stempel waktu, izin, dan ACL) dilakukan terhadap file yang dikelola oleh File Gateway, objek yang ada dihapus dan versi baru objek dibuat di kelas penyimpan an Amazon S3 ini. Anda harus memvalida si bagaimana operasi file memengaruhi pembuatan objek sebelum menggunakan kelas penyimpanan ini dalam produksi karena biaya penghapusan awal berlaku. Lihat harga Amazon S3 untuk detail selengkapnya.

Meskipun Anda dapat menulis objek langsung dari berbagi file ke S3-Standard-IA, S3-One Zone-IA, atau kelas Intelligent-Tiering penyimpanan S3, kami menyarankan Anda menggunakan kebijakan

siklus hidup untuk mentransisikan objek Anda daripada menulis langsung dari berbagi file, terutama jika Anda mengharapkan untuk memperbarui atau menghapus objek dalam waktu 30 hari sejak pengarsipan. Untuk informasi tentang kebijakan siklus hidup, lihat Manajemen siklus hidup objek.

Menggunakan kelas penyimpanan GLACIER dengan File Gateway

Jika Anda mentransisikan file ke Amazon Glacier melalui kebijakan siklus hidup Amazon S3, dan file tersebut terlihat oleh klien berbagi file Anda melalui cache, Anda akan I/O mengalami kesalahan saat memperbarui file. Kami menyarankan Anda mengatur CloudWatch Acara untuk menerima pemberitahuan ketika I/O kesalahan ini terjadi, dan menggunakan pemberitahuan untuk mengambil tindakan. Misalnya, Anda dapat mengambil tindakan untuk memulihkan objek yang diarsipkan ke Amazon S3. Setelah objek dikembalikan ke S3, klien berbagi file Anda dapat mengakses dan memperbaruinya dengan sukses melalui berbagi file.

Untuk informasi tentang cara memulihkan objek yang diarsipkan, lihat Memulihkan objek yang diarsipkan di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

> **Important**
>
> S3 File Gateway tidak secara resmi mendukung kelas penyimpanan S3 Glacier Instant Retrieval. Meskipun Anda dapat menunjuk objek dalam bucket berbagi file untuk Pengambilan Instan S3 Glacier dengan menggunakan kebijakan siklus hidup atau PUT permintaan langsung, S3 File Gateway tidak dapat mengenali file mana yang ada di kelas penyimpanan tersebut, dan akan melakukan operasi file pada objek tersebut seperti objek lainnya. Karena S3 Glacier Instant Retrieval memiliki biaya akses yang lebih tinggi daripada kelas penyimpanan Amazon S3 lainnya, operasi file massal seperti pemindaian virus,, dan penggantian nama`rsync`, dapat menghasilkan tagihan Amazon S3 yang besar jika tidak dikelola dengan hati-hati. Untuk alasan ini, kami tidak menyarankan menggunakan S3 Glacier Instant Retrieval dengan S3 File Gateway.

Menggunakan driver Kubernetes Container Storage Interface

Kubernetes adalah sistem sumber terbuka untuk mengotomatiskan penerapan, penskalaan, dan pengelolaan aplikasi dalam kontainer. Dalam lingkungan Kubernetes, sebuah kontainer mirip dengan VM, tetapi sebuah wadah memiliki properti isolasi santai untuk berbagi Sistem Operasi (OS) di antara aplikasinya. Oleh karena itu, kontainer dianggap lebih ringan daripada VM. Mirip dengan

VM, wadah memiliki sistem file sendiri, bagian dari CPU yang dialokasikan, memori, ruang proses, dan banyak lagi. Karena mereka dipisahkan dari infrastruktur yang mendasarinya, mereka portabel melintasi cloud dan distribusi OS. Jika Anda memiliki klaster Kubernetes, Anda dapat menginstal dan mengonfigurasi driver Kubernetes Container Storage Interface (CSI) di seluruh instance di cluster Anda untuk memungkinkan mereka menggunakan Amazon S3 File Gateway yang ada untuk penyimpanan.

Setelah Anda menginstal driver CSI untuk jenis berbagi file yang ingin Anda gunakan, Anda harus membuat satu atau lebih objek penyimpanan. Bergantung pada jenis provisioning yang ingin Kubernetes gunakan saat pod Anda meminta penyimpanan, Anda harus membuat salah satu objek Kubernetes, atau objek dan *`StorageClass`* *`PersistentVolume`* objek untuk menghubungkan pod komputasi Kubernetes ke `PersistentVolumeClaim` file share Anda. Untuk informasi lebih lanjut, lihat dokumentasi online Kubernetes di. https://kubernetes.io/docs/concepts/storage/

Topik

- Bekerja dengan driver SMB CSI
- Bekerja dengan driver NFS CSI

Bekerja dengan driver SMB CSI

Ikuti prosedur di bagian ini untuk menginstal, mengonfigurasi, atau menghapus driver CSI yang diperlukan untuk menggunakan berbagi file SMB di Amazon S3 File Gateway untuk penyimpanan di cluster Kubernetes Anda. Untuk informasi selengkapnya, lihat dokumentasi driver SMB CSI sumber terbuka di. GitHub https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md

> **Note**
>
> Ketika Anda membuat `PersistentVolume` objek atau `StorageClass` objek, Anda dapat menentukan `ReclaimPolicy` parameter untuk menentukan apa yang terjadi pada penyimpanan eksternal ketika objek dihapus. Driver SMB CSI mendukung `Recycle` opsi `Retain` dan, tetapi saat ini tidak mendukung opsi. `Delete`

Instal driver

Untuk menginstal driver Kubernetes SMB CSI:

1. Dari terminal baris perintah dengan akses ke `kubectl` klaster Kubernetes Anda, jalankan perintah berikut:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. Tunggu sampai perintah sebelumnya selesai, lalu gunakan perintah berikut untuk memastikan bahwa pod driver CSI berjalan:

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   Outputnya akan serupa dengan yang berikut ini:

```
NAME                                 READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-smb-controller-56bfddd689-dh5tk  4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4  4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                   3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                   3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Buat objek SMB StorageClass

Untuk membuat StorageClass objek SMB baru untuk klaster Kubernetes Anda:

1. Buat file konfigurasi bernama `storageclass.yaml` dengan konten yang mirip dengan contoh berikut. Gantikan informasi spesifik penerapan Anda sendiri dengan yang ditampilkan. *`ExampleValues`*

```
---
```

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub
 directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. Dari terminal baris perintah dengan akses ke `kubectl` dan`storageclass.yaml`, jalankan perintah berikut:

   kubectl apply -f storageclass.yaml

   > **Note**
   >
   > Anda juga dapat membuatnya StorageClass dengan menyediakan teks `.yaml` konfigurasi dari langkah sebelumnya ke sebagian besar platform manajemen dan kontainerisasi Kubernetes pihak ketiga.

3. Konfigurasikan pod di klaster Kubernetes Anda untuk menggunakan yang baru StorageClass yang Anda buat. Untuk informasi lebih lanjut, lihat dokumentasi online Kubernetes di. https://kubernetes.io/docs/concepts/storage/

Buat SMB PersistentVolume dan objek PersistentVolumeClaim

Untuk membuat SMB PersistentVolume dan PersistentVolumeClaim objek baru:

1. Buat dua file konfigurasi. Satu bernama`persistentvolume.yaml`, dan satu bernama`persistentvolumeclaim.yaml`.
2. Untuk`persistentvolume.yaml`, tambahkan konten yang mirip dengan contoh berikut. Gantikan informasi spesifik penerapan Anda sendiri dengan yang ditampilkan. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
        driver: smb.csi.k8s.io
        readOnly: false
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. Untuk`persistentvolumeclaim.yaml`, tambahkan konten yang mirip dengan contoh berikut. Gantikan informasi spesifik penerapan Anda sendiri dengan yang ditampilkan. *`ExampleValues`*

```
---
```

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
 name of the PersistentVolume you created
        storageClassName: ""
```

4. Dari terminal baris perintah dengan akses ke `kubectl` dan kedua `.yaml` file yang Anda buat, jalankan perintah berikut:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > Anda juga dapat membuat PersistentVolumeClaim objek PersistentVolume dan dengan menyediakan teks `.yaml` konfigurasi dari langkah sebelumnya ke sebagian besar platform manajemen dan kontainerisasi Kubernetes pihak ketiga.

5. Konfigurasikan pod di klaster Kubernetes Anda untuk menggunakan yang baru PersistentVolumeClaim yang Anda buat. Untuk informasi lebih lanjut, lihat dokumentasi online Kubernetes di. https://kubernetes.io/docs/concepts/storage/

Copot pemasangan driver

Untuk menghapus driver Kubernetes SMB CSI:

- Dari terminal baris perintah dengan akses ke `kubectl` klaster Kubernetes Anda, jalankan perintah berikut:

curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

Bekerja dengan driver NFS CSI

Ikuti prosedur di bagian ini untuk menginstal, mengonfigurasi, atau menghapus driver CSI yang diperlukan untuk menggunakan berbagi file NFS di Amazon S3 File Gateway untuk penyimpanan di cluster Kubernetes Anda. Untuk informasi selengkapnya, lihat dokumentasi driver NFS CSI open-source di. GitHub https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md

Instal driver

Untuk menginstal driver Kubernetes NFS CSI:

1. Dari terminal baris perintah dengan akses ke `kubectl` klaster Kubernetes Anda, jalankan perintah berikut:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --

2. Tunggu sampai perintah sebelumnya selesai, lalu gunakan perintah berikut untuk memastikan bahwa pod driver CSI berjalan:

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   Outputnya akan serupa dengan yang berikut ini:

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-nfs-controller-56bfddd689-dh5tk       4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4       4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                        3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
```

```
csi-nfs-node-dr4s4                          3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Buat objek NFS StorageClass

Untuk membuat StorageClass objek NFS untuk klaster Kubernetes Anda:

1. Buat file konfigurasi bernama `storageclass.yaml` dengan konten yang mirip dengan contoh berikut. Gantikan informasi spesifik penerapan Anda sendiri dengan yang ditampilkan. *`ExampleValues`*

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: example-nfs-classname
    namespace: example-namespace
provisioner: nfs.csi.k8s.io
parameters:
    server: gateway-dns-name-or-ip-address
    share: /example-share-name
reclaimPolicy: Retain
volumeBindingMode: Immediate
mountOptions:
    - hard
    - nfsvers=4.1
```

2. Dari terminal baris perintah dengan akses ke `kubectl` dan`storageclass.yaml`, jalankan perintah berikut:

   kubectl apply -f storageclass.yaml

> **Note**
>
> Anda juga dapat membuatnya StorageClass dengan menyediakan teks `.yaml` konfigurasi dari langkah sebelumnya ke sebagian besar platform manajemen dan kontainerisasi Kubernetes pihak ketiga.

3. Konfigurasikan pod di klaster Kubernetes Anda untuk menggunakan StorageClass objek baru yang Anda buat. Untuk informasi lebih lanjut, lihat dokumentasi online Kubernetes di. https://kubernetes.io/docs/concepts/storage/

Buat NFS PersistentVolume dan objek PersistentVolumeClaim

Untuk membuat NFS PersistentVolume dan PersistentVolumeClaim objek baru:

1. Buat dua file konfigurasi bernama `persistentvolume.yaml` dan`persistentvolumeclaim.yaml`.
2. Untuk`persistentvolume.yaml`, tambahkan konten yang mirip dengan contoh berikut. Gantikan informasi spesifik penerapan Anda sendiri dengan yang ditampilkan. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
            share: /example-share-name
```

3. Untuk`persistentvolumeclaim.yaml`, tambahkan konten yang mirip dengan contoh berikut. Gantikan informasi spesifik penerapan Anda sendiri dengan yang ditampilkan. *`ExampleValues`*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name
 of the PersistentVolume you created
    storageClassName: ""
```

4. Dari terminal baris perintah dengan akses ke `kubectl` dan kedua `.yaml` file, jalankan perintah berikut:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > Anda juga dapat membuat PersistentVolumeClaim objek PersistentVolume dan dengan menyediakan teks `.yaml` konfigurasi dari langkah sebelumnya ke sebagian besar platform manajemen dan kontainerisasi Kubernetes pihak ketiga.

5. Konfigurasikan pod di klaster Kubernetes Anda untuk menggunakan PersistentVolumeClaim objek baru yang Anda buat. Untuk informasi lebih lanjut, lihat dokumentasi online Kubernetes di. https://kubernetes.io/docs/concepts/storage/

Copot pemasangan driver

Untuk menghapus driver Kubernetes NFS CSI:

- Dari terminal baris perintah dengan akses ke `kubectl` klaster Kubernetes Anda, jalankan perintah berikut:

```
curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/
uninstall-driver.sh | bash -s master --
```

AWS Storage Gateway Terraform modul

HashiCorpTerraform adalah mesin Infrastructure as Code (IAc) open-source yang dikembangkan menggunakan HashiCorp Configuration Language (HCL). Terraform menyediakan alur kerja antarmuka baris perintah (CLI) yang konsisten yang, bersama dengan Amazon S3 File Gateway untuk infrastruktur back-end, dapat mengelola ratusan layanan cloud dan mengkodifikasi API cloud menjadi file konfigurasi deklaratif.

Anda dapat menggunakan Terraform untuk menerapkan Gateway File Amazon S3 dengan aman sebagai mesin virtual (VM) di infrastruktur virtual lokal Anda. Terraform menyediakan otomatisasi untuk infrastruktur virtual lokal. Lihat Mengotomatiskan penerapan Gateway File Amazon S3 di VMware dengan Terraform by untuk HashiCorp informasi tentang penerapan Gateway File Amazon S3 dengan cepat menggunakan Terraform dalam lingkungan virtual VMware lokal.

> **Note**
>
> Anda mungkin perlu mengonfigurasi Terraform untuk mendapatkan versi terbaru dari gambar AWS Storage Gateway mesin untuk platform hypervisor pilihan Anda. Gambar mesin Storage Gateway menggunakan konvensi penamaan berikut. Nomor versi yang ditambahkan ke nama gambar berubah dengan setiap rilis versi.
> `aws-storage-gateway-FILE_S3-1.25.0`

Otomatisasi ini memberi Anda modul Terraform yang dapat disesuaikan yang dapat Anda gunakan untuk menyediakan Gateway File Amazon S3 dengan semua sumber daya dan dependensi yang diperlukan untuk sepenuhnya menerapkan gateway dan berbagi file di lingkungan VM Anda. Modul Terraform menyediakan VM gateway, mengaktifkan gateway, mengonfigurasi disk cache, menggabungkan gateway ke domain, membuat bucket Amazon S3, membuat berbagi file, dan memetakannya ke bucket. Untuk contoh lengkap repositori yang berisi kode Terraform guna membuat resource yang diperlukan untuk menjalankan Amazon S3 File Gateway di lokasi, lihat kode sumber modul Terraform Storage Gateway aktif. GitHub

> **Note**
>
> Modul Amazon S3 File Gateway untuk Terraform adalah upaya yang didukung komunitas. Itu bukan bagian dari AWS layanan. Best-effort dukungan disediakan oleh komunitas AWS Storage.

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 Titik Akhir dan Kuota di. Referensi Umum AWS

> **Note**
>
> Anda juga dapat menggunakan AWS SDKs saat mengembangkan aplikasi dengan Storage Gateway. AWS SDKs Untuk Java, .NET, dan PHP membungkus Storage Gateway API yang mendasarinya, menyederhanakan tugas pemrograman Anda. Untuk informasi tentang mengunduh pustaka SDK, lihat Pustaka Kode Contoh.

Topik

AWS Storage Gateway Header Permintaan yang Diperlukan

Bagian ini menjelaskan header yang diperlukan yang harus Anda kirim dengan setiap permintaan POST. AWS 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. AWS 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 AWS 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 YourAccesssKey, 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 jenis konten untuk semua permintaan AWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Header	Deskripsi
`Host`	Gunakan header host untuk menentukan AWS Storage Gateway titik akhir 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 AWS Storage Gateway, lihat AWS Storage Gateway Titik Akhir dan Kuota di. Referensi Umum AWS `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Anda harus memberikan stempel waktu di `Date` header HTTP atau `x-amz-date` header AWS. (Beberapa pustaka klien HTTP tidak mengizinkan Anda mengatur `Date` header.) Ketika `x-amz-date` header hadir, AWS Storage Gateway mengabaikan `Date` header apa pun selama otentikasi permintaan. Formatnya harus ISO8601 Dasar `x-amz-date` dalam format YYYYYMMDD'T'HHMMSS'Z '. Jika kedua `Date` dan `x-amz-date` header digunakan, format header Tanggal tidak harus ISO8601. `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.

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 secret access key, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY , digunakan, tanda tangan yang dihitung adalah:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Langkah terakhir adalah membangun header `Authorization`. Untuk access key demonstrasi AKIAIOSFODNN7EXAMPLE, header (dengan jeda baris yang 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 dalamTindakan API Storage Gateway.	400 Permintaan Buruk
`UnrecognizedClientException`	Token keamanan yang disertakan 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
FileSystemAssociationEndpointConfigurationConflict	Konfigurasi titik akhir Asosiasi Sistem File yang ada bertentangan dengan konfigurasi yang ditentukan.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	Alamat IP endpoint yang ditentukan sudah digunakan.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	Alamat IP Titik Akhir Asosiasi Sistem File tidak ada.	AssociateFileSystem
FileSystemAssociationNotFound	Asosiasi sistem file yang ditentukan tidak ditemukan.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	Sistem file yang ditentukan tidak ditemukan.	AssociateFileSystem

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 tidak valid.	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 valid.	CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`MaximumVolumeCountExceeded`	Jumlah volume maksimum terlampaui.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	Konfigurasi jaringan gateway telah berubah.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`NotSupported`	Operasi yang ditentukan tidak didukung.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache 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 respons kesalahan berikut menunjukkan sintaks keluaran elemen respons yang umum untuk semua respons 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."
}
```

Tindakan API Storage Gateway

Untuk daftar operasi Storage Gateway, lihat Tindakan di Referensi AWS Storage Gateway API.

Riwayat dokumen untuk Panduan Pengguna Gateway File Amazon S3

Tabel berikut menjelaskan perubahan penting dalam setiap rilis panduan pengguna ini setelah April 2018. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
IPv6 dukungan	IPv6dukungan tersedia pada alat gateway versi 2.x atau lebih tinggi.	September 10, 2025
Menambahkan panduan throughput dan optimasi	Bab Kinerja dan pengoptimalan sekarang mencakup rekomendasi dan praktik terbaik untuk memaksimalkan throughput Gateway File S3 Anda dan mengoptimalkan penerapan Anda untuk kasus penggunaan cadangan database SQL Server. Untuk informasi selengkapnya, lihat Memaksimalkan throughput Gateway File S3, dan Mengoptimalkan Gateway File S3 untuk backup database SQL Server.	Juni 13, 2025
Ditambahkan fungsi laporan cache	S3 File Gateway sekarang dapat menghasilkan laporan metadata untuk file yang saat ini berada di cache unggahan lokal untuk berbagi file tertentu. Untuk informasi selengkapnya, lihat Membuat	Maret 31, 2025

	laporan cache untuk Gateway File S3 Anda, Melihat dan mengelola laporan cache untuk Gateway File S3 Anda, dan Memahami informasi yang disediakan dalam laporan cache Gateway File S3.	
Menambahkan dukungan untuk Enkripsi Sisi Server Dual-layer dengan kunci (DSSE-KMS) AWS KMS	Anda sekarang dapat menggunakan enkripsi sisi server dual-layer dengan AWS KMS kunci untuk mengenkripsi file yang diunggah S3 File Gateway ke Amazon S3. Untuk informasi selengkapnya tentang DSSE-KMS, lihat Mengenkripsi objek yang disimpan oleh File Gateway di Amazon S3.	September 13, 2024

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
Menambahkan tingkat keamanan SMB baru	S3 File Gateway sekarang mendukung tingkat keamanan tambahan yang dapat Anda gunakan untuk menegakkan enkripsi AES 256-bit untuk koneksi klien SMB. Untuk informasi selengkapnya, lihat Menetapkan tingkat keamanan untuk gateway Anda.	23 Mei 2024

Pelaporan versi perangkat lunak alat Gateway dan catatan rilis untuk S3 File Gateway	Menambahkan catatan rilis untuk menjelaskan fitur, peningkatan, dan perbaikan baru dan yang diperbarui yang disertakan dengan setiap versi alat Amazon S3 File Gateway. Anda dapat menentukan nomor versi perangkat lunak gateway dari konsol Storage Gateway atau dengan menggunakan AWS CLI. Untuk informasi selengkapnya, lihat Catatan Rilis — Perangkat Lunak Peralatan Gateway.	5 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 Memahami CloudWatch alarm .	2 Oktober 2023

Peningkatan pembagian file maksimum per gateway	S3 File Gateway sekarang mendukung hingga 50 pembagian file per gateway, meningkat dari batas sebelumnya 10. Ini memungkinkan Anda untuk membuat lebih banyak berbagi file pada satu gateway, mengurangi jumlah gateway yang perlu Anda kelola. Untuk informasi selengkapnya, lihat Kuota untuk berbagi file.	18 Januari 2023
Ditambahkan dukungan untuk atribut DOS	S3 File Gateway sekarang mendukung atribut DOS untuk file yang disimpan di Amazon S3. Ini memungkinkan Anda untuk mempertahankan atribut file Windows seperti read-only, hidden, system, dan archive saat file diunggah ke Amazon S3. Untuk informasi selengkapnya, lihat Support untuk atribut file di Amazon S3 File Gateway.	18 Januari 2023

Menambahkan kiat GatewayClockOutOfSync pemecahan masalah	Bagian Troubleshooting: File Gateway issues sekarang menyertakan panduan pemecahan masalah untuk membantu mendiagnosis masalah yang mungkin Anda temui jika jam sistem gateway Anda tidak disinkronkan dengan waktu server Storage Gateway AWS . Untuk informasi selengkapnya, lihat Kesalahan: GatewayClockOutOfSync.	Oktober 19, 2022
Menambahkan pembatasan bandwidth jaringan berbasis jadwal	S3 File Gateway sekarang mendukung pembatasan bandwidth jaringan berbasis jadwal untuk unggahan data ke Amazon S3. Fitur ini memungkinkan Anda untuk membatasi jumlah bandwidth jaringan yang digunakan gateway Anda selama periode waktu tertentu, membantu Anda mengelola penggunaan jaringan selama jam kerja sibuk. Untuk informasi selengkapnya, lihat Mengelola bandwidth untuk Gateway File S3 Anda.	18 Januari 2022

Prosedur pembuatan gateway yang diperbarui	Prosedur untuk membuat gateway baru telah diperbaru i untuk mencerminkan perubahan di konsol Storage Gateway. Untuk informasi selengkapnya, lihat Membuat dan mengaktifkan Gateway File Amazon S3.	Oktober 12, 2021
Support untuk menutup paksa file pada berbagi file SMB	Anda sekarang dapat menggunakan pengaturan Grup Lokal untuk menetapka n izin Admin Gateway. Admin Gateway dapat menggunak an snap-in Shared Folder Microsoft Management Console untuk menutup paksa file yang terbuka dan terkunci pada berbagi file SMB. Untuk informasi selengkapnya, lihat Mengonfigurasi Grup Lokal untuk gateway Anda.	Oktober 12, 2021

Dukungan log audit untuk berbagi file NFS	Anda sekarang dapat mengonfigurasi berbagi file NFS untuk menghasilkan log audit yang memberikan detail tentang akses pengguna ke file dan folder dalam berbagi file. Anda dapat menggunakan log ini untuk memantau aktivitas pengguna dan mengambil tindakan jika pola aktivitas yang tidak pantas diidentifikasi. Untuk informasi selengkapnya, lihat Memahami log audit Gateway File.	Oktober 12, 2021
Dukungan alias titik akses	Berbagi file File Gateway sekarang dapat terhubung ke penyimpanan Amazon S3 menggunakan alias titik akses bergaya ember. Untuk informasi selengkapnya, lihat Membuat berbagi file.	Oktober 12, 2021
Dukungan titik akhir VPC dan titik akses	Berbagi file File Gateway sekarang dapat terhubung ke bucket S3 melalui titik akses atau titik akhir antarmuka di VPC Anda yang didukung oleh. AWS PrivateLink Untuk informasi selengkapnya, lihat Membuat berbagi file.	7 Juli 2021

Dukungan penguncian oportunistik	File Gateway berbagi file sekarang dapat menggunakan penguncian oportunistik untuk mengoptimalkan strategi buffering file mereka, yang meningkatkan kinerja dalam banyak kasus, terutama yang berkaitan dengan menu konteks Windows. Untuk informasi selengkapnya, lihat Membuat berbagi file SMB.	7 Juli 2021
Kepatuhan FedRAMP	Storage Gateway sekarang sesuai dengan FedRAMP. Untuk informasi selengkapnya, lihat Validasi kepatuhan untuk Storage Gateway.	24 November 2020
Pemberitahuan unggahan file untuk File Gateway	File Gateway sekarang menyediakan pemberitahuan unggahan file, yang memberi tahu Anda ketika file telah sepenuhnya diunggah ke Amazon S3 oleh File Gateway. Untuk informasi selengkapnya, lihat Mendapatkan notifikasi unggahan file.	9 November 2020
Pencacahan berbasis akses untuk File Gateway	File Gateway sekarang menyediakan enumerasi berbasis akses, yang memfilter enumerasi file dan folder pada berbagi file SMB berdasarkan share. ACLs Untuk informasi selengkapnya, lihat Membuat berbagi file SMB.	9 November 2020

Migrasi File Gateway	File Gateway sekarang menyediakan proses terdokumentasi untuk mengganti File Gateway yang ada dengan File Gateway baru. Untuk informasi selengkapnya, lihat Mengganti Gateway File dengan Gateway File baru.	30 Oktober 2020
File Gateway cache dingin membaca kinerja 4x meningkat	Storage Gateway telah meningkatkan kinerja pembacaan cache dingin 4x. Untuk informasi selengkapnya, lihat Panduan kinerja untuk Gateway File.	31 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 AWS 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

Dukungan untuk beberapa berbagi file yang dilampirkan ke satu bucket Amazon S3	File Gateway sekarang mendukung pembuatan beberapa berbagi file untuk satu bucket S3 dan menyinkronkan cache lokal File Gateway dengan bucket berdasarkan frekuensi akses direktori. Anda dapat membatasi jumlah bucket yang diperlukan untuk mengelola pembagian file yang Anda buat di File Gateway Anda. Anda dapat menentukan beberapa awalan S3 untuk bucket S3 dan memetakan awalan S3 tunggal ke berbagi file gateway tunggal. Anda juga dapat menentukan nama berbagi file gateway agar tidak bergantung pada nama bucket agar sesuai dengan konvensi penamaan berbagi file lokal. Untuk informasi selengkapnya, lihat Membuat berbagi file NFS atau Membuat berbagi file SMB.	7 Juli 2020

File Gateway penyimpanan cache lokal meningkat 4x	Storage Gateway sekarang mendukung cache lokal hingga 64 TB untuk File Gateway, meningkatkan kinerja untuk aplikasi lokal dengan menyediakan akses latensi rendah ke kumpulan data kerja yang lebih besar. Untuk informasi selengkap nya, lihat Ukuran disk lokal yang direkomendasikan untuk gateway Anda di Panduan Pengguna Storage Gateway.	7 Juli 2020
Lihat CloudWatch alarm Amazon di konsol Storage Gateway	Anda sekarang dapat melihat CloudWatch alarm di konsol Storage Gateway. Untuk informasi selengkapnya, lihat Memahami CloudWatch alarm.	29 Mei 2020
Dukungan untuk titik akhir Federal Information Processin g Standard (FIPS)	Anda sekarang dapat mengaktifkan gateway dengan titik akhir FIPS di Wilayah. AWS GovCloud (US) Untuk memilih titik akhir FIPS untuk File Gateway, lihat Memilih titik akhir layanan.	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
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

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
Baru Wilayah AWS	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
Baru Wilayah AWS	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
Dukungan berbagi file SMB untuk Microsoft Windows ACLs	Untuk File Gateways, Anda sekarang dapat menggunak an daftar kontrol akses Microsoft Windows (ACLs) untuk mengontrol akses ke berbagi file Server Message Block (SMB). Untuk informasi selengkap nya, lihat Menggunakan Microsoft Windows ACLs untuk Mengontrol Akses ke Berbagi File SMB.	8 Mei 2019

Dukungan File Gateway untuk otorisasi berbasis tag	File Gateway sekarang mendukung otorisasi berbasis tag. Anda dapat mengontrol akses ke sumber daya File Gateway berdasarkan tag pada sumber daya tersebut. Anda juga dapat mengontrol akses berdasarkan tag yang dapat diteruskan dalam kondisi permintaan IAM. Untuk informasi selengkapnya, lihat Mengontrol Akses ke Sumber Daya Gateway File.	4 Maret 2019
Ketersediaan AWS Storage Gateway Hardware Appliance di Eropa	AWS Storage Gateway Hardware Appliance sekarang tersedia di Eropa. Untuk informasi selengkapnya, lihat Wilayah Peralatan AWS Storage Gateway Perangkat Keras di Referensi Umum AWS. Selain itu, Anda sekarang dapat meningkatkan penyimpanan yang dapat digunakan pada Storage Gateway Hardware Appliance dari 5 TB menjadi 12 TB dan mengganti kartu jaringan tembaga yang terpasang dengan kartu jaringan serat optik 10-gigabit. AWS Untuk informasi selengkapnya, lihat Menyiapkan Peralatan Perangkat Keras Anda.	25 Februari 2019

Support untuk AWS Storage Gateway Hardware Appliance	AWS Storage Gateway Hardware Appliance mencakup perangkat lunak Storage Gateway yang sudah diinstal sebelumnya di server pihak ketiga. Anda dapat mengelola alat dari Konsol Manajemen AWS. Alat ini dapat meng-host file, tape, dan Volume Gateways. Untuk informasi selengkapnya, lihat Menggunakan Storage Gateway Hardware Appliance.	18 September 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

Pembaruan lebih awal

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS Storage Gateway Pengguna sebelum Mei 2018.

Ubah	Deskripsi	Tanggal Diubah
Support untuk kelas penyimpan an IA Satu Zona S3	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

Ubah	Deskripsi	Tanggal Diubah
Baru Wilayah AWS	Tape Gateway sekarang tersedia di Wilayah Asia Pasifik (Singapura). Untuk detail informasi, lihat Wilayah AWSyang mendukung Storage Gateway.	3 April 2018
Support untuk pemberitahuan cache refresh, Requester Pays, dan kaleng 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 selengkap nya, lihat RefreshCache.html di Referensi API Storage Gateway. Untuk File Gateways, Anda sekarang dapat menentukan bahwa pemohon atau pembaca membayar biaya akses, bukan pemilik bucket. File Gateway sekarang dapat memberikan kontrol penuh atas file tertulis kepada pemilik bucket S3 yang memetakan ke berbagi file NFS. Untuk informasi selengkapnya, lihat Membuat berbagi file.	1 Maret 2018
Baru Wilayah AWS	Storage Gateway sekarang tersedia di Wilayah Eropa (Paris). Untuk detail informasi, lihat Wilayah AWSyang mendukung Storage Gateway.	18 Desember 2017
Support untuk pemberitahuan unggahan file dan tebakan jenis Multipurp ose Internet Mail Extension (MIME)	File Gateway sekarang dapat mengirim pemberita huan ketika semua file yang ditulis ke berbagi file NFS Anda telah diunggah ke Amazon S3. Untuk informasi selengkapnya, lihat NotifyWhenUploadedi Referensi API Storage Gateway. File Gateway sekarang dapat menebak jenis MIME untuk objek yang diunggah berdasarkan ekstensi file. Untuk informasi selengkapnya, lihat Membuat berbagi file.	21 November 2017

Ubah	Deskripsi	Tanggal Diubah
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
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
Baru Wilayah AWS	Storage Gateway sekarang tersedia di Wilayah Asia Pasifik (Mumbai). Untuk detail informasi, lihat Wilayah AWSyang 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

Ubah	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 AMI komunitas. Untuk informasi tentang cara membuat File Gateway dan menerapkannya pada instans EC2, lihat. Membuat dan mengaktifkan Gateway File Amazon S3 Untuk informasi tentang cara meluncurkan AMI File Gateway, lihatMenerapkan host Amazon EC2 default untuk S3 File Gateway. Selain itu, File Gateway sekarang mendukung konfigurasi proxy HTTP. Untuk informasi selengkap nya, lihat Merutekan gateway Anda yang digunakan di Amazon EC2 melalui proxy HTTP.	Februari 08, 2017
Baru Wilayah AWS	Storage Gateway sekarang tersedia di Wilayah Eropa (London). Untuk detail informasi, lihat Wilayah AWSyang mendukung Storage Gateway.	13 Desember 2016
Baru Wilayah AWS	Storage Gateway sekarang tersedia di Wilayah Kanada (Tengah). Untuk detail informasi, lihat Wilayah AWSyang mendukung Storage Gateway.	Desember 08, 2016
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

Storage Gateway AL2 ke Kampanye Migrasi AL2023

AWSsedang mentransisikan Storage Gateway appliance operating system (OS) dari Amazon Linux 2 ke AL2023 untuk mengaktifkan fitur penyimpanan cloud hybrid baru dan mempertahankan standar kinerja dan keamanan yang optimal. Transisi ini akan berdampak pada semua versi alat AL2-based Storage Gateway S3 File Gateway Version 1.x, Tape Gateway Version 2.x, dan Volume Gateway Version 2.x. Anda diminta untuk menyelesaikan migrasi sebelum 30 Juni 2026, karena AWS akan berhenti mendukung sistem ini setelahnya.

Anda dapat mengidentifikasi apakah gateway Anda memerlukan migrasi melalui beberapa metode. AWSKonsol menampilkan pesan penghentian di tab Detail gateway untuk gateway yang terpengaruh. Selain itu, `DescribeGatewayInformation`API menyediakan akses terprogram untuk memeriksa bidang tanggal penghentian. Dasbor AWS Kesehatan mencantumkan gateway yang terpengaruh di bawah tab Sumber daya yang terpengaruh. Namun, daftar tidak diperbarui segera setelah gateway dimigrasi. Proses migrasi itu sendiri dirancang dengan keamanan data sebagai prioritas, menyimpan salinan data VM gateway lokal AWS sebelum migrasi dimulai untuk memungkinkan pemulihan yang mudah jika diperlukan.

AWSmenyediakan panduan migrasi komprehensif khusus untuk setiap jenis gateway. Setelah menyelesaikan migrasi, Anda harus memverifikasi keberhasilan dengan memeriksa bahwa peringatan penghentian tidak lagi muncul di tab Detail gateway AWS Konsol, atau dengan menggunakan `DescribeGatewayInformation`API untuk mengonfirmasi bahwa bidang tanggal penghentian tidak ada. Secara kritis, Anda tidak boleh kembali ke gateway AL2 Anda setelah berhasil bermigrasi ke AL2023, karena pengembalian dapat menyebabkan masalah operasional.

Selama periode migrasi, AWS akan mengirimkan pemberitahuan pengingat bulanan melalui email, dan tab Perubahan Terjadwal Dasbor AWS Kesehatan untuk membantu Anda merencanakan dan menyelesaikan migrasi Anda. Jika Anda mengalami masalah selama migrasi, hubungi AWSSupport untuk bantuan dan panduan pemecahan masalah.

Tautan dan Sumber Daya Cepat

Referensi Migrasi Versi Gateway

Memahami gateway mana yang memerlukan migrasi sangat mudah berdasarkan nomor versi perangkat lunak gateway. Penting untuk dicatat bahwa gateway yang baru diaktifkan berdasarkan OS Amazon Linux 2 masih memerlukan migrasi pada 30 Juni 2026.

Jenis Gateway	Versi AL2 (Membutuhkan Migrasi)	Versi AL2023 (Target)
Gerbang File S3	Versi 1.x	Versi 2.x
Gateway Tape	Versi 2.x	Versi 3.x
Gateway Volume	Versi 2.x	Versi 3.x

Garis Waktu Migrasi

Garis waktu migrasi mencakup beberapa tonggak penting:

- 28 Oktober 2025: Semua penerapan gateway baru yang dimulai dari konsol Storage Gateway akan default ke gambar AL2023.
- 5 Januari 2026: AWS akan mulai membatasi aktivasi gateway AL2 baru.
- 30 Juni 2026: AL2-based gateway akan berhenti menerima pembaruan perangkat lunak dan AWS dukungan akan berakhir. Setelah tanggal ini, sementara Anda dapat terus menggunakan AL2-based peralatan, mereka tidak akan menerima pembaruan perangkat lunak baru, patch keamanan, atau perbaikan bug, dan memelihara sistem ini menjadi tanggung jawab Anda sendiri.

Pre-migration Daftar periksa

> **Important**
>
> Sebelum memulai proses migrasi, verifikasi persyaratan berikut untuk memastikan migrasi berhasil.

- Gunakan gambar gateway terbaru. Saat membuat VM Storage Gateway baru:
  - Untuk gateway Amazon EC2, gunakan AMI terbaru dari parameter SSM publik atau gunakan konsol Storage Gateway.
  - Untuk gateway lokal, unduh gambar VM terbaru dari konsol Storage Gateway.

- Cocokkan konfigurasi perangkat keras. Pastikan VM gateway baru menggunakan CPU, memori, dan throughput jaringan yang sama dengan gateway yang ada. Untuk gateway EC2, gunakan jenis instans yang sama.
- Verifikasi ukuran disk root. Disk root gateway baru VM harus setidaknya berukuran sama dengan disk root gateway yang ada. Jika disk root yang ada memiliki kurang dari 20 GB ruang yang tersedia, ukuran disk root baru ke: (ukuran disk root yang ada) + (20 GB dikurangi ruang yang tersedia pada disk root yang ada).
- Terapkan pembaruan perangkat lunak yang tertunda. Sebelum memulai migrasi, terapkan pembaruan perangkat lunak yang tertunda pada gateway yang ada. Buka konsol Storage Gateway, pilih gateway Anda, dan pilih Perbarui Sekarang jika tersedia.
- Verifikasi konektivitas jaringan dari gateway baru. Sebelum memulai migrasi, konfirmasikan bahwa VM gateway baru dapat mencapai:
  - Titik akhir layanan Storage Gateway (atau titik akhir VPC Anda).
  - Titik akhir Amazon S3.
  - Active Directory /DNS server (jika gateway Anda bergabung dengan domain).
  - Gunakan uji konektivitas jaringan konsol lokal gateway untuk memvalidasi semua titik akhir yang lulus.
- Mengatasi unggahan file yang gagal. Pastikan `FilesFailingUpload` CloudWatch metrik gateway Anda nol sebelum memulai migrasi. File dalam keadaan gagal menunjukkan kesalahan yang belum terselesaikan yang harus ditangani terlebih dahulu. Untuk mengidentifikasi file yang terpengaruh, buat laporan cache, lalu selesaikan masalah mendasar sebelum melanjutkan.
- Tunggu cache disinkronkan. Verifikasi bahwa `CachePercentDirty` metrik pada tab Pemantauan gateway adalah 0. Ini mengonfirmasi bahwa semua data yang di-cache telah diunggah ke S3.

Panduan Migrasi

- Panduan Migrasi Gateway File S3
- Panduan Migrasi Tape Gateway
- Panduan Migrasi Volume Gateway

Support dan Monitoring

- Konsol Storage Gateway

- AWSDashboard Personal Health
- Hubungi AWS Support

Pertanyaan yang Sering Diajukan

Apa yang terjadi pada data saya selama migrasi?

Data Anda tetap disimpan dengan tahan lama AWS selama proses migrasi. Prosedur migrasi termasuk menyimpan salinan data VM gateway lokal Anda AWS untuk pemulihan yang mudah jika diperlukan.

Apakah akan ada downtime selama migrasi?

Waktu migrasi dan setiap gangguan layanan potensial bergantung pada jenis dan konfigurasi gateway Anda. Tinjau panduan migrasi khusus gateway untuk penerapan Anda untuk informasi terperinci.

Apa yang terjadi jika saya tidak bermigrasi pada 30 Juni 2026?

Gateway Anda akan terus beroperasi secara normal, dan data akan tetap disimpan dengan amanAWS, tetapi Anda harus memigrasikan gateway yang terpengaruh sebelum 30 Juni 2026, untuk terus menerima pembaruan dan dukungan.

Dapatkah saya terus menggunakan gateway berbasis AL2 saya setelah bermigrasi?

Tidak, Anda tidak boleh menggunakan gateway AL2 Anda di samping gateway AL2023 baru Anda setelah berhasil bermigrasi. Gunakan hanya AL2023-based gateway baru Anda ke depan. Menggunakan gateway AL2 dan AL2023 secara bersamaan dapat menyebabkan masalah operasional.

Saya mengalami masalah selama migrasi. Apa yang harus saya lakukan?

Hubungi AWSSupport untuk bantuan. Tim dukungan kami dapat membantu memecahkan masalah migrasi dan memandu Anda melalui prosesnya.

Catatan rilis untuk perangkat lunak alat gateway

Catatan rilis ini menjelaskan fitur, peningkatan, dan perbaikan baru dan yang diperbarui yang disertakan dengan setiap versi alat Amazon S3 File Gateway Amazon File 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 bukan S3 File Gateway.

Untuk informasi selengkapnya tentang pembaruan Gateway File S3 Gateway, termasuk cara mengubah pemeliharaan otomatis default dan jadwal pembaruan untuk gateway, lihat Mengelola Pembaruan Gateway Menggunakan Konsol Gateway Storage Mengelola Pembaruan Gateway Menggunakan Konsol AWS Gateway Storage .

Untuk informasi selengkapnya tentang memigrasi Gateway File S3 dari Amazon Linux 2 ke AL2023, lihat. Migrasi AL2 ke AL2023

Gateway berbasis Amazon Linux 2023 (AL2023)

Tabel berikut mencantumkan catatan rilis untuk gateway berdasarkan AL2023.

> **Note**
>
> Gateway versi 1.xx tidak dapat diperbarui ke 2.xx.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-07-20	2.1.10	• Memperbarui komponen sistem operasi dan paket perangkat lunak untuk meningkatkan keamanan dan kinerja. • Memperbaiki potensi masalah stabilitas gateway saat cache berjalan sangat rendah.
2026-07-15	2.1.9	• Memperbarui komponen sistem operasi dan paket perangkat lunak untuk meningkatkan keamanan dan kinerja.
2026-06-16	2.1.8	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-05-21	2.1.7	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-05-14	2.1.6	Pembaruan Pemeliharaan:

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
		• Peningkatan migrasi 1.x ke 2.x (AL2 ke AL2023). • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-04-16	2.1.5	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-03-26	2.1.4	Pembaruan Pemeliharaan: **Note** Rilis ini memperkenalkan ketergantungan yang lebih keras pada layanan DCE/RPC Endpoint Mapper (port TCP 135) pada Pengontrol Domain AD. Jika lingkungan Anda memblokir lalu lintas keluar pada port ini, buka blokir untuk menghindari masalah konektivitas. Lihat Persyaratan Port Gateway File untuk detailnya. • Lanjutkan penghentian NTLM untuk interaksi antara Active Directory Domain Controllers dan Gateway. • Peningkatan ketahanan tumpukan SMB selama gangguan jaringan.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-03-16	2.1.3	Pembaruan Pemeliharaan: • Peningkatan resilensi DNS dengan lalu lintas SMB. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-03-02	2.0.7	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-02-12	2.1.2	Pembaruan Pemeliharaan: **Note** Peluncuran dijeda. Rilis ini diluncurkan ke satu set gateway terbatas. • Perbaiki masalah dengan tab keamanan dan kuota yang hilang saat menggunakan Windows Explorer pada berbagi SMB. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-02-02	2.1.1	Pembaruan Pemeliharaan: **Note** Peluncuran dijeda. Rilis ini diluncurkan ke satu set gateway terbatas. • Perbaiki masalah dengan SMB terkait akses file yang tidak peka huruf besar/kecil. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-01-21	2.0.6	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-01-16	2.1.0	Pembaruan Pemeliharaan: **Note** Peluncuran dijeda. Rilis ini diluncurkan ke satu set gateway terbatas. • Tumpukan SMB yang diperbarui. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2025-12-15	2.0.5	Pembaruan Pemeliharaan: • Memperbaiki masalah dengan metrik ukuran disk root. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2025-11-12	2.0.4	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-11-12	2.0.4	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-10-15	2.0.3	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-09-15	2.0.2	Pembaruan Pemeliharaan: • Memperbaiki masalah yang mencegah perubahan kapasitas gateway. • Memperbaiki masalah dengan `UpdateSMB LocalGroups` API. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-08-29	2.0.1	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja. • Rilis awal untuk gateway lokal.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-08-21	2.0.0	Fitur-fitur: • Rilis awal sistem operasi baru. • Menambahkan dukungan IPv6.

Amazon Linux 2 (AL2) gateway berbasis

Tabel berikut mencantumkan catatan rilis untuk gateway berdasarkan. AL2

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-07-20	1.28.10	**Note** Rilis ini diluncurkan ke satu set gateway terbatas. • Memperbarui komponen sistem operasi dan paket perangkat lunak untuk meningkatkan keamanan dan kinerja. • Memperbaiki potensi masalah stabilitas gateway saat cache berjalan sangat rendah.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-07-15	1.28.9	**Note** Rilis ini diluncurkan ke satu set gateway terbatas. • Memperbarui komponen sistem operasi dan paket perangkat lunak untuk meningkatkan keamanan dan kinerja.
2026-06-16	1.28.8	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-05-26	1.28.7	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-05-18	1.28.6	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-04-16	1.28.5	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-03-26	1.28.4	Pembaruan Pemeliharaan: **Note** Rilis ini hanya tersedia untuk gateway yang sudah ada di 1.28. * **Note** Rilis ini memperken alkan ketergantungan yang lebih keras pada layanan DCE/RPC Endpoint Mapper (port TCP 135) pada Pengontrol Domain AD. Jika lingkunga n Anda memblokir lalu lintas keluar pada port ini, buka blokir untuk menghindari masalah konektivitas. Lihat Persyaratan Port Gateway File untuk detailnya. • Lanjutkan penghentian NTLM untuk interaksi antara Active Directory Domain Controllers dan Gateway.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
		• Peningkatan ketahanan tumpukan SMB selama gangguan jaringan.
2026-03-16	1.27.21	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-03-16	1.28.3	Pembaruan Pemeliharaan: **Note** Rilis ini hanya tersedia untuk gateway yang sudah ada di 1.28. * • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-02-27	1.27.20	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-02-11	1.28.2	Pembaruan Pemeliharaan: **Note** Peluncuran dijeda. Rilis ini diluncurkan ke satu set gateway terbatas. • Perbaiki masalah dengan tab keamanan dan kuota yang hilang saat menggunakan Windows Explorer pada berbagi SMB. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-02-02	1.28.1	Pembaruan Pemeliharaan: **Note** Peluncuran dijeda. Rilis ini diluncurkan ke satu set gateway terbatas. • Perbaiki masalah dengan SMB terkait akses file yang tidak peka huruf besar/kecil. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2026-01-21	1.27.19	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2026-01-16	1.28.0	Pembaruan Pemeliharaan: **Note** Peluncuran dijeda. Rilis ini diluncurkan ke satu set gateway terbatas. • Tumpukan SMB yang diperbarui. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2025-12-15	1.27.18	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2025-11-17	1.27.17	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-10-15	1.27.16	Pembaruan Pemeliharaan: • Memperbaiki masalah di log Upload Rename Order. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2025-09-22	1.27.15	Pembaruan Pemeliharaan: • Memperbaiki masalah di log Upload Rename Order.
2025-09-15	1.27.14	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2025-08-21	1.27.13	Pembaruan Pemeliharaan: • Menambahkan statistik dan metrik sistem untuk memberikan wawasan yang lebih dalam tentang kinerja gateway.
2025-08-18	1.27.12	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-08-11	1.27.11	Pembaruan Pemeliharaan: • Memperbaiki masalah yang memengaruhi pembaruan S3 metadata di bawah operasi file tertentu untuk beberapa gateway.
2025-07-15	1.27.10	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja. • Masalah teratasi untuk Upload Rename Order log untuk gateway.
2025-06-23	1.27.9	Pembaruan Pemeliharaan: • Masalah teratasi untuk Upload Rename Order log untuk gateway. • Diaktifkan Upload Rename Order log untuk gateway baru. • Memperbaiki masalah sehingga gateway sekarang menangani operasi penghapusan dengan benar untuk file yang tidak berhasil diunggah.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-06-16	1.27.8	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-05-26	1.27.7	Pembaruan Pemeliharaan: • Masalah yang diselesaikan untuk Ganti Nama Pemesanan. **Note** Masalah ini hanya memengaruhi beberapa gateway. Anda akan diberi tahu jika gateway Anda perlu diperbarui. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-05-15	1.27.6	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-04-28	1.27.5	Pembaruan Pemeliharaan: • Memperbaiki masalah yang terkait dengan log pesanan ganti nama unggahan. • Menambahkan alat debug untuk membantu menentukan penyebab masalah unggahan. • Menambahkan statistik dan metrik sistem untuk wawasan yang lebih dalam tentang kinerja gateway. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-04-14	1.27.4	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-04-01	1.27.3	Pembaruan Pemeliharaan: • Pembaruan untuk konfigurasi logging gateway. Tidak ada tindakan pelanggan yang diperlukan.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-03-17	1.27.2	Pembaruan Pemeliharaan: • Menambahkan tindakan API yang menghapus data berbagi file cache dan metadata untuk file yang gagal diunggah dari gateway Anda ke Amazon S3. Anda Akun AWS harus diizinkan untuk menggunakan fungsi ini. Jika gateway Anda memiliki masalah dengan file yang gagal diunggah, AWS Dukungan dapat membuka kunci fungsi dan memberikan panduan tentang penggunaannya. • Menambahkan kemampuan untuk gateway baru untuk mencatat urutan operasi pengunggahan nama objek. Ini membantu mencegah file gagal diunggah ke Amazon S3 setelah operasi penggantian nama berulang atau tumpang tindih. • Memperbaiki masalah yang terkait dengan SMB membuka port secara tidak sengaja. • Sistem operasi dan elemen perangkat lunak yang

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
		diperbarui untuk meningkat kan keamanan dan kinerja.
2025-02-17	1.27.1	Pembaruan Pemeliharaan: • Dihapus Java 11. • Ditambahkan fungsi cache untuk Dukungan digunakan. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2025-01-17	1.27.0	Fitur-fitur: • Laporan Cache (segera hadir) - Perangkat lunak gateway yang diperbarui untuk mendukung peluncuran fitur mendatang yang dirancang untuk menghasilkan laporan metadata file yang saat ini di-cache oleh Gateway File S3. Anda akan dapat menggunakan laporan ini untuk memecahkan masalah jika Anda memiliki file yang gagal diunggah dari gateway Anda ke Amazon S3. Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2025-01-09	1.26.9	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2024-12-18	1.26.8	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2024-11-18	1.26.7	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2024-10-17	1.26.6	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2024-09-30	1.26.5	Pembaruan Pemeliharaan: • Memperbaiki masalah dengan gateway lokal yang tidak mengizinkan saluran dukungan • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2024-09-16	1.26.3	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2024-08-21	1.26.1	Pembaruan Pemeliharaan: • Memperbaiki masalah yang terkait dengan logging.
2024-08-19	1.26.0	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2024-07-16	1.25.2	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2024-06-17	1.25.1	Pembaruan Pemeliharaan: • Memperbaiki masalah dengan peningkatan saat menggunakan proxy dan DNS dinonaktifkan. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2024-05-15	1.25.0	Fitur-fitur: • Ditambahkan kemampuan untuk mengatur AES-128 atau AES-256 enkripsi minimum. Ini adalah perubahan gateway saja dan akan tersedia di konsol Storage Gateway dalam rilis mendatang. • Peningkatan rotasi log sistem saat ruang disk rendah. Sebelumnya, penulisan log yang mengisi disk root akan menyebabk an gateway berhenti. Sekarang, saat ruang berkurang, gateway akan membuat lebih banyak ruang untuk log yang lebih baru dengan menghilangkan log yang lebih lama. • Menambahkan jalur S3 dalam pemberitahuan kesehatan untuk kesalahan unggahan file. Sebelumnya, pemberitahuan kesehatan hanya menunjukkan jalur ke file di gateway. Pemberita huan sekarang menunjukk an jalur untuk membantu pengguna menemukan file di S3.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
		• Layanan sekarang mengabaikan pemblokir backend selama penghapus an berbagi file paksa. Sebelumnya, penghapusan paksa akan berhenti tanpa penjelasan saat menghadap i pemblokir. Penghapusan paksa sekarang terus tanpa gangguan dalam skenario ini. Pembaruan Pemeliharaan: • Memperbarui tumpukan NFS. • Upgrade Java 17 JRE. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2024-04-15	1.24.5	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.
2024-04-01	1.24.4	Pembaruan Pemeliharaan: • Mengatasi komponen Network Time Protocol (NTP) yang hilang.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2024-03-18	1.24.3	Pembaruan Pemeliharaan: • Memperbaiki masalah yang terkait dengan kinerja pencarian peka huruf besar/kecil. • Memperbaiki masalah yang menyebabkan proses macet. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.
2024-01-12	1.24.2	Pembaruan Pemeliharaan: • Mengatasi masalah pencatatan SMB.
2023-12-27	1.24.1	Pembaruan Pemeliharaan: • Mengatasi masalah stabilitas SMB.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis

2023-12-01	1.24.0	Fitur-fitur:
		• Tumpukan SMB yang diperbarui.
		  • Menambahkan dukungan untuk AES-256 enkripsi, ditambah varian AES-128 enkripsi dan penandata nganan yang lebih aman saat menggunakan klien SMB 3.1.1 yang memintanya.
		  • SMBv1 (LANMAN/C IFS) salinan sisi server dan fungsionalitas ekspansi wildcard sisi server telah dihapus. (SMBv2 dan SMBv3 tidak terpengaruh.) Hal ini dapat berdampak negatif pada kinerja beban kerja SMBv1 tertentu. Jika Anda menggunakan SMBv1, Anda dianjurka n untuk bermigrasi ke SMBv2 atau SMBv3.
		
		Pembaruan Pemeliharaan:
		• Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkat kan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2023-10-24	1.23.2	Pembaruan Pemeliharaan: • Memperbaiki masalah terkait Saluran Dukungan yang tidak terhubung dengan benar untuk pengguna tertentu.
2023-08-14	1.23.1	Pembaruan Pemeliharaan: • Server NTP yang diperbarui untuk menggunakan server sinkronisasi untuk gateway baru.
2023-06-12	1.23.0	Fitur-fitur: • Peningkatan utas unggahan untuk beberapa AWS akun. Pembaruan Pemeliharaan: • Memperbaiki masalah pelanggaran akses pada salinan besar. • Memperbaiki masalah NFS. • Dihapus Java 8. • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2023-04-19	1.22.1	Pembaruan Pemeliharaan: • Memperbaiki masalah yang terkait dengan mengganti nama folder dan file.
2023-01-18	1.22.0	Fitur-fitur: • Ditambahkan dukungan untuk atribut DOS. • Meningkatkan jumlah pembagian file yang didukung per gateway dari 10 menjadi 50. • Menerapkan mekanisme deteksi kemiringan jam untuk menentukan kapan gateway dan layanan tidak sinkron. Pembaruan Pemeliharaan: • Tumpukan SMB yang diperbarui.
2022-07-06	1.21.2	Pembaruan Pemeliharaan: • Sistem operasi dan elemen perangkat lunak yang diperbarui untuk meningkatkan keamanan dan kinerja.

Tanggal rilis	Versi Perangkat Lunak	Catatan Rilis
2022-02-16	1.21.1	Fitur-fitur: • Menambahkan metrik baru untuk mengganti nama dan penghapusan dalam cache. Pembaruan Pemeliharaan: • Memperbaiki masalah lain-lain.
2022-01-18	1.21.0	Fitur-fitur: • Menambahkan CloudWatch metrik baru. • Ditambahkan bandwidth throttling untuk upload data.
2021-12-12	1.20.0	***URGENT UPDATE***: • Mengatasi kerentanan Log4j.

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