Panduan Pengguna Amazon FSx File Gateway

AWS Storage Gateway

Versi API 2021-03-31

AWS Storage Gateway: Panduan Pengguna Amazon FSx File Gateway

Table of Contents

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

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

Apa itu Amazon FSx File Gateway

Amazon FSx File Gateway (FSx File Gateway) adalah jenis File Gateway baru yang menyediakan latensi rendah dan akses efisien ke in-cloud FSx untuk berbagi file Windows File Server dari fasilitas lokal Anda. Jika Anda mempertahankan penyimpanan file lokal karena persyaratan latensi atau bandwidth, Anda dapat menggunakan FSx File Gateway untuk akses tanpa batas ke berbagi file Windows yang terkelola sepenuhnya, sangat andal, dan hampir tidak terbatas yang disediakan di AWS Cloud by FSx for Windows File Server.

Manfaat menggunakan Amazon FSx File Gateway

FSx File Gateway memberikan manfaat berikut:

- Membantu menghilangkan server file lokal dan mengkonsolidasikan semua datanya AWS untuk memanfaatkan skala dan ekonomi penyimpanan cloud.
- Menyediakan opsi yang dapat Anda gunakan untuk semua beban kerja file, termasuk yang memerlukan akses lokal ke data cloud.
- Aplikasi yang perlu tetap berada di tempat sekarang dapat mengalami latensi rendah dan kinerja tinggi yang sama dengan yang mereka miliki AWS, tanpa membebani jaringan Anda atau memengaruhi latensi yang dialami oleh aplikasi Anda yang paling menuntut.

Cara kerja Amazon FSx File Gateway

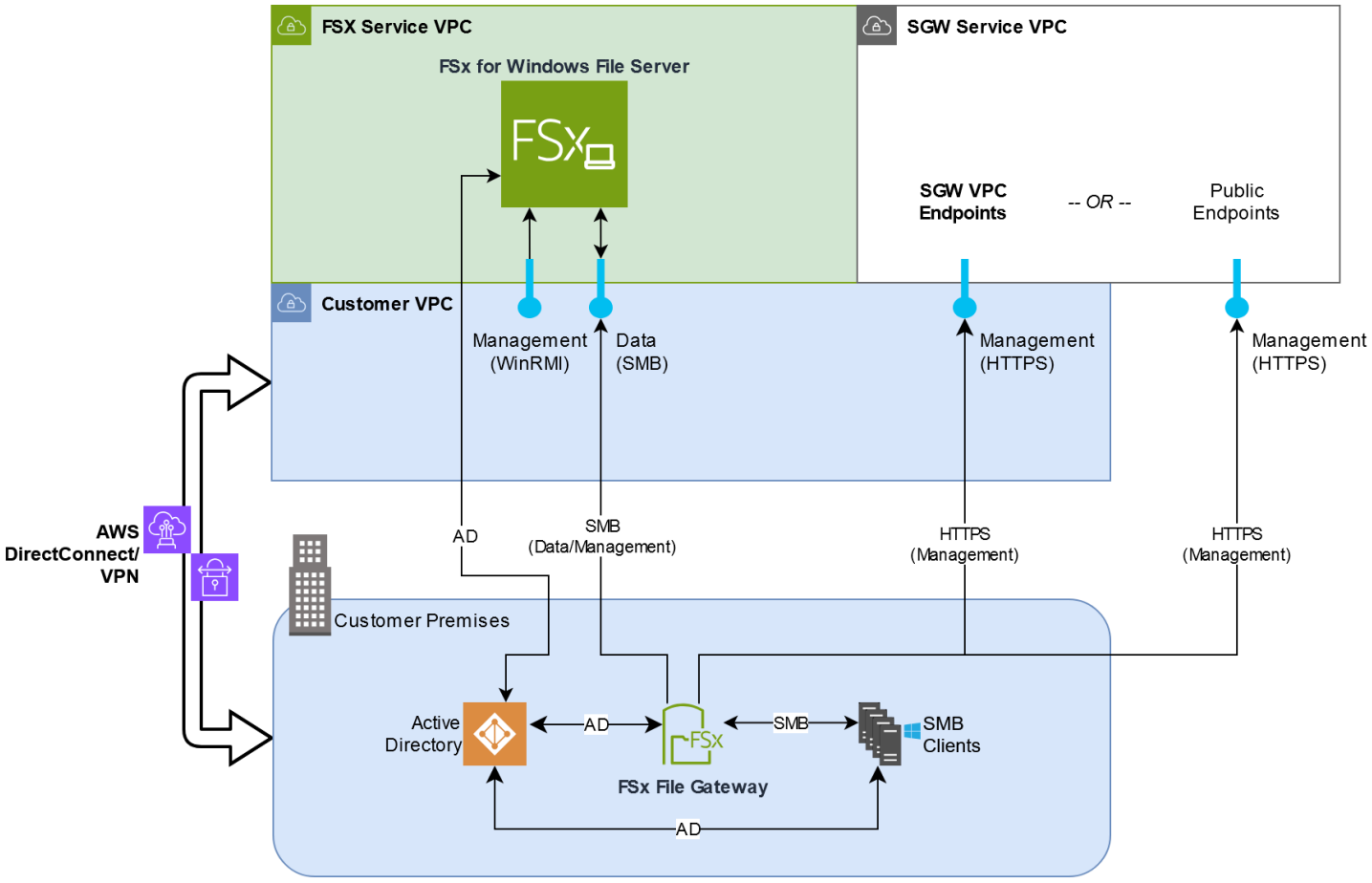
Untuk menggunakan Amazon FSx File Gateway (FSx File Gateway), Anda harus memiliki setidaknya satu sistem file Amazon FSx untuk Windows File Server. Anda juga harus memiliki akses lokal FSx untuk Windows File Server, baik melalui VPN atau melalui Direct Connect koneksi. Untuk informasi selengkapnya tentang menggunakan sistem FSx file Amazon, lihat Apa itu Amazon FSx untuk Windows File Server?

Anda menerapkan gateway ke lingkungan lokal Anda sebagai mesin virtual (VM) yang berjalan, VMware ESXi Microsoft Hyper-V, atau Linux Kernel-based Virtual Machine (KVM), atau sebagai perangkat keras yang Anda pesan dari pengecer pilihan Anda. Anda juga dapat menerapkan Storage Gateway VM di VMware Cloud on AWS, atau sebagai AMI di Amazon. EC2 Setelah menerapkan perangkat, Anda mengaktifkan FSx File Gateway dari konsol Storage Gateway atau melalui Storage Gateway API.

Setelah Amazon FSx File Gateway diaktifkan dan dapat mengakses FSx untuk Windows File Server, gunakan konsol Storage Gateway untuk bergabung ke domain Microsoft Active Directory Anda. Setelah gateway berhasil bergabung dengan domain, Anda menggunakan konsol Storage Gateway untuk melampirkan gateway ke Server File Windows yang sudah ada FSx . FSx untuk Windows File Server membuat semua saham di server tersedia sebagai saham di Amazon FSx File Gateway Anda. Anda kemudian dapat menggunakan klien untuk menelusuri dan terhubung ke berbagi file di FSx File Gateway yang sesuai dengan FSx File Gateway yang dipilih.

Ketika berbagi file terhubung, Anda dapat membaca dan menulis file Anda secara lokal, sambil memanfaatkan semua fitur yang tersedia FSx untuk Windows File Server. FSx File Gateway memetakan berbagi file lokal dan isinya ke berbagi file yang disimpan dari jarak jauh FSx untuk Windows File Server. Ada korespondensi 1:1 antara file jarak jauh dan yang terlihat secara lokal dan bagiannya.

Diagram berikut memberikan gambaran umum tentang penyebaran penyimpanan file untuk Storage Gateway.



Perhatikan hal berikut dalam diagram:

- Direct Connect atau VPN diperlukan untuk mengizinkan FSx File Gateway mengakses berbagi FSx file Amazon menggunakan SMB dan mengizinkan Server File Windows FSx untuk bergabung dengan domain Active Directory lokal Anda.
- Amazon Virtual Private Cloud (Amazon VPC) diperlukan untuk terhubung ke VPC layanan Windows File Server dan VPC layanan Storage Gateway menggunakan endpoint pribadi. FSx FSx File Gateway juga dapat terhubung ke titik akhir publik.

Anda dapat menggunakan Amazon FSx File Gateway di semua AWS Wilayah di mana FSx untuk Windows File Server tersedia.

Memulai dengan AWS Storage Gateway

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

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

Topik

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

Mendaftar Amazon Web Services

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

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

Untuk mendaftar untuk Akun AWS

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

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

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

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

Buat pengguna IAM dengan hak administrator

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

Untuk membuat pengguna administrator, pilih salah satu opsi berikut.

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

Warning

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

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

Mengakses AWS Storage Gateway

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

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

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

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

Wilayah AWS yang mendukung Storage Gateway

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

EC2 mendukung replikasi lintas Wilayah. Beberapa layanan, seperti AWS Identity and Access Management, tidak memiliki sumber daya Regional. Anda dapat meluncurkan AWS sumber daya di lokasi yang memenuhi persyaratan bisnis Anda. Misalnya, Anda mungkin ingin meluncurkan 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.

Amazon FSx File Gateway menyimpan data file di AWS Wilayah tempat sistem FSx file Amazon Anda berada. Sebelum Anda mulai menerapkan gateway Anda, pilih Wilayah di sudut kanan atas konsol Storage Gateway.

- Amazon FSx File Gateway - Untuk AWS Wilayah yang didukung dan daftar titik akhir AWS layanan yang dapat Anda gunakan dengan Amazon FSx File Gateway, lihat titik akhir dan kuota Amazon FSx File Gateway di. Referensi Umum AWS
- Storage Gateway — Untuk AWS Wilayah yang didukung 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
- Storage Gateway Hardware Appliance — Untuk Wilayah yang didukung yang dapat Anda gunakan dengan AWS Storage Gateway perangkat 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 pengaturan gateway sebelum menerapkan gateway.

Topik

Prasyarat

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

- Buat dan konfigurasikan sistem file Windows File Server FSx untuk Windows. Untuk petunjuk, lihat Langkah 1: Membuat Sistem File Anda di Amazon FSx untuk Panduan Pengguna Server File Windows.
- Konfigurasikan Microsoft Active Directory (AD) dan buat akun layanan Active Directory dengan izin yang diperlukan. Untuk informasi selengkapnya, lihat izin akun layanan Direktori Aktif.
- 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.

Persyaratan perangkat keras untuk lokal VMs

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

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. Instans berbasis ARM yang menggunakan prosesor Graviton tidak didukung.

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

Direkomendasikan untuk tipe File Gateway

- Keluarga instance tujuan umum — tipe instans m5, m6, atau m7. Pilih ukuran instans xlarge atau lebih tinggi untuk memenuhi persyaratan prosesor dan RAM Storage Gateway.

- Keluarga instans yang dioptimalkan komputasi — tipe instans c5, c6, atau c7. Pilih ukuran instans 2xlarge atau lebih tinggi untuk memenuhi persyaratan prosesor dan RAM Storage Gateway.
- Keluarga instans yang dioptimalkan untuk memori — tipe instans r5, r6, atau r7. Pilih ukuran instans xlarge atau lebih tinggi untuk memenuhi persyaratan prosesor dan RAM Storage Gateway.
- Keluarga instans yang dioptimalkan untuk penyimpanan — 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.

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.

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

FSx 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 titik akhir VPC.

Untuk FSx File Gateway, Anda harus menggunakan Microsoft Active Directory untuk memungkinkan pengguna domain mengakses berbagi file Blok Pesan Server (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.

untuk FSx 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.

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
								VM Storage Gateway tidak memerlukan port 80 agar dapat diakses publik. Tingkat akses yang diperlukan ke port 80 tergantung pada konfigurasi jaringan Anda. Jika Anda mengaktifkan gateway dari Storage Gateway Management Console, host

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
								tempat Anda terhubung ke konsol harus memiliki akses ke port gateway 80 Anda.
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.
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	UDP NetBIOS	137	✓	✓	✓	Nama layanan
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	UDP NetBIOS	138	✓	✓	✓	Layanan datagram
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	LDAP TCP & UDP	389	✓	✓	✓	Koneksi klien Directory System Agent (DSA)

Elemen Jaringan	Dari	Ke	Protokol	Port	Ke dalam	Ke luar	Diperlukan	Catatan
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	TCP & UDP Kerberos	88	✓	✓	✓	Kerberos
Microsoft Active Directory	Storage Gateway VM	Server Direktori Aktif	Pemetaar Environme nt/End Titik Komputas Terdistri busi TCP (DCE/ EMAP)	135	✓	✓	✓	RPC
FSx Koneksi Amazon	Storage Gateway VM	FSx untuk Windows File Server	TCP atau UDP SMBv3	445	✓	✓	✓	Layanan sesi transfer data berbagi file

Persyaratan jaringan dan firewall untuk Storage Gateway Hardware Appliance

Setiap Storage Gateway Hardware Appliance memerlukan layanan jaringan berikut:

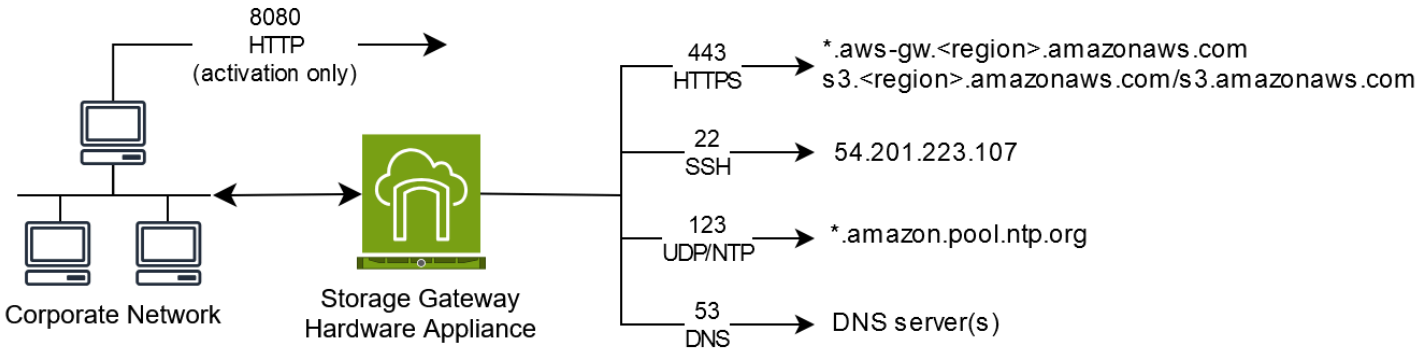
- Akses Internet — koneksi jaringan yang selalu aktif ke internet melalui antarmuka jaringan apa pun di server.
- Layanan DNS — Layanan DNS untuk komunikasi antara perangkat keras dan server DNS.
- Sinkronisasi waktu - layanan waktu Amazon NTP yang dikonfigurasi secara otomatis harus dapat dijangkau.

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

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

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

Anda dapat menggunakan port IDRac untuk manajemen server jarak jauh.



Alat perangkat keras membutuhkan port berikut untuk beroperasi.

Protokol	Port	Arahan	Sumber	Tujuan	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

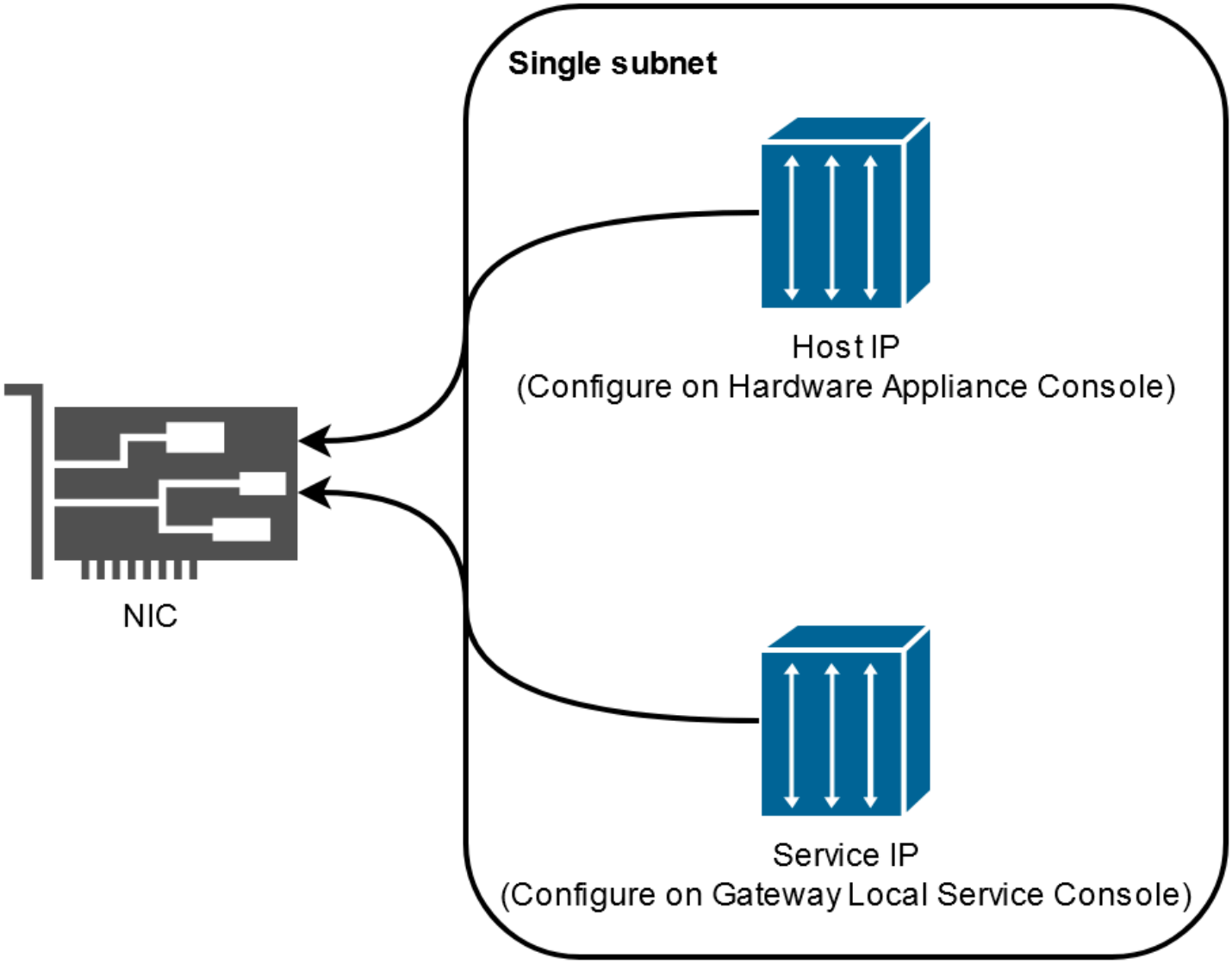
Protokol	Port	Arahan	Sumber	Tujuan	Penggunaan
UDP/NTP	123	Ke luar	Alat perangkat keras	`*.amazon.pool.ntp.org`	Sinkronisasi waktu
HTTPS	443	Ke luar	Alat perangkat keras	`*.amazonaws.com`	Transfer data
HTTP	8080	Ke dalam	AWS	Alat perangkat keras	Aktivasi (hanya sebentar)

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

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

> **Note**
>
> Untuk ilustrasi yang menunjukkan bagian belakang server dengan port-portnya, 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 Storage Gateway Hardware Appliance

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 IPv4 lalu lintas 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
```

Selain Storage Gateway dan endpoint layanan Amazon S3, Storage Gateway VMs 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.

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.
- Mesin Virtual berbasis Kernel Linux (KVM) – Sebuah teknologi virtualisasi gratis, sumber terbuka. KVM disertakan dalam semua versi Linux versi 2.6.20 dan yang lebih baru. Storage Gateway diuji dan didukung untuk distribusi CentOS/RHEL 7.7, 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 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 (Acropolis Hypervisor) dimulai dengan versi 10.0.1.1 — Platform virtualisasi berbasis KVM 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 FSx Amazon EC2 default untuk 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 SMB yang didukung untuk File Gateway

File Gateway mendukung klien Blok Pesan Layanan (SMB) berikut:

- Microsoft Windows Server 2008 R2 dan yang lebih baru
- Versi desktop Windows: 10, 8, dan 7.
- Windows Terminal Server berjalan pada Windows Server 2008 dan yang lebih baru

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

Operasi sistem file yang didukung untuk File Gateway

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

Menulis dan membaca dioptimalkan karena hanya bagian yang diubah atau diminta yang ditransfer melalui gateway Anda. Menghapus menghapus file dari Amazon FSx.

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 tertunda diunggah ke . 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 , pertimbangkan berapa banyak disk cache yang akan dialokasikan. File Gateway menggunakan algoritma yang paling jarang digunakan untuk secara otomatis mengusir data dari cache. Cache pada 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), 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 File Gateway 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/rumah.
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

Kami tidak merekomendasikan penggunaan disk sementara untuk penyimpanan cache di FSx File Gateways.

Disk ephemeral menyediakan penyimpanan tingkat blok sementara untuk instans Amazon EC2 Anda. 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.

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.

Menggunakan AWS Storage Gateway Hardware Appliance

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

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

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

Menyiapkan AWS Storage Gateway Hardware Appliance

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

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

Untuk menginstal dan mengkonfigurasi alat perangkat keras Anda

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

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, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), atau Amazon EC2.

Meningkatkan penyimpanan cache yang dapat digunakan

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

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

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

Opsi kartu antarmuka jaringan

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

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

Memasang alat perangkat keras Anda secara fisik

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

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

Prasyarat

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

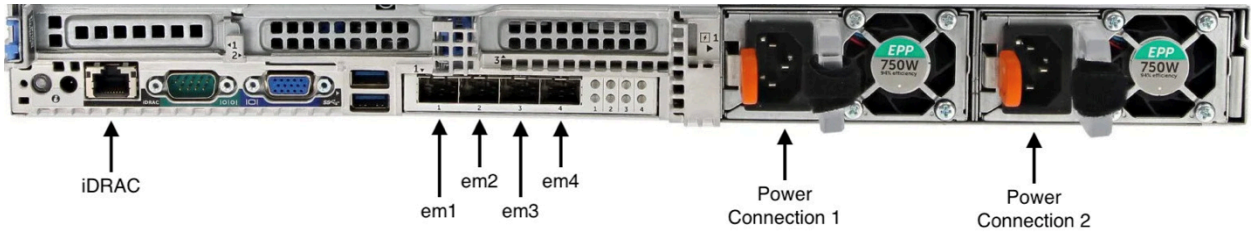
- Kabel daya: satu diperlukan, dua direkomendasikan.
- Kabel jaringan yang didukung (tergantung pada Kartu Antarmuka Jaringan (NIC) yang disertakan dalam alat perangkat keras). Twinax Copper DAC, modul optik SFP+(kompatibel dengan Intel) atau transceiver tembaga SFP ke Base-T.
- Keyboard dan monitor,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

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

Untuk menginstal alat perangkat keras Anda secara fisik

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

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



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

2. Colokkan sambungan daya ke masing-masing dari dua catu daya. Dimungkinkan untuk menyambungkan hanya ke satu koneksi daya, tetapi kami merekomendasikan koneksi daya ke kedua catu daya untuk redundansi.
3. Colokkan kabel Ethernet ke `em1` port untuk menyediakan koneksi internet yang selalu aktif. `em1`Port adalah yang pertama dari empat port jaringan fisik di belakang, dari kiri ke kanan.

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

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

bagian depan alat perangkat keras dengan label tombol daya.

Langkah selanjutnya

[Mengakses konsol alat perangkat keras]

Mengakses konsol alat perangkat keras

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

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

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

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

Untuk menyetel kata sandi admin

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

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

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

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

Langkah selanjutnya

Mengkonfigurasi parameter jaringan alat perangkat keras

Mengkonfigurasi parameter jaringan alat perangkat keras

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

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

Untuk mengatur alamat jaringan

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

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

Perhatikan alamat ini untuk digunakan nanti dalam langkah aktivasi.

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

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

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

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

Untuk keluar dari konsol perangkat keras

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

Langkah selanjutnya

Mengaktifkan AWS Storage Gateway Hardware Appliance

Mengaktifkan AWS Storage Gateway Hardware Appliance

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

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

Setelah mengonfigurasi alamat IP Anda, Anda memasukkan alamat IP ini di halaman Perangkat Keras AWS Storage Gateway konsol untuk mengaktifkan alat perangkat keras Anda. Proses aktivasi mendaftarkan alat ke AWS akun Anda.

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

Untuk mengaktifkan AWS Storage Gateway Hardware Appliance

1. Buka Konsol AWS Storage Gateway Manajemen dan masuk dengan kredensyal akun yang ingin Anda gunakan untuk mengaktifkan perangkat keras Anda.

   > **Note**
   >
   > Untuk aktivasi saja, berikut ini harus benar:
   >
   > - Browser Anda harus berada di jaringan yang sama dengan perangkat keras Anda.
   > - Firewall Anda harus mengizinkan akses HTTP pada port 8080 ke alat untuk lalu lintas masuk.

2. Pilih Hardware dari menu navigasi di sisi kiri halaman.
3. Pilih Aktifkan alat.
4. Untuk Alamat IP, masukkan alamat IP yang Anda konfigurasikan untuk perangkat keras Anda, lalu pilih Connect.

   Untuk informasi selengkapnya tentang mengonfigurasi alamat IP, lihat .
5. Untuk Nama, masukkan nama untuk perangkat keras Anda. Nama dapat mencapai 255 karakter dan tidak dapat menyertakan karakter garis miring.
6. Untuk zona waktu perangkat keras, masukkan zona waktu lokal dari mana sebagian besar beban kerja untuk gateway akan dihasilkan., lalu pilih Berikutnya.

   Zona waktu mengontrol saat pembaruan perangkat keras berlangsung, dengan jam 2 pagi digunakan sebagai waktu terjadwal default untuk melakukan pembaruan. Idealnya, jika zona

waktu diatur dengan benar, pembaruan akan dilakukan di luar jendela hari kerja lokal secara default.

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

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

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

Langkah selanjutnya

Membuat gateway pada alat perangkat keras Anda

Membuat gateway pada 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.

Anda dapat membuat S3 File Gateway, FSx File Gateway, Tape Gateway, atau Volume Gateway pada AWS Storage Gateway Hardware Appliance 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/rumah.
2. Ikuti prosedur yang dijelaskan dalam Membuat Gateway Anda untuk menyiapkan, menghubungkan, dan mengonfigurasi jenis Storage Gateway yang ingin Anda gunakan.

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

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

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

   Masukkan angka yang sesuai untuk menavigasi ke halaman Konfigurasi Jaringan.

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

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

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

Untuk keluar dari konsol lokal gateway

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

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

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

Menghapus perangkat lunak gateway dari alat perangkat keras Anda

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

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

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

Untuk menghapus gateway dari alat perangkat keras

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

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

> **Note**
>
> Setelah Anda menghapus perangkat lunak gateway, Anda tidak dapat membatalkan tindakan. Untuk jenis gateway tertentu, Anda dapat kehilangan data saat penghapusan, terutama data yang di-cache. Untuk informasi selengkapnya tentang menghapus gateway, lihatMenghapus gateway Anda dan menghapus sumber daya terkait.

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

Menghapus AWS Storage Gateway Hardware Appliance

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

Jika Anda tidak lagi memerlukan 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.

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

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

Ikhtisar - Aktivasi Gateway

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

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.

Buat sistem file Amazon FSx untuk Windows File Server

Untuk membuat Amazon FSx File Gateway di AWS Storage Gateway, langkah pertama adalah membuat sistem file Amazon FSx untuk Windows File Server. Jika Anda sudah membuat sistem FSx file Amazon, lanjutkan ke langkah berikutnya,Membuat dan mengaktifkan Amazon FSx File Gateway.

Note

Batasan berikut berlaku saat menulis ke sistem FSx file Amazon dari FSx File Gateway:

- Sistem FSx file Amazon dan FSx File Gateway Anda harus dimiliki oleh AWS akun yang sama dan terletak di AWS Wilayah yang sama.
- Setiap gateway dapat mendukung lima sistem file terlampir. Saat melampirkan sistem file, konsol Storage Gateway memberi tahu Anda jika gateway yang dipilih berkapasitas. Dalam hal ini, Anda harus memilih gateway yang berbeda atau melepaskan sistem file sebelum Anda dapat melampirkan yang lain.
- FSx File Gateway mendukung kuota penyimpanan lunak (mengeluarkan peringatan ketika pengguna melampaui batas data mereka), tetapi tidak mendukung kuota keras (menegakkan batas data dengan menolak akses tulis). Kuota lunak didukung untuk semua pengguna kecuali pengguna FSx admin Amazon. Untuk informasi selengkapnya tentang mengatur kuota penyimpanan, lihat Kuota penyimpanan di Panduan Pengguna Amazon FSx untuk Windows File Server.
- Kami tidak menyarankan menggunakan Microsoft Distributed File System (DFS) untuk mengarahkan pengguna ke sistem FSx file Amazon Anda melalui FSx File Gateway. Sebagai gantinya, konfigurasikan DFS untuk mengarahkan langsung ke sistem FSx file Amazon AWS Cloud seperti yang dijelaskan dalam Mengelompokkan beberapa sistem file dengan Ruang Nama DFS di FSx Amazon untuk Panduan Pengguna Server File Windows.
- Beberapa operasi file pada FSx File Gateway, seperti penggantian nama folder tingkat atas atau perubahan izin, dapat menghasilkan beberapa operasi file yang mengarah ke I/O beban tinggi pada sistem file Windows File Server Anda FSx . Jika sistem file Anda tidak memiliki sumber daya kinerja yang cukup untuk beban kerja Anda, sistem file mungkin menghapus salinan bayangan karena memprioritaskan ketersediaan untuk berkelanjutan I/O daripada retensi salinan bayangan historis.

  Di FSx konsol Amazon, periksa halaman Pemantauan dan kinerja untuk melihat apakah sistem file Anda kurang disediakan. Jika ya, Anda dapat beralih ke penyimpanan SSD, meningkatkan kapasitas throughput, atau meningkatkan IOPS SSD untuk menangani beban kerja Anda.

Untuk membuat sistem file Windows File Server FSx untuk Windows

1. Buka Konsol Manajemen AWS di https://console.aws.amazon.com/fsx/rumah/, dan pilih Wilayah tempat Anda ingin membuat gateway Anda.
2. Ikuti petunjuk di Memulai Amazon FSx di Panduan Pengguna Server File Amazon FSx untuk Windows.

Membuat dan mengaktifkan Amazon FSx File Gateway

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

Topik

- Siapkan Gateway FSx File Amazon
- Hubungkan Amazon FSx File Gateway Anda ke AWS
- Tinjau pengaturan dan aktifkan Amazon FSx File Gateway Anda
- Konfigurasikan Gateway FSx File Amazon Anda

Siapkan Gateway FSx File Amazon

Untuk menyiapkan FSx File Gateway 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 FSx 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.
   - 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 Amazon FSx File Gateway Anda ke AWS

Untuk menghubungkan FSx File Gateway baru ke AWS

1. Jika Anda belum melakukannya, selesaikan prosedur yang dijelaskan di Siapkan Gateway FSx File Amazon. Setelah selesai, pilih Berikutnya untuk membuka AWS halaman Connect to di AWS Storage Gateway konsol.
2. Di bagian opsi Endpoint, untuk titik akhir Layanan, pilih jenis titik akhir yang akan digunakan gateway Anda untuk berkomunikasi. AWS Anda dapat memilih dari opsi berikut:

- Dapat diakses publik — Gateway Anda berkomunikasi AWS melalui internet publik. Jika Anda memilih opsi ini, gunakan kotak centang titik akhir yang diaktifkan FIPS untuk menentukan apakah koneksi harus mematuhi Standar Pemrosesan Informasi Federal (FIPS).

  > **Note**
  >
  > Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir yang sesuai dengan FIPS. Untuk informasi selengkapnya, lihat Federal Information Processing Standard (FIPS) 140-2.
  >
  > Titik akhir layanan FIPS hanya tersedia di beberapa AWS Wilayah. Untuk informasi selengkapnya, lihat 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).

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

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

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

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

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

Tinjau pengaturan dan aktifkan Amazon FSx File Gateway Anda

Untuk mengaktifkan FSx File Gateway baru

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

   - Siapkan Gateway FSx File Amazon
   - Hubungkan Amazon FSx File Gateway 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.

Konfigurasikan Gateway FSx File Amazon Anda

Untuk melakukan konfigurasi pertama kali pada FSx File Gateway baru

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

   - Siapkan Gateway FSx File Amazon
   - Hubungkan Amazon FSx File Gateway Anda ke AWS
   - Tinjau pengaturan dan aktifkan Amazon FSx File Gateway

   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 diberikan secara otomatis 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 diberi tahu 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 gunakan CloudWatch alarm untuk diberi tahu 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 Anda telah membuat gateway Anda, Anda harus melampirkan sistem file untuk digunakan. Untuk petunjuk, lihat Melampirkan sistem file Amazon FSx untuk Windows File Server.

Jika Anda tidak memiliki sistem FSx file Amazon yang ada untuk dilampirkan, Anda harus membuatnya. Untuk petunjuk, lihat Memulai Amazon FSx.

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 dan dapatkan ID titik akhir VPC, lalu tentukan ID titik akhir VPC ini saat Anda membuat dan mengaktifkan gateway. Untuk informasi selengkapnya, lihat File Amazon Anda. AWS

Untuk mengonfigurasi FSx File Gateway Anda untuk mentransfer data melalui VPC, Anda harus membuat VPN atau AWS DirectConnect tautan antara Amazon FSx untuk Windows File Server VPC dan jaringan tempat gateway Anda digunakan.

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

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 Create dan mengaktifkan Amazon FSx File Gateway.

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

Konfigurasikan pengaturan akses domain Microsoft Active Directory

Pada langkah ini, Anda mengonfigurasi pengaturan akses untuk bergabung dengan Amazon FSx File Gateway Anda ke domain Microsoft Active Directory.

Untuk mengkonfigurasi pengaturan Active Directory

1. Di konsol Storage Gateway, pilih sistem FSx file dari menu navigasi.
2. Pilih Lampirkan sistem FSx file.
3. Pada halaman Confirm gateway, pilih gateway yang ingin Anda gabungkan ke domain Active Directory dari menu drop-down.

   Jika Anda tidak memiliki gateway, Anda harus membuatnya. Pastikan gateway Anda dapat menyelesaikan nama Active Directory Domain Controller Anda. Untuk informasi, lihat Prasyarat.
4. Masukkan nilai untuk pengaturan Active Directory:

   > **Note**
   >
   > Jika gateway Anda sudah bergabung dengan domain, Anda tidak perlu bergabung lagi. Pergi ke langkah berikutnya.

   - Untuk nama Domain, masukkan nama domain Active Directory yang ingin Anda gunakan.
   - Untuk pengguna Domain, masukkan nama pengguna pengguna Active Directory yang ingin Anda gunakan untuk bergabung dengan gateway ke domain. Pengguna ini harus memiliki izin yang diperlukan. Untuk selengkapnya, lihat akun layanan Direktori Aktif.
   - Untuk kata sandi Domain, masukkan kata sandi untuk pengguna.
   - Untuk unit Organisasi- opsional, Anda dapat menentukan unit organisasi yang menjadi milik Active Directory.

     > **Note**
     >
     > Jika Anda membiarkan bidang ini kosong, bergabung dengan domain akan 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 Active Directory 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.

- Masukkan nilai untuk pengontrol Domain - opsional.

5. Pilih Berikutnya untuk membuka halaman Attach FSx File system.

Langkah selanjutnya

Lampirkan sistem file Amazon FSx untuk Windows File Server

Lampirkan sistem file Amazon FSx untuk Windows File Server

Anda harus memiliki sistem file FSx untuk Windows File Server sebelum Anda dapat melampirkannya ke FSx File Gateway. Jika Anda tidak memiliki sistem file, Anda harus membuatnya. Untuk petunjuk, lihat Langkah 1: Membuat Sistem File Anda di Amazon FSx untuk Panduan Pengguna Server File Windows.

Langkah selanjutnya adalah melampirkan sistem FSx file Amazon ke gateway. Saat Anda melampirkan sistem FSx file Amazon, semua pembagian file pada sistem file tersedia untuk Amazon FSx File Gateway (FSx File Gateway) untuk Anda pasang.

> **Note**
>
> Batasan berikut berlaku saat menulis ke sistem FSx file Amazon dari Amazon FSx File Gateway:
>
> - Sistem FSx file Amazon Anda dan FSx File Gateway Anda harus dimiliki oleh yang sama Akun AWS dan terletak di tempat yang sama Wilayah AWS.
> - Setiap gateway dapat mendukung hingga lima sistem file terlampir. Saat Anda melampirkan sistem file, konsol Storage Gateway akan memberi tahu Anda jika gateway yang dipilih berkapasitas. Dalam hal ini, Anda harus memilih gateway yang berbeda atau melepaskan sistem file sebelum Anda dapat melampirkan yang lain.
> - FSx File Gateway mendukung kuota penyimpanan lunak (yang memperingatkan Anda ketika pengguna melampaui batas data mereka), tetapi tidak mendukung kuota keras (yang memberlakukan batas data dengan menolak akses tulis). Kuota lunak didukung untuk semua pengguna kecuali pengguna FSx admin Amazon. Untuk informasi selengkapnya tentang menyiapkan kuota penyimpanan, lihat Kuota penyimpanan di FSx Panduan Pengguna Amazon.
> - Kami tidak menyarankan menggunakan Microsoft Distributed File System (DFS) untuk mengarahkan pengguna ke sistem FSx file Amazon Anda melalui FSx File Gateway. Sebagai gantinya, konfigurasikan DFS untuk mengarahkan langsung ke sistem FSx file Amazon AWS Cloud seperti yang dijelaskan dalam Mengelompokkan beberapa sistem file dengan Ruang Nama DFS di FSx Amazon untuk Panduan Pengguna Server File Windows.

Untuk melampirkan sistem FSx file Amazon

1. Di konsol Storage Gateway, pada halaman sistem FSx FSx file > Lampirkan sistem file, lengkapi bidang berikut di bagian pengaturan sistem FSx file:

   - Untuk nama sistem FSx file, pilih sistem file yang ingin Anda lampirkan dari daftar dropdown.
   - Untuk alamat IP Endpoint Lokal, masukkan alamat IP gateway yang akan digunakan klien untuk menelusuri berbagi file pada sistem FSx file.

   > **Note**
   >
   > - Anda harus menentukan alamat IP untuk setiap sistem file yang dilampirkan ke gateway.
   > - Untuk EC2 gateway Amazon, Anda dapat menentukan alamat IP pribadi EC2 instance, kecuali jika sudah digunakan oleh sistem file yang berbeda, dalam hal ini Anda harus menambahkan alamat pribadi baru ke gateway, lalu restart. Untuk informasi selengkapnya, lihat Beberapa alamat IP di Panduan EC2 Pengguna Amazon.
   > - Untuk gateway lokal, Anda dapat menentukan alamat IP antarmuka jaringan utama (statis atau DHCP), kecuali jika sudah digunakan oleh sistem file yang berbeda, dalam hal ini Anda harus memberikan alamat IP yang berbeda dari subnet yang sama dengan antarmuka utama, yang akan tersedia sebagai IP virtual. Jangan gunakan alamat IP yang ditetapkan ke antarmuka jaringan apa pun selain yang utama.

2. Di bagian Pengaturan akun layanan, berikan kredenal masuk akun layanan yang terkait dengan sistem file Amazon FSx .

   > **Note**
   >
   > Akun layanan ini harus memiliki hak istimewa Operator Cadangan dari layanan Direktori Aktif yang terkait dengan sistem FSx file Amazon Anda atau memiliki izin yang setara.

> **Important**
>
> Untuk memastikan izin yang memadai untuk file, folder, dan metadata file, sebaiknya Anda menjadikan akun layanan sebagai anggota grup administrator sistem file.
> Jika Anda menggunakan AWS Directory Service Microsoft Active Directory dengan Amazon FSx untuk Windows File Server, akun layanan harus menjadi anggota grup FSx Administrator AWS Delegasi.
> Jika Anda menggunakan Active Directory yang dikelola sendiri dengan Amazon FSx untuk Windows File Server, sebaiknya akun layanan menjadi anggota grup administrator sistem file yang didelegasikan khusus yang Anda tentukan untuk administrasi sistem file saat Anda membuat sistem file Amazon FSx .
> Jika Anda memilih untuk tidak membuat grup administrator sistem file yang didelegasikan khusus saat Anda membuat sistem FSx file Amazon, grup defaultnya adalah Admin Domain. Meskipun Anda dapat menjadikan akun layanan sebagai anggota grup ini, itu tidak disarankan sebagai praktik terbaik.
> Untuk informasi selengkapnya, lihat Mendelegasikan hak istimewa ke akun FSx layanan Amazon Anda di Panduan Pengguna Amazon FSx untuk Windows File Server.

3. Di bagian Log audit, pilih Grup log yang ada, dan pilih log yang ingin Anda gunakan untuk memantau akses ke sistem FSx file Amazon Anda. Anda dapat membuat yang baru. Jika Anda tidak ingin memantau sistem Anda, pilih Nonaktifkan logging.
4. Untuk pengaturan penyegaran cache otomatis, jika Anda ingin cache disegarkan secara otomatis, pilih Setel interval penyegaran dan tentukan interval antara 5 menit dan 30 hari.
5. (Opsional) Di bagian Tag, pilih Tambahkan tag baru untuk menambahkan satu atau beberapa kunci dan nilai untuk menandai pengaturan Anda.
6. Pilih Berikutnya dan tinjau pengaturannya. Untuk mengubah pengaturan Anda, Anda dapat memilih Edit di setiap bagian.
7. Setelah selesai, pilih Selesai.

Langkah selanjutnya

Pasang dan gunakan berbagi FSx file Amazon Anda

Pasang dan gunakan berbagi FSx file Amazon Anda

Sebelum memasang berbagi file Anda di klien, tunggu status sistem FSx file Amazon berubah menjadi Tersedia. Setelah berbagi file Anda dipasang, Anda dapat mulai menggunakan Amazon FSx File Gateway (FSx File Gateway).

Topik

Pasang berbagi file SMB Anda di klien Anda

Pada langkah ini, Anda me-mount berbagi file SMB 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 adalah beberapa opsi tambahan untuk dicoba.

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

- `net use`Perintah - Tidak bertahan di seluruh reboot sistem, kecuali Anda menggunakan sakelar. `/persistent:(yes:no)`
- Utilitas baris `CmdKey` perintah — Membuat koneksi persisten ke file share SMB yang terpasang yang tersisa setelah reboot.
- Drive jaringan yang dipetakan di File Explorer - Mengonfigurasi berbagi file yang dipasang untuk menyambung kembali saat masuk dan mengharuskan Anda memasukkan kredensil jaringan Anda.
- PowerShell script — Dapat persisten, dan dapat terlihat atau tidak terlihat oleh sistem operasi saat dipasang.

> **Note**
>
> Jika Anda adalah pengguna Microsoft Active Directory, tanyakan kepada administrator Anda untuk memastikan bahwa Anda memiliki akses ke berbagi file SMB sebelum memasang file share ke sistem lokal Anda.
> Amazon FSx File Gateway tidak mendukung penguncian SMB atau atribut yang diperluas SMB.

Untuk me-mount file share SMB untuk pengguna Active Directory menggunakan perintah net use

1. Pastikan Anda memiliki akses ke berbagi file SMB sebelum memasang file share ke sistem lokal Anda.
2. Untuk klien Microsoft Active Directory, masukkan perintah berikut pada prompt perintah:

   ```
   net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
   ```

Untuk me-mount berbagi file SMB di Windows menggunakan CmdKey

1. Tekan tombol Windows dan enter **cmd** untuk melihat item menu command prompt.
2. Buka menu konteks (klik kanan) untuk Command Prompt, dan pilih Run as administrator.
3. Masukkan perintah berikut:

   ```
   C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
   ```

> **Note**
>
> Saat memasang file share, Anda mungkin perlu melakukan remount file share setelah me-reboot klien Anda.

Untuk me-mount berbagi file SMB menggunakan Windows File Explorer

1. Tekan tombol Windows dan masukkan **File Explorer** di kotak Cari Windows, atau tekan**Win +E**.
2. Di panel navigasi, pilih PC ini. Kemudian, pada tab Komputer, pilih Peta drive jaringan.
3. Dalam kotak dialog Map network drive, pilih huruf drive untuk Drive.
4. Untuk Folder, masukkan**\\[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 Active Directory atau kata sandi pengguna akun tamu.

7. Pilih Selesai untuk menyelesaikan titik pemasangan Anda.

Uji FSx File Gateway Anda

Anda dapat menyalin file dan direktori ke drive yang dipetakan. File secara otomatis mengunggah ke sistem file Windows File Server Anda FSx .

Untuk mengunggah file dari klien Windows Anda ke Amazon FSx

1. Pada klien Windows Anda, navigasikan ke drive tempat Anda memasang sistem file Anda. Nama drive didahului dengan nama sistem file Anda.
2. Salin file atau direktori ke drive.

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

Mengelola sumber daya Amazon FSx File Gateway

Bagian berikut memberikan informasi tentang cara mengelola sumber daya Amazon FSx File Gateway (FSx File Gateway) Anda, termasuk melampirkan dan melepaskan sistem FSx file Amazon, dan mengonfigurasi pengaturan Microsoft Active Directory.

Topik

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.

Status	Arti
`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.

Memahami status sistem berkas

Anda dapat melihat kesehatan sistem file secara sekilas dengan melihat statusnya. Jika status menunjukkan bahwa sistem 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 sistem file di konsol Storage Gateway di kolom Status. Sistem 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	Sistem file dikonfigurasi dengan benar dan tersedia untuk digunakan. Ini adalah status standar untuk sistem file yang berfungsi dengan baik.
CREATING	Sistem file belum sepenuhnya dibuat dan belum siap digunakan. Status CREATING adalah transisi. Tidak ada tindakan yang diperlukan. Jika sistem file macet dalam status ini, itu mungkin karena gateway VM kehilangan koneksi ke AWS.
UPDATING	Konfigurasi sistem file sedang diperbarui. Status UPDATE adalah transisi. Tidak ada tindakan yang diperlukan. Jika sistem file macet dalam status ini, itu mungkin karena gateway VM kehilangan koneksi ke AWS.

Status	Arti
DELETING	Sistem file sedang dihapus. Sistem file tidak dihapus sampai semua data diunggah ke AWS. Status DELETING bersifat transisi, dan tidak ada tindakan yang diperlukan.
FORCE_DELETING	Sistem file sedang dihapus secara paksa. Sistem file segera dihapus dan data tidak diunggah ke AWS. Status FORCE_DELETING bersifat transisi, dan tidak ada tindakan yang diperlukan.
ERROR	Sistem file dalam keadaan tidak sehat. Tindakan diperlukan. Beberapa kemungkinan penyebab termasuk masalah dengan kredensi akses atau hak istimewa, masalah konektivitas, atau ruang penyimpanan yang tidak memadai pada sistem file. Ketika masalah yang menyebabkan keadaan tidak sehat diselesaikan, sistem file kembali ke status AVAILABLE.

Mengedit informasi dasar untuk FSx 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.

Tetapkan tingkat keamanan untuk gateway Anda

Anda dapat mengonfigurasi tingkat keamanan SMB untuk FSx File Gateway Anda untuk menentukan apakah gateway harus memerlukan penandatanganan Blok Pesan Server (SMB) atau enkripsi SMB.

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 keamanan yang lebih tinggi dapat memengaruhi kinerja gateway.

   - Enkripsi wajib - Jika Anda memilih opsi ini, FSx 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 klien SMB di Microsoft Windows 8, Windows Server 2012, atau yang lebih baru.

- Menerapkan enkripsi — Jika Anda memilih opsi ini, FSx 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 klien SMB di Microsoft Windows 8, Windows Server 2012, atau yang lebih baru.
- Menegakkan penandatanganan — Jika Anda memilih opsi ini, FSx File Gateway hanya mengizinkan koneksi dari SMBv2 atau SMBv3 klien yang telah mengaktifkan penandatanganan. Opsi ini bekerja dengan klien SMB di Microsoft Windows Vista, Windows Server 2008, atau yang lebih baru.

> **Note**
>
> Tingkat keamanan default untuk FSx File Gateway adalah Enforce encryption.

5. Pilih Simpan.

Mengedit pengaturan Active Directory untuk n FSx File Gateway

Untuk menggunakan Microsoft Active Directory perusahaan Anda atau AWS Managed Microsoft AD untuk akses yang diautentikasi pengguna ke sistem FSx file Amazon Anda, edit setelan SMB untuk gateway Anda dan berikan kredensi domain Active Directory Anda. Melakukan hal ini memungkinkan gateway Anda untuk bergabung dengan domain Active Directory Anda dan memungkinkan anggota domain untuk mengakses sistem file.

> **Note**
>
> Dengan menggunakan Directory Service, Anda dapat membuat layanan domain Active Directory yang dihosting di 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.

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 ingin gateway Anda bergabung.

   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 akun layanan Direktori Aktif.
   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.

Pengaturan pengeditan untuk sistem FSx file Amazon

Setelah membuat sistem file Amazon FSx untuk Windows File Server, Anda dapat mengedit pengaturan untuk CloudWatch log, penyegaran cache otomatis, dan kredenal akun FSx layanan Amazon.

Untuk mengedit pengaturan sistem FSx file Amazon

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi, pilih Sistem file, dan pilih sistem file yang pengaturannya ingin Anda edit.
3. Untuk Tindakan, pilih Edit pengaturan sistem file.
4. Di bagian pengaturan sistem file, verifikasi gateway, FSx lokasi Amazon, dan informasi alamat IP.

   > **Note**
   >
   > Anda tidak dapat mengedit alamat IP sistem file setelah dilampirkan ke gateway. Untuk mengubah alamat IP, Anda harus melepaskan dan memasang kembali sistem file.

5. Di bagian log Audit, pilih opsi untuk menggunakan grup CloudWatch log untuk memantau akses ke sistem FSx file Amazon. Anda dapat menggunakan grup log yang ada.
6. Untuk pengaturan penyegaran cache otomatis, pilih opsi. Jika Anda memilih Setel interval penyegaran, atur waktu dalam hari, jam, dan menit untuk menyegarkan cache sistem file menggunakan Time To Live (TTL).

   TTL adalah lamanya waktu sejak penyegaran terakhir. Ketika direktori diakses setelah jangka waktu tersebut, File Gateway menyegarkan konten direktori tersebut dari sistem FSx file Amazon.

   > **Note**
   >
   > Nilai interval penyegaran yang valid adalah antara 5 menit dan 30 hari.

7. Di pengaturan akun Layanan - bagian opsional, masukkan nama pengguna dan Kata Sandi. Kredensi ini untuk pengguna yang memiliki peran Administrator Cadangan dari layanan Direktori Aktif yang terkait dengan sistem FSx file Amazon Anda.
8. Pilih Simpan perubahan.

Melepaskan sistem FSx file Amazon

Melepaskan sistem file tidak menghapus data Anda FSx untuk Windows File Server. Data yang ditulis ke sistem file ini sebelum Anda melepaskannya masih akan diunggah ke Windows File FSx Server Anda.

Untuk melepaskan sistem FSx file Amazon

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

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 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 informasi selengkapnya tentang metrik yang digunakan untuk memantau , lihat Memahami metrik gateway dan Memahami metrik file. 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
- Kesalahan sistem file: `FileSystem-ERROR` > = 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 Amazon 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 Anda

Anda dapat memantau 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 File Gateway dengan grup CloudWatch log
- Menggunakan CloudWatch metrik Amazon
- Memahami metrik gateway
- Memahami metrik sistem file
- Memahami

Mendapatkan log kesehatan File Gateway dengan grup CloudWatch log

Anda dapat menggunakan Amazon CloudWatch Logs untuk mendapatkan informasi tentang kesehatan 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 Anda dan mendapatkan pemberitahuan ketika Gateway FSx File Anda gagal mengunggah file ke sistem FSx file Amazon. 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, lihatKonfigurasikan Gateway FSx File Amazon Anda. Untuk informasi umum tentang grup CloudWatch log, lihat Bekerja dengan Grup Log dan Aliran Log di Panduan CloudWatch Pengguna Amazon.

Untuk informasi tentang cara memecahkan masalah kesalahan yang mungkin dilaporkan oleh , 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 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 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 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

Memahami metrik gateway

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

Selalu tentukan apakah Anda ingin bekerja dengan gateway atau sistem 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 .

Metrik	Deskripsi
`AvailabilityNotifications`	Metrik ini melaporkan jumlah pemberitahuan kesehatan terkait ketersediaan yang dihasilkan oleh gateway dalam periode pelaporan. Unit: Hitungan
`CacheDirectorySize`	Metrik ini melacak ukuran folder di cache gateway. Ukuran folder ditentukan oleh jumlah

Metrik	Deskripsi
	file dan subfolder di tingkat pertama, ini tidak dihitung secara rekursif ke dalam subfolder. Gunakan metrik ini dengan `Average` statistik untuk mengukur ukuran rata-rata folder di cache gateway. Gunakan metrik ini dengan `Max` statistik untuk mengukur ukuran maksimum folder di cache gateway. 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. Unit: Persen
`CachePercentUsed`	Persentase keseluruhan dari penyimpanan cache gateway yang digunakan. 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
`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

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
FileShares	Metrik ini melaporkan jumlah pembagian file di gateway. Unit: Hitungan
FileSystem-ERROR	Metrik ini memberikan jumlah asosiasi sistem file pada gateway ini yang berada dalam status ERROR. Jika metrik ini melaporkan asosiasi sistem file apa pun berada dalam status ERROR, maka kemungkinan 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
HealthNotifications	Metrik ini melaporkan jumlah pemberitahuan kesehatan yang dihasilkan oleh gateway ini dalam periode pelaporan. Unit: Hitungan

Metrik	Deskripsi
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
MemUsedBytes	Metrik ini melaporkan jumlah memori yang digunakan pada gateway. Unit: Byte

Metrik	Deskripsi
`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
`SmbV2Sessions`	Metrik ini melaporkan jumlah SMBv2 sesi yang aktif di gateway. Metrik ini dipancarkan sekali untuk setiap sistem file yang terkait dengan gateway. Gunakan stat SUM untuk menghitun g jumlah total SMBv2 sesi aktif di semua sistem file. Unit: Hitungan
`SmbV3Sessions`	Metrik ini melaporkan jumlah SMBv3 sesi yang aktif di gateway. Metrik ini dipancarkan sekali untuk setiap sistem file yang terkait dengan gateway. Gunakan stat SUM untuk menghitun g jumlah total SMBv3 sesi aktif di semua sistem file. Unit: Hitungan
`TotalCacheSize`	Metrik ini melaporkan ukuran total cache. Unit: Byte

Metrik	Deskripsi
`UserCpuPercent`	Metrik ini melaporkan persentase waktu yang dihabiskan untuk pemrosesan gateway. Unit: Persen

Memahami metrik sistem file

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

Selalu tentukan apakah Anda ingin bekerja dengan gateway atau metrik sistem file sebelum bekerja dengan metrik. Secara khusus, ketika bekerja dengan metrik sistem file, Anda harus menentukan `File system ID` yang mengidentifikasi sistem 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.

Metrik	Deskripsi
	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 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

Metrik	Deskripsi
`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
`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

Metrik	Deskripsi
`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 Amazon FSx FSx File Gateway (File Gateway) memberi Anda detail tentang akses pengguna ke file dan folder dalam asosiasi sistem file. Anda dapat menggunakan log audit untuk memantau aktivitas pengguna dan mengambil tindakan jika pola aktivitas yang tidak pantas diidentifikasi. Log diformat mirip dengan peristiwa log keamanan Windows Server, untuk mendukung kompatibilitas dengan alat pemrosesan log yang ada untuk peristiwa keamanan Windows.

Operasi

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

Atribut	Definisi
`securityDescriptor`	Menampilkan daftar kontrol akses diskresioner (DACL) yang disetel pada objek, dalam format SDDL.
`sourceAddress`	Alamat IP mesin klien berbagi file.
`SubjectDomainName`	Domain Active Directory (AD) yang menjadi milik akun klien.
`SubjectUserName`	Nama pengguna Active Directory klien.
`source`	ID dari Storage Gateway `FileSyste mAssociation` yang sedang diaudit.
`mtime`	Kali ini konten objek dimodifikasi, ditetapkan oleh klien.
`version`	Versi format log audit.
`ObjectType`	Mendefinisikan apakah objek adalah file atau folder.
`locationDnsName`	Nama DNS sistem FSx File Gateway.
`objectName`	Jalur penuh ke objek.
`ctime`	Waktu konten atau metadata objek dimodifik asi, ditetapkan oleh klien.
`shareName`	Nama saham yang sedang diakses.
`operation`	Nama operasi akses objek.
`newObjectName`	Jalur lengkap ke objek baru setelah diganti namanya.

Atribut	Definisi
`gateway`	ID Storage Gateway.
`status`	Status operasi. Hanya keberhasilan yang dicatat (kegagalan dicatat dengan pengecualian kegagalan yang timbul dari izin ditolak).
`fileSizeInBytes`	Ukuran file dalam byte, ditetapkan oleh klien pada waktu pembuatan file.

Atribut dicatat per operasi

Tabel berikut menjelaskan atribut log audit FSx 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)	Tulis atribut (chown)	Tulis atribut (chmod)	Tulis atribut (chgrp)
`securi escrip`							X			
`source ress`	X	X	X	X	X	X	X	X	X	X
`Subjec mainNa`	X	X	X	X	X	X	X	X	X	X
`Subjec erName`	X	X	X	X	X	X	X	X	X	X
`source`	X	X	X	X	X	X	X	X	X	X
`mtime`			X	X						
`versic`	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)	Tulis atribut (chown)	Tulis atribut (chmod)	Tulis atribut (chgrp)
`object`	X	X	X	X	X	X	X	X	X	X
`locationsName`	X	X	X	X	X	X	X	X	X	X
`object`	X	X	X	X	X	X	X	X	X	X
`ctime`			X	X						
`shareN`	X	X	X	X	X	X	X	X	X	X
`operat`	X	X	X	X	X	X	X	X	X	X
`newObjName`					X					
`gatewa`	X	X	X	X	X	X	X	X	X	X
`status`	X	X	X	X	X	X	X	X	X	X
`fileSinBytes`				X						

Mempertahankan gateway Anda

Mempertahankan Amazon FSx File Gateway File Anda 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 Amazon FSx File Gateway Amazon Gateway 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 ada dengan instance baru— Pelajari cara mengganti 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 .

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 menonaktifkan 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/rumah.
2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda konfigurasikan pembaruan pemeliharaan.

3. Pilih Tindakan, lalu pilih Edit pengaturan pemeliharaan.
4. Untuk pembaruan Pemeliharaan, pilih Aktif atau Mati.
5. Pilih Simpan perubahan setelah selesai.

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

Ubah jadwal jendela pemeliharaan gateway

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

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

Untuk mengubah jadwal jendela pemeliharaan menggunakan konsol Storage Gateway:

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda konfigurasikan pembaruan pemeliharaan.
3. Pilih Tindakan, lalu pilih Edit pengaturan pemeliharaan.
4. Di bawah waktu mulai jendela Pemeliharaan, lakukan hal berikut:
    a. Untuk Jadwal, pilih Mingguan atau Bulanan untuk mengatur irama jendela pemeliharaan.
    b. Jika Anda memilih Mingguan, ubah nilai untuk Hari dalam seminggu dan Waktu untuk mengatur titik tertentu selama setiap minggu ketika jendela pemeliharaan akan dimulai.

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

> **Note**
>
> Nilai maksimum yang dapat ditetapkan untuk hari dalam sebulan adalah 28. 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/rumah.
2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda perbarui.

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

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

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

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 menghosting 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 Linux Kernel-based Virtual Machine (KVM), VMware ESXi atau platform Microsoft Hyper-V Manager.
- 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 Hyper-V Manager.

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 daftar VMs yang saat ini tersedia di KVM.

   ```
   # virsh list
   ```

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

2. Gunakan perintah berikut untuk mengakses konsol lokal.

   ```
   # virsh console Id
   ```

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

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

3. Masukkan nama pengguna dan kata sandi Anda untuk masuk ke konsol lokal gateway. Untuk informasi selengkapnya, lihat 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 kredensyal masuk yang diberikan kepada Anda oleh administrator hypervisor.

   Setelah beberapa saat, konsol lokal gateway AWS Appliance meminta Anda untuk masuk untuk mengubah konfigurasi jaringan dan pengaturan lainnya.
4. Masukkan nama pengguna dan kata sandi Anda untuk masuk ke konsol lokal gateway. Untuk informasi selengkapnya, lihat 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 VMware, Microsoft Hyper-V, dan Linux Kernel-based Virtual Machine (KVM) hypervisor.

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/rumah.
2. Pada panel navigasi, pilih Gateway, lalu pilih gateway yang ingin Anda atur kata sandi baru.
3. Untuk Tindakan, pilih Setel Kata Sandi Konsol Lokal.
4. Dalam kotak dialog Setel Kata Sandi Konsol Lokal, 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 VMware ESXi lokal, lihatMengakses Konsol Lokal Gateway dengan VMware ESXi.
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. Akses Konsol Lokal Gateway dengan Microsoft Hyper-V
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal 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 akan 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 VMware ESXi lokal, lihatMengakses Konsol Lokal Gateway dengan VMware ESXi.

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

2. Dari menu utama 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 untuk memasukkan informasi berikut untuk mengkonfigurasi IP statis: • Nama adaptor jaringan • Alamat IP • Netmask • Alamat gateway default • Alamat Layanan Nama Domain Utama (DNS) • Alamat DNS sekunder **Important** Jika gateway Anda telah diaktifkan, Anda harus mematikannya dan memulai ulang dari konsol Storage Gateway agar pengaturan diterapkan. Untuk informasi selengkapnya, lihat Mematikan VM gateway Anda. Jika gateway Anda menggunakan lebih dari satu antarmuka jaringan, Anda harus mengatur semua antarmuka 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 VMware ESXi lokal, lihatMengakses Konsol Lokal Gateway dengan VMware ESXi.
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. Akses Konsol Lokal Gateway dengan Microsoft Hyper-V
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal KVM, lihat. Mengakses Konsol Lokal Gateway dengan Linux KVM

2. Dari menu utama 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 VMware ESXi konsol, lihatMengakses Konsol Lokal Gateway dengan VMware ESXi.
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. Akses Konsol Lokal Gateway dengan Microsoft Hyper-V

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

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

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

Pesan	Deskripsi
[Oke]	Sumber daya telah lulus pemeriksaan sumber daya sistem.
[PERINGATAN]	Sumber daya tidak memenuhi persyaratan yang disarankan, tetapi gateway Anda dapat terus berfungsi. Storage Gateway menampilk an pesan yang menjelaskan hasil pemeriksaan sumber daya.
[GAGAL]	Sumber daya tidak memenuhi persyarat an minimum. Gateway Anda mungkin tidak berfungsi dengan baik. Storage Gateway 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 VMware ESXi lokal, lihatMengakses Konsol Lokal Gateway dengan VMware ESXi.
- Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. Akses Konsol Lokal Gateway dengan Microsoft Hyper-V
- Untuk informasi selengkapnya tentang masuk ke konsol lokal KVM, lihat. Mengakses Konsol Lokal Gateway dengan Linux KVM

2. Dari menu utama 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 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 Sinkronkan waktu VM dengan waktu host Hyper-V atau 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 VMware ESXi lokal, lihatMengakses Konsol Lokal Gateway dengan VMware ESXi.
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. Akses Konsol Lokal Gateway dengan Microsoft Hyper-V
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal KVM, lihat. Mengakses Konsol Lokal Gateway dengan Linux KVM

2. Dari menu utama Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Gateway Console.

3. Dari prompt perintah konsol gateway, masukkan**h**.

   Konsol menampilkan menu AVAILABLE COMMANDS, yang mencantumkan perintah yang tersedia:

Perintah	Fungsi
menggali	Kumpulkan output dari penggalian untuk pemecahan masalah DNS.
keluar	Kembali ke menu Konfigurasi.
-h	Tampilkan daftar perintah yang tersedia.
ifconfig	Lihat atau konfigurasikan antarmuka jaringan. **Note** Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus. Untuk petunjukn ya, lihat Mengonfigurasi setelan jaringan gateway Anda Mengonfigurasi pengaturan .

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 petunjukn ya, lihat Mengonfigurasi setelan jaringan gateway Anda Mengonfigurasi pengaturan .
iptables	Alat administrasi untuk penyaringan IPv4 paket dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.
nping	Kumpulkan output dari nping untuk pemecahan masalah jaringan.
open-support-channel	Connect to AWS Support Untuk petunjuk tentang cara mengaktifkan akses AWS dukungan, lihat EC2 Anda.
passwd	Perbarui token otentikasi.
simpan-iptables	Pertahankan tabel IP.
save-routing-table	Simpan entri tabel routing yang baru ditambahk an.
tcptraceroute	Kumpulkan output traceroute pada lalu lintas TCP ke tujuan.

Perintah	Fungsi
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. Connect 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 akan ditampilkan.
   - Hapus konfigurasi proxy HTTP - Pesan `HTTP Proxy Configuration Removed` ditampilkan.

Menguji konektivitas jaringan gateway Anda

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

Untuk menguji konektivitas gateway Anda

1. Masuk ke konsol lokal gateway Anda. Untuk petunjuk, lihat Masuk ke konsol lokal 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
[Oke]	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 Aktivasi AWS Alat - Konfigurasi, masukkan angka yang sesuai untuk memilih Gateway Console.
3. Dari prompt perintah konsol gateway, masukkan**h**.

   Konsol menampilkan menu AVAILABLE COMMANDS, yang mencantumkan perintah yang tersedia:

Perintah	Fungsi
menggali	Kumpulkan output dari penggalian untuk pemecahan masalah DNS.
keluar	Kembali ke menu Konfigurasi.
-h	Tampilkan daftar perintah yang tersedia.
ifconfig	Lihat atau konfigurasikan antarmuka jaringan. **Note** Sebaiknya konfigurasi pengaturan jaringan atau IP menggunakan konsol Storage Gateway atau opsi menu konsol lokal khusus. Untuk petunjukn ya, lihat Mengonfigurasi setelan jaringan gateway Anda Mengonfigurasi pengaturan .
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 petunjukn ya, lihat Mengonfigurasi setelan jaringan gateway Anda Mengonfigurasi pengaturan .
iptables	Alat administrasi untuk penyaringan IPv4 paket dan NAT.
ncport	Uji konektivitas ke port TCP tertentu pada jaringan.
nping	Kumpulkan output dari nping untuk pemecahan masalah jaringan.
open-support-channel	Connect to AWS Support
simpan-iptables	Pertahankan tabel IP.
save-routing-table	Simpan entri tabel routing yang baru ditambahk an.
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

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 ada dengan instance baru

Anda dapat mengganti yang ada dengan instance baru saat data dan kebutuhan kinerja Anda bertambah, atau jika Anda menerima AWS pemberitahuan untuk 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.

> **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.

> **Note**
>
> Migrasi hanya dapat dilakukan antara gateway dari jenis yang sama. Misalnya, Anda tidak dapat memigrasikan pengaturan atau data dari Gateway FSx File ke Gateway File S3.

Untuk mengganti gateway FSx File Gateway Anda dengan instance baru dengan disk cache kosong dan ID Gateway baru:

1. Hentikan aplikasi apa pun yang menulis ke yang ada. Verifikasi bahwa `CachePercentDirty` metrik pada tab Monitoring adalah `0` sebelum Anda mengatur asosiasi sistem file di gateway baru.
2. Gunakan AWS Command Line Interface (AWS CLI) untuk mengumpulkan dan menyimpan informasi konfigurasi tentang yang ada dan sistem file terkait dengan melakukan hal berikut:

a. Simpan informasi konfigurasi gateway untuk .

```
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 .

```
aws storagegateway describe-smb-settings --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Perintah ini mengeluarkan blok JSON yang berisi nama domain Microsoft Active Directory tempat gateway bergabung.

c. Simpan informasi berbagi file untuk setiap sistem file yang terkait dengan :

Gunakan perintah berikut untuk setiap sistem file terkait.

```
aws storagegateway describe-file-system-associations --file-system-
association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-
association/fsa-987A654B"
```

Perintah ini mengeluarkan blok JSON yang berisi metadata tentang sistem file, seperti ARN lokasinya, tujuan log audit, atribut refresh cache, alamat IP yang dikonfigurasi, dan tag.

3. Buat baru dengan pengaturan dan konfigurasi yang sama dengan gateway lama. Jika perlu, lihat informasi yang Anda simpan di Langkah 2.
4. Buat asosiasi sistem file baru untuk gateway baru dengan pengaturan dan konfigurasi yang sama dengan sistem file yang dikonfigurasi pada gateway lama. Jika perlu, lihat informasi yang Anda simpan di Langkah 2.
5. Konfirmasikan bahwa gateway baru Anda berfungsi dengan benar, lalu petakan ulang/potong klien Anda dari sistem file lama ke sistem 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 , pastikan 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 sistem file 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, Microsoft Hyper-V Manager, atau Linux Kernel-based Virtual Machine (KVM) klien untuk terhubung ke host dan menghapus VM. Perhatikan bahwa Anda tidak dapat menggunakan kembali VM gateway yang dihapus untuk mengaktifkan gateway baru.

Untuk menghapus gateway

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih Gateway, lalu pilih satu atau beberapa gateway untuk dihapus.
3. Untuk Tindakan, pilih Hapus gateway. Kotak dialog konfirmasi muncul.

   > **Warning**
   >
   > Sebelum Anda melakukan langkah ini, pastikan bahwa tidak ada aplikasi yang saat ini menulis ke volume gateway. Jika Anda menghapus gateway saat sedang digunakan, kehilangan data dapat terjadi. Ketika gateway dihapus, tidak ada cara untuk mendapatkannya kembali.

4. Pastikan Anda ingin menghapus gateway yang ditentukan, lalu ketik kata hapus di kotak konfirmasi, dan pilih Hapus.
5. (Opsional) Jika Anda ingin memberikan umpan balik tentang gateway yang dihapus, lengkapi kotak dialog umpan balik, lalu pilih Kirim. Jika tidak, pilih Lewati.

Important

Anda tidak lagi membayar biaya perangkat lunak setelah menghapus gateway, tetapi sumber daya seperti bucket Amazon S3 dan instans Amazon EC2 tetap ada. Anda dapat menghapus gateway Amazon EC2 instans setelah gateway file dihapus.

Kinerja dan optimasi

Bagian ini menjelaskan panduan dan praktik terbaik untuk mengoptimalkan kinerja File Gateway.

Topik

Panduan kinerja dasar untuk

Di bagian ini, Anda dapat menemukan panduan untuk penyediaan perangkat keras untuk FSx 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
> Batas ukuran yang disarankan untuk direktori individual dalam sistem file 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 tekan cache dibaca dari data file yang disajikan dari cache. Operasi gagal baca cache dibaca dari data file yang disajikan dari Amazon FSx untuk Windows File Server.

Tabel berikut menunjukkan contoh konfigurasi FSx File Gateway.

FSx 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 Cakram cache: 2 x 2 TiB NVME Kinerja jaringan minimum: 10 Gbps CPU: 32 vCPU | RAM: 244 GB	SMBv3 - 1 utas	162 MiB/sec (1,4 Gbps)	403 MiB/sec (3,4 Gbps)	288 MiB/sec (2,4 Gbps)
	SMBv3 - 8 utas	511 MiB/sec (4,3 Gbps)	571 MiB/sec (4,8 Gbps)	567 MiB/sec (4,8 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.

Mengoptimalkan kinerja gateway

Anda dapat menemukan informasi berikut tentang cara mengoptimalkan kinerja gateway Anda. Panduan ini didasarkan pada penambahan sumber daya ke gateway Anda dan menambahkan sumber daya ke server aplikasi Anda.

Tambahkan Sumber Daya ke Gateway Anda

Anda dapat mengoptimalkan kinerja gateway dengan menambahkan sumber daya ke gateway Anda dengan satu atau beberapa cara berikut.

Gunakan disk berkinerja lebih tinggi

Untuk mengoptimalkan kinerja gateway, Anda dapat menambahkan disk berkinerja tinggi seperti solid-state drive (SSDs) dan pengontrol. NVMe Anda juga dapat melampirkan disk virtual ke VM Anda langsung dari jaringan area penyimpanan (SAN) alih-alih Microsoft Hyper-V NTFS. Peningkatan kinerja disk umumnya menghasilkan throughput yang lebih baik dan lebih banyak input/output operasi per detik (IOPS). Untuk informasi tentang menambahkan disk, lihatMengkonfigurasi penyimpanan cache tambahan.

Untuk mengukur throughput, gunakan `ReadBytes` dan `WriteBytes` metrik dengan statistik `Samples` Amazon CloudWatch . Misalnya, `Samples` statistik `ReadBytes` metrik selama periode sampel 5 menit dibagi 300 detik memberi Anda IOPS. Sebagai aturan umum, saat Anda meninjau metrik ini untuk gateway, cari throughput rendah dan tren IOPS rendah untuk menunjukkan kemacetan terkait disk.

> **Note**
>
> CloudWatch metrik tidak tersedia untuk semua gateway. Untuk informasi tentang metrik gateway, lihatMemantau Anda.

Tambahkan sumber daya CPU ke host gateway Anda

Persyaratan minimum untuk server host gateway adalah empat prosesor virtual. Untuk mengoptimalkan kinerja gateway, konfirmasikan bahwa empat prosesor virtual yang ditugaskan ke VM gateway didukung oleh empat inti. Selain itu, konfirmasikan bahwa Anda tidak kelebihan langganan CPUs server host.

Ketika Anda menambahkan tambahan CPUs ke server host gateway Anda, Anda meningkatkan kemampuan pemrosesan gateway. Melakukan hal ini memungkinkan gateway Anda untuk menangani, secara paralel, baik menyimpan data dari aplikasi Anda ke penyimpanan lokal Anda dan mengunggah data ini ke S3 untuk Windows File Server. Tambahan CPUs juga membantu memastikan bahwa gateway Anda mendapatkan sumber daya CPU yang cukup saat host dibagikan dengan yang lain VMs. Menyediakan sumber daya CPU yang cukup memiliki efek umum meningkatkan throughput.

Storage Gateway mendukung penggunaan 24 CPUs di server host gateway Anda. Anda dapat menggunakan 24 CPUs untuk meningkatkan kinerja gateway Anda secara signifikan. Kami merekomendasikan konfigurasi gateway berikut untuk server host gateway Anda:

- 24 CPUs.
- 16 GiB RAM yang dicadangkan untuk File Gateways
  - 16 GiB RAM cadangan untuk gateway dengan ukuran cache hingga 16 TiB
  - 32 GiB RAM cadangan untuk gateway dengan ukuran cache 16 TiB hingga 32 TiB
  - 48 GiB RAM cadangan untuk gateway dengan ukuran cache 32 TiB hingga 64 TiB
- Disk 1 melekat pada controller paravirtual 1, untuk digunakan sebagai cache gateway sebagai berikut:
  - SSD menggunakan NVMe pengontrol.
- Adaptor jaringan 1 dikonfigurasi pada jaringan VM 1:
  - Gunakan jaringan VM 1 dan tambahkan VMXnet3 (10 Gbps) yang akan digunakan untuk konsumsi.
- Adaptor jaringan 2 dikonfigurasi pada jaringan VM 2:
  - Gunakan jaringan VM 2 dan tambahkan VMXnet3 (10 Gbps) yang akan digunakan untuk terhubung. AWS

Back gateway virtual disk dengan disk fisik terpisah

Saat Anda menyediakan disk gateway, kami sangat menyarankan agar Anda tidak menyediakan disk lokal untuk penyimpanan lokal yang menggunakan disk penyimpanan fisik dasar yang sama. Misalnya, untuk VMware ESXi, sumber daya penyimpanan fisik yang mendasarinya direpresentasikan sebagai penyimpanan data. Saat Anda menyebarkan VM gateway, Anda memilih penyimpanan data untuk menyimpan file VM. Saat Anda menyediakan disk virtual (misalnya, sebagai buffer unggahan), Anda dapat menyimpan disk virtual di penyimpanan data yang sama dengan VM atau penyimpanan data yang berbeda.

Jika Anda memiliki lebih dari satu penyimpanan data, maka kami sangat menyarankan Anda memilih satu penyimpanan data untuk setiap jenis penyimpanan lokal yang Anda buat. Penyimpanan data yang didukung oleh hanya satu disk fisik yang mendasarinya dapat menyebabkan kinerja yang buruk. Contohnya adalah ketika Anda menggunakan disk seperti itu untuk mendukung penyimpanan cache dan mengunggah buffer dalam pengaturan gateway. Demikian pula, penyimpanan data yang didukung oleh konfigurasi RAID yang kurang berkinerja tinggi seperti RAID 1 dapat menyebabkan kinerja yang buruk.

Tambahkan Sumber Daya ke Lingkungan Aplikasi Anda

Tingkatkan bandwidth antara server aplikasi dan gateway Anda

Untuk mengoptimalkan kinerja gateway, pastikan bandwidth jaringan antara aplikasi Anda dan gateway dapat mempertahankan kebutuhan aplikasi Anda. Anda dapat menggunakan `ReadBytes` dan `WriteBytes` metrik gateway untuk mengukur total throughput data.

Untuk aplikasi Anda, bandingkan throughput yang diukur dengan throughput yang diinginkan. Jika throughput yang diukur kurang dari throughput yang diinginkan, maka meningkatkan bandwidth antara aplikasi dan gateway Anda dapat meningkatkan kinerja jika jaringan adalah hambatan. Demikian pula, Anda dapat meningkatkan bandwidth antara VM dan disk lokal Anda, jika tidak terpasang langsung.

Tambahkan sumber daya CPU ke lingkungan aplikasi Anda

Jika aplikasi Anda dapat menggunakan sumber daya CPU tambahan, menambahkan lebih banyak CPUs dapat membantu aplikasi Anda untuk menskalakan I/O bebannya.

Beberapa operasi file pada FSx File Gateway, seperti penggantian nama folder tingkat atas atau perubahan izin, dapat menghasilkan beberapa operasi file yang mengarah ke I/O beban tinggi pada sistem file Windows File Server Anda FSx . Jika sistem file Anda tidak memiliki sumber daya kinerja yang cukup untuk beban kerja Anda, sistem file mungkin menghapus salinan bayangan karena memprioritaskan ketersediaan untuk berkelanjutan I/O daripada retensi salinan bayangan historis.

Di FSx konsol Amazon, periksa halaman Pemantauan dan kinerja untuk melihat apakah sistem file Anda kurang disediakan. Jika ya, Anda dapat beralih ke penyimpanan SSD, meningkatkan kapasitas throughput, atau meningkatkan IOPS SSD untuk menangani beban kerja Anda.

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. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS Storage Gateway, lihat AWS Layanan dalam Lingkup menurut AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Storage Gateway. Topik berikut menunjukkan cara mengonfigurasi Storage Gateway untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Storage Gateway Anda.

Perlindungan data di AWS Storage Gateway

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Storage Gateway. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil 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 SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data menggunakan AWS KMS

Amazon FSx File Gateway mendukung enkripsi SMB hingga spesifikasi SMB v3.1.1 terbaru, termasuk AES 128 CCM dan AES 128 GCM. Klien yang kompatibel akan terhubung menggunakan enkripsi secara otomatis. Selain itu, FSx File Gateway menggunakan enkripsi SMB saat berkomunikasi dengan FSx Windows File Server di. AWS Anda harus mengonfigurasi Direct Connect

tautan ke AWS, dan menetapkan kebijakan yang sesuai untuk memungkinkan lalu lintas SMB dan lalu lintas manajemen melewatinya AWS.

Mengenkripsi sistem file

Untuk informasi, lihat, Enkripsi Data FSx di Amazon di Panduan Pengguna Server File Amazon FSx untuk Windows.

Saat menggunakan AWS KMS untuk mengenkripsi data Anda, ingatlah hal berikut:

- Data Anda dienkripsi saat istirahat di cloud. Artinya, data dienkripsi di Amazon . FSx
- 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?

Manajemen identitas dan 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
- Contoh kebijakan berbasis identitas untuk Storage Gateway AWS
- Memecahkan masalah identitas dan AWS akses Storage Gateway
- Menggunakan tag untuk mengontrol akses ke gateway dan sumber daya Anda

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 Memecahkan masalah identitas dan AWS 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 Contoh kebijakan berbasis identitas untuk Storage Gateway AWS)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensil dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensional. 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 kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensil 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 kredensi 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.

Kebijakan berbasis identitas

Kebijakan berbasis identitas 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.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. 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.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

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 (SCPs) — Tentukan 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 (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- 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 dengan AWS Storage Gateway

Fitur IAM	AWS Dukungan SGW
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak

Fitur IAM	AWS Dukungan SGW
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja AWS SGW dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk SGW AWS

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk SGW AWS

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

Kebijakan berbasis sumber daya dalam SGW AWS

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya 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. Contoh kebijakan berbasis identitas untuk Storage Gateway AWS

Sumber daya kebijakan untuk AWS SGW

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, 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 jenis sumber daya AWS SGW dan jenisnya ARNs, lihat Sumber Daya yang Ditetapkan oleh AWS Storage Gateway di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh AWS Storage Gateway.

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

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. Contoh kebijakan berbasis identitas untuk Storage Gateway AWS

ACLs di AWS SGW

Mendukung ACLs: Tidak

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

ABAC dengan SGW AWS

Mendukung ABAC (tag dalam kebijakan): Sebagian

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. 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 kredensil sementara dengan SGW AWS

Mendukung kredensial sementara: Ya

Kredensi 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 kredensi 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.

Peran terkait layanan untuk SGW AWS

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Storage Gateway AWS

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 ARNs untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk AWS Storage Gateway di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol AWS SGW
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya AWS SGW di akun Anda. Tindakan ini 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 konsol AWS SGW

Untuk mengakses konsol AWS Storage Gateway, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya AWS

SGW di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol AWS SGW, lampirkan juga AWS SGW *ConsoleAccess* atau kebijakan *ReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Memecahkan masalah identitas dan AWS akses Storage Gateway

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS SGW dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS SGW
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya AWS SGW saya

Saya tidak berwenang untuk melakukan tindakan di AWS SGW

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `sgw:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `sgw:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke AWS SGW.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan dalam AWS SGW. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

> **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 sumber daya AWS SGW saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah AWS SGW mendukung fitur-fitur ini, lihat. Bagaimana AWS Storage Gateway bekerja dengan IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

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 nilainya disetel keyes.

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"
               }
            }
         }
      ]
}
```

Validasi kepatuhan untuk AWS Storage Gateway

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS Storage Gateway sebagai bagian dari beberapa program AWS kepatuhan. Ini termasuk SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR, dan HITRUST CSF.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan . Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Storage Gateway ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan Panduan Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- Arsitektur untuk Whitepaper Keamanan dan Kepatuhan HIPAA — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi yang sesuai dengan HIPAA. AWS
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.

- Mengevaluasi sumber daya dengan aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub 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 Storage Gateway AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones.

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

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

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Storage Gateway mendukung VMware vSphere High Availability (VMware HA) untuk membantu melindungi beban kerja penyimpanan terhadap hardware, hypervisor, atau kegagalan jaringan. Untuk informasi selengkapnya, lihat Menggunakan Ketersediaan Tinggi VMware vSphere dengan Storage Gateway Menggunakan Ketersediaan Tinggi VMware Gateway.

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 support Keamanan Lapisan Pengangkutan (TLS) 1.2. Klien juga harus support suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan 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 ulasan, analisis, dan remediasi CVEs secara teratur. Kami menggabungkan perbaikan untuk masalah ini ke dalam Storage Gateway sebagai bagian dari siklus rilis perangkat lunak normal kami. Perbaikan ini biasanya diterapkan sebagai bagian dari proses pembaruan gateway normal selama jendela pemeliharaan terjadwal. Untuk informasi selengkapnya tentang pembaruan gateway, lihat 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 kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Storage Gateway

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan tindakan.

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

```
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                      "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
             }]
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan ListGateways tindakan.

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

```
                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
             }]
}
```

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, sistem file, ketersediaan tinggi, pemulihan data, dan snapshot. Informasi pemecahan masalah gateway lokal mencakup gateway yang digunakan pada platform virtualisasi yang didukung. Informasi pemecahan masalah untuk masalah ketersediaan tinggi mencakup gateway yang berjalan pada platform VMware vSphere High Availability (HA).

Topik

- Pemecahan masalah: masalah offline gateway- Pelajari cara mendiagnosis masalah yang dapat menyebabkan gateway Anda muncul offline di konsol Storage Gateway.
- Pemecahan masalah: Masalah Direktori Aktif- Pelajari apa yang harus dilakukan jika Anda menerima pesan galat sepertiNETWORK_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 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 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 . 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 jaringan gateway .

> **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 titik akhir Amazon VPC

Untuk mengatasi kesalahan aktivasi saat mengaktifkan gateway menggunakan titik akhir Amazon Virtual Private Cloud (Amazon VPC), lakukan pemeriksaan dan konfigurasi berikut.

Periksa port yang diperlukan

Pastikan port yang diperlukan dalam firewall lokal Anda (untuk gateway yang digunakan di lokasi) atau grup keamanan (untuk gateway yang digunakan di Amazon 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.

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 server terjadi saat mencoba mengimpor mesin virtual. Impor gagal. Tidak dapat menemukan	Kesalahan ini dapat terjadi karena alasan berikut: • Jika Anda tidak menunjuk ke root dari file sumber gateway yang tidak di-zip. Bagian terakhir dari lokasi yang Anda tentukan di kotak dialog Impor Mesin Virtual seharusnya`AWS-Storage-Gateway` . Contoh: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` .

Isu	Tindakan yang Harus Dilakukan
file impor mesin virtual di bawah lokasi [...]. Anda dapat mengimpor mesin virtual hanya jika Anda menggunakan Hyper-V untuk membuat dan mengekspornya.	• Jika Anda telah menerapkan gateway dan Anda tidak memilih opsi Salin mesin virtual dan centang opsi Duplikat semua file di kotak dialog Impor Mesin Virtual, maka VM dibuat di lokasi di mana Anda memiliki file gateway yang tidak di-zip dan Anda tidak dapat mengimpor dari lokasi ini lagi. Untuk memperbaiki masalah ini, dapatkan salinan baru dari file sumber gateway yang tidak di-zip dan salin ke lokasi baru. Gunakan lokasi baru sebagai sumber impor. Jika Anda berencana membuat beberapa gateway dari satu lokasi file sumber yang tidak di-zip, Anda harus memilih Salin mesin virtual dan centang Duplikat semua file kotak di kotak dialog Impor Mesin Virtual.
Anda mencoba mengimpor gateway dan menerima pesan galat berikut: “Kesalahan server terjadi saat mencoba mengimpor mesin virtual. Impor gagal. Tugas impor gagal menyalin file dari [...]: File ada. (0x80070050)”	Jika Anda telah menggunakan gateway dan Anda mencoba menggunakan kembali folder default yang menyimpan file hard disk virtual dan file konfigurasi mesin virtual, maka kesalahan ini akan terjadi. Untuk memperbaiki masalah ini, tentukan lokasi baru di bawah Server di panel di sisi kiri kotak dialog Pengaturan Hyper-V.

Isu	Tindakan yang Harus Dilakukan
Anda mencoba mengimpor gateway dan menerima pesan galat berikut: “Kesalahan server terjadi saat mencoba mengimpor mesin virtual. Impor gagal. Impor gagal karena mesin virtual harus memiliki pengenal baru. Pilih pengenal baru dan coba impor lagi.”	Saat Anda mengimpor gateway, pastikan Anda memilih Salin mesin virtual dan centang Duplikat semua file kotak di kotak dialog Impor Mesin Virtual untuk membuat ID unik baru untuk VM.
Anda mencoba memulai VM gateway dan menerima pesan galat berikut: “Terjadi kesalahan saat mencoba memulai mesin virtual yang dipilih. Pengaturan prosesor partisi anak tidak kompatibel dengan partisi induk. 'AWS-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 FSx Amazon EC2 default untuk File Gateway

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: FileMissing

`FileMissing`Kesalahannya mirip dengan `ObjectMissing` kesalahan, dan langkah-langkah untuk mengatasinya identik. Anda bisa mendapatkan `FileMissing` kesalahan ketika penulis selain Gateway File yang ditentukan menghapus file yang ditentukan dari Amazon FSx. Setiap unggahan berikutnya ke Amazon FSx atau pengambilan dari Amazon FSx untuk objek gagal.

Untuk mengatasi FileMissing kesalahan

1. Simpan salinan file terbaru ke sistem file lokal klien SMB Anda (Anda memerlukan salinan file ini pada langkah 3).

2. Hapus file dari File Gateway menggunakan klien SMB Anda.
3. Salin versi terbaru dari file yang Anda simpan di langkah 1 Amazon FSx menggunakan klien SMB Anda. Lakukan ini melalui File Gateway Anda.

Kesalahan: FsxFileSystemAuthenticationFailure

Anda bisa mendapatkan `FsxFileSystemAuthenticationFailure` kesalahan ketika kredensi yang diberikan saat melampirkan sistem file kedaluwarsa atau, hak istimewanya telah dicabut.

Untuk mengatasi FsxFileSystemAuthenticationFailure kesalahan

1. Pastikan bahwa kredensi yang diberikan pada saat melampirkan sistem FSx file Amazon masih valid.
2. Pastikan bahwa pengguna memiliki semua izin yang diperlukan seperti yang dijelaskan dalam Lampirkan sistem file Amazon FSx untuk Windows File Server.

Kesalahan: FsxFileSystemConnectionFailure

Anda bisa mendapatkan `FsxFileSystemConnectionFailure` kesalahan ketika FSx server Amazon tidak dapat diakses dari mesin gateway.

Untuk mengatasi FsxFileSystemConnectionFailure kesalahan

1. Pastikan bahwa semua aturan firewall dan VPC memungkinkan koneksi antara mesin gateway dan server Amazon FSx .
2. Pastikan FSx server Amazon berjalan.

Kesalahan: FsxFileSystemFull

Anda bisa mendapatkan `FsxFileSystemFull` kesalahan ketika tidak ada cukup ruang disk kosong di sistem FSx file Amazon.

Untuk mengatasi FsxFileSystemFull kesalahan

- Tingkatkan ruang penyimpanan untuk sistem FSx file Amazon.

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 .

Kesalahan: InvalidFileState

Anda bisa mendapatkan `InvalidFileState` kesalahan ketika penulis selain gateway yang ditentukan memodifikasi file yang ditentukan dalam berbagi file yang ditentukan. Akibatnya, status file di gateway tidak cocok dengan statusnya di Amazon FSx. Setiap unggahan atau pengambilan file berikutnya dari Amazon FSx bisa gagal.

Untuk mengatasi InvalidFileState kesalahan

1. Simpan salinan file terbaru ke sistem file lokal klien SMB Anda (Anda memerlukan file ini untuk disalin pada langkah 4). Jika versi file di Amazon FSx adalah yang terbaru, unduh versi itu. Anda dapat melakukan ini dengan langsung mengakses FSx berbagi Amazon menggunakan klien SMB apa pun.
2. Hapus file di Amazon FSx secara langsung.
3. Hapus file dari gateway menggunakan klien SMB Anda.
4. Menggunakan klien SMB Anda, salin versi terbaru dari file yang Anda simpan di langkah 1, melalui File Gateway Anda, ke Amazon FSx.

Kesalahan: ObjectMissing

Anda bisa mendapatkan `ObjectMissing` kesalahan ketika penulis selain Gateway File yang ditentukan menghapus file yang ditentukan dari Amazon FSx. Setiap unggahan berikutnya ke Amazon FSx atau pengambilan dari Amazon FSx untuk objek gagal.

Untuk mengatasi ObjectMissing kesalahan

1. Simpan salinan file terbaru ke sistem file lokal klien SMB Anda (Anda memerlukan salinan file ini pada langkah 3).
2. Hapus file dari File Gateway menggunakan klien SMB Anda.
3. Salin versi terbaru dari file yang Anda simpan di langkah 1 Amazon FSx menggunakan klien SMB Anda. Lakukan ini melalui File Gateway Anda.

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: Masalah domain Direktori Aktif

FSx File Gateway tidak menghasilkan pesan log khusus untuk masalah domain Active Directory. Jika Anda mengalami masalah saat bergabung dengan gateway ke domain Active Directory, lakukan hal berikut:

- Verifikasi bahwa gateway tidak mencoba menggunakan pengontrol domain hanya-baca (RODC) untuk bergabung dengan domain.
- Verifikasi bahwa gateway dikonfigurasi untuk menggunakan server DNS yang benar.

  Misalnya, jika Anda mencoba menggabungkan instance gateway Amazon EC2 ke Direktori Aktif yang AWS dikelola, verifikasi bahwa opsi DHCP yang disetel untuk VPC EC2 Anda menentukan server DNS Direktori Aktif yang dikelola. AWS

  Server DNS yang Anda konfigurasikan melalui set opsi VPC DHCP disediakan untuk semua instans EC2 di VPC. Jika Anda ingin menentukan server DNS untuk gateway individual, Anda dapat melakukannya menggunakan konsol lokal EC2 gateway itu.

  Untuk gateway lokal, Anda menentukan server DNS menggunakan konsol lokal VM.
- Verifikasi konektivitas jaringan gateway dengan menjalankan perintah berikut dari prompt perintah di konsol lokal gateway. Ganti variabel yang disorot dengan nama domain dan alamat IP yang sebenarnya dari penerapan Anda.

```
dig -d ExampleDomainName
ncport -d ExampleDomainControllerIPAddress -p 445
ncport -d ExampleDomainControllerIPAddress -p 389
```

- Verifikasi bahwa akun layanan Direktori Aktif Anda memiliki izin yang diperlukan. Untuk selengkapnya, lihat akun layanan Direktori Aktif.
- Verifikasi bahwa gateway bergabung dengan Unit Organisasi (OU) yang benar.

  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 Active Directory Anda memiliki OU yang ditunjuk untuk objek komputer baru, Anda harus menentukan OU tersebut saat bergabung dengan domain.

  Jika Anda menemukan kesalahan akses ditolak saat mencoba bergabung dengan OU yang ditunjuk, periksa dengan administrator domain Active Directory Anda. Administrator mungkin perlu melakukan pra-tahap akun komputer gateway sebelum dapat bergabung dengan domain. Untuk informasi selengkapnya, lihat Bagaimana cara memecahkan masalah dengan menggabungkan gateway file Storage Gateway ke domain untuk otentikasi Microsoft Active Directory? .
- Verifikasi bahwa nama host gateway Anda dapat diselesaikan dalam DNS dengan menjalankan perintah berikut dari prompt perintah di konsol lokal gateway. Ganti variabel yang disorot dengan nama host yang sebenarnya untuk gateway Anda.

  ```
  dig -d ExampleHostName -r A
  ```

  Jika Anda mengonfigurasi nama host khusus untuk gateway Anda, Anda harus menambahkan DNS A-record secara manual yang menunjuk ke alamat IP-nya.
- Verifikasi bahwa latensi jaringan antara gateway dan pengontrol domain cukup rendah. Kueri untuk bergabung dengan domain dapat habis jika gateway tidak menerima respons dari pengontrol domain dalam waktu 20 detik.

  Jika Anda bergabung dengan gateway ke domain menggunakan perintah JoinDomainCLI, Anda dapat menambahkan `--timeout-in-seconds` bendera untuk meningkatkan batas waktu hingga maksimum 3.600 detik.
- Verifikasi bahwa pengguna Active Directory yang Anda gunakan untuk bergabung dengan gateway ke domain memiliki hak istimewa yang diperlukan untuk melakukannya.

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 S3 untuk Windows 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 konten sistem FSx file Amazon 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 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.

Anda tidak melihat file di sistem FSx file Amazon Anda

Jika Anda melihat bahwa file di gateway tidak tercermin dalam sistem FSx file Amazon, periksa `FilesFailingUpload` metriknya. 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.

Anda tidak melihat snapshot lama di sistem FSx file Amazon Anda

Beberapa operasi file pada FSx File Gateway, seperti penggantian nama folder tingkat atas atau perubahan izin, dapat menghasilkan beberapa operasi file yang mengarah ke I/O beban tinggi pada sistem file Windows File Server Anda FSx . Jika sistem file Anda tidak memiliki sumber daya kinerja yang cukup untuk beban kerja Anda, sistem file mungkin menghapus salinan bayangan karena memprioritaskan ketersediaan untuk berkelanjutan I/O daripada retensi salinan bayangan historis.

Di FSx konsol Amazon, periksa halaman Pemantauan dan kinerja untuk melihat apakah sistem file Anda kurang disediakan. Jika ya, Anda dapat beralih ke penyimpanan SSD, meningkatkan kapasitas throughput, atau meningkatkan IOPS SSD untuk menangani beban kerja Anda.

Gateway Anda lambat mentransfer data ke Amazon FSx

Jika File Gateway Anda lambat mentransfer data ke Amazon FSx untuk Windows File Server, lakukan hal berikut:

- Jika `CachePercentDirty` metriknya 80 atau lebih besar, File Gateway Anda menulis data lebih cepat ke disk daripada dapat mengunggah data ke Amazon FSx untuk Windows File Server. Pertimbangkan untuk meningkatkan bandwidth untuk diunggah dari File Gateway Anda, menambahkan satu atau lebih disk cache, atau memperlambat penulisan klien, atau meningkatkan kapasitas throughput FSx untuk Amazon terkait untuk Windows File Server.
- 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.

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 S3 untuk Windows File 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 S3 untuk Windows File 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.

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
- Metrik-metrik

Pemberitahuan Kesehatan

Saat Anda menjalankan gateway Anda di VMware vSphere HA, semua gateway menghasilkan pemberitahuan kesehatan berikut ke grup log Amazon Anda yang dikonfigurasi. CloudWatch Pemberitahuan ini masuk ke aliran log yang disebut`AvailabilityMonitor`.

Topik

- Pemberitahuan: Reboot
- Pemberitahuan: HardReboot
- Pemberitahuan: HealthCheckFailure
- Pemberitahuan: AvailabilityMonitorTest

Pemberitahuan: Reboot

Anda bisa mendapatkan notifikasi reboot saat gateway VM dimulai ulang. Anda dapat memulai ulang VM gateway dengan menggunakan konsol VM Hypervisor Management atau konsol Storage Gateway. Anda juga dapat memulai ulang dengan menggunakan perangkat lunak gateway selama siklus pemeliharaan gateway.

Tindakan 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 sistem file baru ke untuk Windows File Server yang berisi data yang ingin Anda pulihkan.

1. Buat dan aktifkan File Gateway baru di host Amazon EC2. Untuk informasi selengkapnya, lihat Menerapkan host FSx Amazon EC2 default untuk File Gateway.
2. Buat sistem file baru di gateway EC2 yang Anda buat. Untuk informasi selengkapnya, lihat Membuat sistem file Windows File Server FSx untuk Windows.
3. Pasang sistem file Anda pada klien Anda dan petakan ke untuk Windows File Server yang berisi data yang ingin Anda pulihkan. Untuk informasi selengkapnya, lihat Mount dan gunakan berbagi file Anda.

Memulihkan dari cadangan atau snapshot langsung di Amazon FSx

Dalam beberapa kasus, Anda mungkin perlu memulihkan data di sistem FSx file Amazon Anda secara langsung, menggunakan cadangan atau snapshot dari titik waktu sebelumnya. Dalam hal ini,

ada risiko membuat skenario dual-writer antara aplikasi cadangan dan FSx File Gateway, yang dapat mengakibatkan file macet atau salah cocok. Untuk menghindari masalah saat memulihkan sistem FSx file Amazon Anda dari cadangan atau snapshot, gunakan prosedur berikut.

> **Note**
>
> Setiap data cache yang saat ini disimpan di FSx File Gateway Anda tidak akan valid setelah Anda memulihkan sistem FSx file Amazon Anda dari cadangan atau snapshot menggunakan prosedur ini.

Untuk menghindari masalah saat memulihkan sistem FSx file Amazon Anda dari cadangan atau snapshot

1. Lepaskan sistem FSx file Amazon dari FSx File Gateway menggunakan konsol Storage Gateway.
2. Kembalikan cadangan atau snapshot langsung di sistem FSx file Amazon Anda.
3. Pasang kembali sistem FSx file Amazon ke FSx File Gateway menggunakan konsol Storage Gateway.

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

- Penyiapan 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.
- 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 sumber daya IDs- Pelajari cara AWS mengidentifikasi sumber daya dan subresource yang dibuat oleh Storage Gateway.
- Memberikan tag ke sumber daya Anda- Pelajari cara menggunakan tag metadata untuk mengkategorikan sumber daya Anda dan membuatnya lebih mudah dikelola.
- Komponen sumber terbuka- 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.

Menyebarkan dan mengonfigurasi host VM gateway

Topik berikut memberikan informasi tentang pengaturan platform host mesin virtual untuk gateway Anda.

Topik

- Menerapkan host FSx Amazon EC2 default untuk File Gateway

- Menerapkan host FSx Amazon EC2 yang disesuaikan untuk File Gateway
- Ubah opsi metadata instans Amazon EC2
- Sinkronkan waktu VM dengan waktu host Hyper-V atau 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 FSx Amazon EC2 default untuk File Gateway

Topik ini mencantumkan langkah-langkah untuk menerapkan host Amazon EC2 menggunakan spesifikasi default.

Anda dapat menerapkan dan mengaktifkan Amazon di FSx instans Amazon Elastic Compute Cloud (Amazon EC2). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai komunitas AMI.

> **Note**
>
> Komunitas AMIs Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.

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, . FSx
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.

- Tetapkan IP Publik Otomatis - Diaktifkan
- Grup keamanan EC2 dibuat dan dikaitkan dengan Instans EC2. Grup keamanan memiliki aturan port masuk berikut:

> **Note**
>
> Anda akan membutuhkan Port 80 terbuka selama aktivasi gateway. Port ditutup segera setelah aktivasi. Setelah itu, instans EC2 Anda hanya dapat diakses melalui port lain dari VPC yang dipilih.
> 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
137	UDP	NetBIOS
138	UDP	NetBIOS

Port	Protokol	Protokol Sistem File
139	TCP, UDP	SMB
389	TCP	LDAP
445	TCP	SMB

- 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
Hapus saat pengakhiran	Ya	Ya
Dienkripsi	Tidak	Tidak
Throughput	125	125

Menerapkan host FSx Amazon EC2 yang disesuaikan untuk File Gateway

Anda dapat menerapkan dan mengaktifkan Amazon di FSx instans Amazon Elastic Compute Cloud (Amazon EC2). AWS Storage Gateway Amazon Machine Image (AMI) tersedia sebagai komunitas AMI.

> **Note**
>
> Komunitas AMIs Storage Gateway diterbitkan dan didukung sepenuhnya oleh AWS. Anda dapat melihat bahwa penerbit adalah AWS, penyedia terverifikasi.
> File Gateway AMIs menggunakan konvensi penamaan berikut. Nomor versi yang ditambahkan ke nama AMI berubah dengan setiap rilis versi.
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

Untuk menerapkan instans Amazon EC2 untuk meng-host Gateway File Amazon FSx Anda

1. Mulai menyiapkan gateway baru menggunakan konsol Storage Gateway. Untuk petunjuk, lihat File Amazon. 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. Untuk informasi selengkapnya tentang spesifikasi default Amazon EC2 Quicklaunch, lihat Spesifikasi Konfigurasi .
3. Untuk Nama, masukkan nama untuk instans Amazon EC2. Setelah instance diterapkan, 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 NVMe disk SSD. 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 Tetapkan Otomatis IP Publik, pilih Aktifkan.
7. Di subbagian Firewall (grup keamanan), tinjau pengaturan yang telah dikonfigurasi sebelumnya. Anda dapat mengubah nama default dan deskripsi grup keamanan baru yang akan dibuat untuk instans Amazon EC2 Anda jika Anda mau, atau memilih untuk menerapkan aturan firewall dari grup keamanan yang ada.
8. Dalam subbagian aturan grup keamanan masuk, tambahkan aturan firewall untuk membuka port yang akan digunakan klien untuk terhubung ke instans Anda. Untuk informasi selengkapnya tentang port yang diperlukan untuk Gateway, lihat port. Untuk informasi selengkapnya tentang menambahkan aturan firewall, lihat Aturan grup keamanan di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

> **Note**
>
> Amazon FSx 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.
> Selain itu, Anda harus membuka port TCP 445 untuk akses SMB, port UDP 137 untuk akses NetBIOS, port UDP 138 untuk akses NetBIOS, dan port TCP 389 untuk akses LDAP.

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 Pengaturan gateway di konsol Storage Gateway untuk melanjutkan pengaturan Anda.

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 File Amazon. 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_FSX_SMB/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_FSX_SMB/latest
  ```

  Perintah CLI mengembalikan output yang mirip dengan berikut ini.

  ```
  {
      "Parameter": {
          "Type": "String",
          "LastModifiedDate": 1561054105.083,
          "Version": 18,
           "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
  FILE_FSX_SMB/latest",
           "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
          "Value": "ami-033d1edba5606cffb"
      }
  }
  ```

Ubah opsi metadata instans Amazon EC2

Layanan metadata instance (IMDS) adalah komponen on-instance yang menyediakan akses aman ke metadata instans Amazon EC2. Instance dapat dikonfigurasi untuk menerima permintaan metadata masuk yang menggunakan IMDS Versi 1 (IMDSv1) atau mengharuskan semua permintaan metadata menggunakan IMDS Versi 2 (). IMDSv2 IMDSv2 menggunakan permintaan berorientasi sesi dan mengurangi beberapa jenis kerentanan yang dapat digunakan untuk mencoba mengakses IMDS. Untuk selengkapnya IMDSv2, lihat Cara Kerja Layanan Metadata Instans Versi 2 di Panduan Pengguna Amazon Elastic Compute Cloud.

Sebaiknya Anda 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 IMDSv1 metadata, lihat Memerlukan penggunaan IMDSv2 dalam Panduan Pengguna Amazon Elastic Compute Cloud untuk petunjuk mengubah opsi metadata instans Anda agar memerlukan penggunaan. IMDSv2 Menerapkan perubahan ini tidak memerlukan reboot instance.

Sinkronkan waktu VM dengan waktu host Hyper-V atau Linux KVM

Untuk gateway yang digunakan VMware ESXi, mengatur waktu host hypervisor dan menyinkronkan waktu mesin virtual ke host sudah cukup untuk menghindari penyimpangan waktu. Untuk informasi selengkapnya, lihat Sinkronisasi waktu VM dengan waktu host VMware. Untuk gateway yang digunakan di Microsoft Hyper-V atau Linux KVM, kami sarankan Anda memeriksa waktu mesin virtual secara berkala menggunakan prosedur yang dijelaskan berikut.

Untuk melihat dan menyinkronkan waktu mesin virtual gateway hypervisor ke server Network Time Protocol (NTP)

1. Masuk ke konsol lokal gateway Anda:
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal Microsoft Hyper-V, lihat. Akses Konsol Lokal Gateway dengan Microsoft Hyper-V
   - Untuk informasi selengkapnya tentang masuk ke konsol lokal untuk Linux Kernel-based Virtual Machine (KVM), lihat. Mengakses Konsol Lokal Gateway dengan Linux KVM
2. Pada layar menu utama Storage Gateway Configuration, masukkan angka yang sesuai untuk memilih System Time Management.
3. Pada Manajemen Waktu Sistem layar menu, masukkan angka yang sesuai untuk memilih Lihat dan Sinkronisasi Waktu Sistem.

Konsol lokal gateway menampilkan waktu sistem saat ini dan membandingkannya dengan waktu yang dilaporkan oleh server NTP, kemudian melaporkan perbedaan yang tepat antara dua kali dalam detik.

4. Jika perbedaan waktu lebih besar dari 60 detik, masukkan **y** untuk menyinkronkan waktu sistem dengan waktu NTP. Jika tidak, masukkan**n**.

   Sinkronisasi waktu mungkin memakan waktu beberapa saat.

Sinkronisasi waktu VM dengan waktu host VMware

Agar berhasil mengaktifkan gateway Anda, Anda harus memastikan bahwa waktu VM Anda disinkronkan dengan waktu host, dan waktu host diatur dengan benar. Di bagian ini, Anda terlebih dahulu menyinkronkan waktu pada VM ke waktu host. Kemudian Anda memeriksa waktu host dan, jika perlu, mengatur waktu host dan mengkonfigurasi host untuk menyinkronkan waktunya secara otomatis ke server Network Time Protocol (NTP).

> **Important**
>
> Sinkronisasi waktu VM dengan waktu host diperlukan untuk aktivasi gateway yang berhasil.

Untuk menyinkronkan waktu VM dengan waktu host

1. Konfigurasikan waktu VM Anda.

   a. Di klien vSphere, klik kanan pada nama gateway VM Anda di panel di sisi kiri jendela aplikasi untuk membuka menu konteks untuk VM, dan kemudian pilih Edit Pengaturan.

      Kotak dialog Virtual Machine Properties terbuka.

   b. Pilih tab Opsi, lalu pilih VMware Alat dari daftar opsi.

   c. Centang Sinkronisasi waktu tamu dengan host pilihan di Advanced bagian di sisi kanan kotak dialog Virtual Machine Properties, lalu pilih OK.

      VM menyinkronkan waktunya dengan host.

2. Konfigurasikan waktu host.

Penting untuk memastikan bahwa jam host Anda diatur ke waktu yang tepat. Jika Anda belum mengonfigurasi jam host Anda, lakukan langkah-langkah berikut untuk mengatur dan menyinkronkannya dengan server NTP.

a. Di klien VMware vSphere, pilih node host vSphere di panel kiri, lalu pilih tab Konfigurasi.

b. Pilih Konfigurasi Waktu di panel Perangkat Lunak, lalu pilih tautan Properties.

   Kotak dialog Konfigurasi Waktu muncul.

c. Di bawah Tanggal dan Waktu, atur tanggal dan waktu untuk host vSphere Anda.

d. Konfigurasikan host untuk menyinkronkan waktunya secara otomatis ke server NTP.

   i. Pilih Opsi di kotak dialog Konfigurasi Waktu, dan kemudian di kotak dialog Opsi Daemon NTP (ntpd), pilih Pengaturan NTP di panel kiri.

   ii. Pilih Tambah untuk menambahkan server NTP baru.

   iii. Dalam kotak dialog Add NTP Server, ketik alamat IP atau nama domain yang sepenuhnya memenuhi syarat dari server NTP, lalu pilih OK.

   Anda dapat menggunakan `pool.ntp.org` nama domain.

   iv. Dalam kotak dialog Opsi Daemon NTP (ntpd), pilih Umum di panel kiri.

   v. Di bawah Perintah Layanan, pilih Mulai untuk memulai layanan.

   Perhatikan bahwa jika Anda mengubah referensi server NTP ini atau menambahkan yang lain nanti, Anda harus memulai ulang layanan untuk menggunakan server baru.

e. Pilih OK untuk menutup kotak dialog Opsi Daemon NTP (ntpd).

f. Pilih OK untuk menutup kotak dialog Konfigurasi Waktu.

Mengkonfigurasi adapter jaringan untuk gateway Anda

Storage Gateway menggunakan adaptor jaringan tunggal VMXNET3 (10 GbE) 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

- Mengonfigurasi Gateway Anda untuk Beberapa NICs di Host VMware ESXi
- Mengkonfigurasi Gateway Anda untuk Beberapa NICs di Microsoft Hyper-V Host

Mengonfigurasi Gateway Anda untuk Beberapa NICs di Host VMware ESXi

Prosedur berikut mengasumsikan bahwa VM gateway Anda sudah memiliki satu adaptor jaringan yang ditentukan, dan menjelaskan cara menambahkan adaptor. VMware ESXi

Untuk mengkonfigurasi gateway Anda untuk menggunakan adaptor jaringan tambahan di VMware ESXi host

1. Matikan pintu gerbangnya.
2. Di klien VMware vSphere, pilih VM gateway Anda.

   VM dapat tetap dihidupkan untuk prosedur ini.
3. Di klien, buka menu konteks (klik kanan) untuk VM gateway Anda, dan pilih Edit Pengaturan.

4. Pada tab Hardware pada kotak dialog Virtual Machine Properties, pilih Tambah untuk menambahkan perangkat.
5. Ikuti panduan Add Hardware untuk menambahkan adaptor jaringan.

   a. Di panel Jenis Perangkat, pilih Adaptor Ethernet untuk menambahkan adaptor, lalu pilih Berikutnya.

   b. Di panel Network Type, pastikan Connect at power on dipilih untuk Type, lalu pilih Next.

      Kami menyarankan Anda menggunakan adaptor VMXNET3 jaringan dengan Storage Gateway. Untuk informasi selengkapnya tentang jenis adaptor yang mungkin muncul di daftar adaptor, lihat Jenis Adaptor Jaringan di Dokumentasi Server vCenter ESXi dan vCenter.

   c. Di panel Siap Selesai, tinjau informasinya, lalu pilih Selesai.
6. Pilih tab Ringkasan untuk VM, dan pilih Lihat Semua di sebelah kotak Alamat IP. Jendela Alamat IP Mesin Virtual menampilkan semua alamat IP yang dapat Anda gunakan untuk mengakses gateway. Konfirmasikan bahwa alamat IP kedua terdaftar untuk gateway.

   > **Note**
   >
   > Mungkin perlu beberapa saat agar perubahan adaptor diterapkan dan informasi ringkasan VM disegarkan.

7. Di konsol Storage Gateway, nyalakan gateway.
8. Di panel Navigasi konsol Storage Gateway, pilih Gateways dan pilih gateway tempat Anda menambahkan adaptor. Konfirmasikan bahwa alamat IP kedua tercantum di tab Detail.

Untuk informasi tentang tugas konsol lokal yang umum untuk host VMware Hyper-V, dan KVM, lihat Melakukan tugas pada konsol lokal mesin virtual

Mengkonfigurasi Gateway Anda untuk Beberapa NICs di Microsoft Hyper-V Host

Prosedur berikut mengasumsikan bahwa VM gateway Anda sudah memiliki satu adaptor jaringan yang ditentukan dan Anda menambahkan adaptor kedua. Prosedur ini menunjukkan cara menambahkan adaptor untuk host Microsoft Hyper-V.

Untuk mengonfigurasi gateway Anda untuk menggunakan adaptor jaringan tambahan di Microsoft Hyper-V Host

1. Pada konsol Storage Gateway, matikan gateway.
2. Di Microsoft Hyper-V Manager, pilih VM gateway Anda dari panel Mesin Virtual.
3. Jika VM gateway belum dimatikan, klik kanan nama VM untuk membuka menu konteks, lalu pilih Matikan.
4. Klik kanan nama VM gateway untuk membuka menu konteks, lalu pilih Pengaturan.
5. Di kotak dialog Settings, di bawah Hardware, pilih Add Hardware.
6. Di panel Add Hardware di sisi kanan kotak dialog Pengaturan, pilih Adaptor Jaringan, lalu pilih Tambah untuk menambahkan perangkat.
7. Konfigurasikan adaptor jaringan, lalu pilih Terapkan untuk menerapkan pengaturan.
8. Di kotak dialog Pengaturan, di bawah Perangkat Keras, konfirmasikan bahwa adaptor jaringan baru ditambahkan ke daftar perangkat keras, lalu pilih OK.
9. Nyalakan gateway menggunakan konsol Storage Gateway.
10. Di panel Navigasi konsol Storage Gateway, pilih Gateways, lalu pilih gateway tempat Anda menambahkan adaptor. Konfirmasikan bahwa alamat IP kedua tercantum di tab Detail.

Untuk informasi tentang tugas konsol lokal yang umum untuk host VMware Hyper-V, dan KVM, lihat Melakukan tugas pada konsol lokal mesin virtual

Menggunakan VMware VSphere Ketersediaan Tinggi dengan Storage Gateway

Storage Gateway menyediakan ketersediaan tinggi VMware melalui serangkaian pemeriksaan kesehatan tingkat aplikasi yang terintegrasi dengan VMware vSphere High Availability (HA). VMware Pendekatan ini membantu melindungi beban kerja penyimpanan terhadap kegagalan perangkat keras, hypervisor, atau jaringan. Ini juga membantu melindungi terhadap kesalahan perangkat lunak, seperti batas waktu koneksi dan berbagi file atau tidak tersedianya volume.

Dengan integrasi ini, gateway yang diterapkan di VMware lingkungan lokal atau di VMware Cloud on 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 klaster 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 klaster VMware HA:

Topik

Konfigurasikan Cluster HA vSphere VMware Anda

Pertama, jika Anda belum membuat VMware cluster, buat satu. Untuk informasi tentang cara membuat VMware klaster, lihat Membuat Cluster HA vSphere di VMware dokumentasi.

Selanjutnya, konfigurasikan VMware cluster Anda untuk bekerja dengan Storage Gateway.

Untuk mengonfigurasi VMware klaster Anda

1. Pada halaman Edit Pengaturan Cluster di VMware vSphere, pastikan bahwa pemantauan VM dikonfigurasi untuk pemantauan VM dan aplikasi. Untuk melakukannya, atur nilai berikut untuk setiap opsi:

   - Respon Kegagalan Host: Mulai Ulang VMs
   - Respons untuk Isolasi Host: Matikan dan mulai ulang VMs
   - Datastore dengan PDL: Dinonaktifkan
   - Datastore dengan APD: Dinonaktifkan
   - Pemantauan VM: VM dan Pemantauan Aplikasi
2. Sempurnakan sensitivitas cluster dengan menyesuaikan nilai-nilai berikut:

   - Interval kegagalan — Setelah interval ini, VM dimulai ulang jika detak jantung VM tidak diterima.
   - Waktu aktif minimum - Cluster menunggu selama ini setelah VM mulai memantau detak jantung alat VM.
   - Reset per-VM maksimum - Cluster me-restart VM maksimal ini berkali-kali dalam jendela waktu reset maksimum.
   - Jendela waktu reset maksimum — Jendela waktu untuk menghitung reset maksimum per VM reset.

   Jika Anda tidak yakin nilai apa yang akan ditetapkan, gunakan contoh pengaturan ini:

   - Interval kegagalan: **`30`** detik
   - Waktu aktif minimum: detik **`120`**
   - Reset per-VM maksimum: **`3`**
   - Jendela waktu reset maksimum: jam **`1`**

Jika Anda memiliki yang lain yang VMs berjalan di cluster, Anda mungkin ingin menetapkan nilai-nilai ini secara khusus untuk VM Anda. Anda tidak dapat melakukan ini sampai Anda menerapkan VM dari .ova. Untuk informasi selengkapnya tentang menyetel nilai-nilai ini, lihat(Opsional) Tambahkan Opsi Override untuk Lainnya VMs di Cluster Anda.

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 Amazon FSx File Gateway

Menyebarkan Gateway

Di cluster yang dikonfigurasi, terapkan image .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 Lainnya VMs di Cluster Anda

Jika Anda memiliki yang lain yang VMs berjalan di cluster Anda, Anda mungkin ingin mengatur nilai cluster secara khusus untuk setiap VM. Untuk petunjuk, lihat Menyesuaikan Mesin Virtual Individu di dokumentasi online VMware vSphere.

Untuk menambahkan opsi penggantian untuk yang lain VMs di klaster Anda

1. Pada halaman Ringkasan di VMware vSphere, pilih cluster Anda untuk membuka halaman cluster, lalu pilih Configure.
2. Pilih tab Configuration, lalu pilih VM Overrides.
3. Tambahkan opsi penggantian VM baru untuk mengubah setiap nilai.

   Mengatur nilai-nilai berikut untuk setiap pilihan di bawah vSphere HA - VM Monitoring:

   - Pemantauan VM: Ganti Diaktifkan - VM dan Pemantauan Aplikasi
   - Sensitivitas pemantauan VM: Ganti Diaktifkan - VM dan Pemantauan Aplikasi
   - Pemantauan VM: Kustom

- Interval kegagalan: **30** detik
- Waktu aktif minimum: detik **120**
- Reset per-VM maksimum: **5**
- Jendela waktu reset maksimum: Dalam beberapa jam **1**

Aktifkan Gateway Anda

Setelah .ova di-deploy di VMware lingkungan Anda, aktifkan gateway Anda menggunakan konsol Storage Gateway. Untuk petunjuknya, lihat dan mengaktifkan Gateway FSx File Amazon Anda.

Uji Konfigurasi Ketersediaan VMware Tinggi Anda

Setelah Anda mengaktifkan gateway Anda, uji konfigurasi Anda.

Untuk menguji konfigurasi VMware HA Anda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pada panel navigasi, pilih Gateways, lalu pilih gateway yang ingin Anda uji untuk HA. VMware
3. Untuk Tindakan, pilih Verifikasi VMware HA.
4. Di kotak Verifikasi Konfigurasi Ketersediaan VMware Tinggi yang muncul, pilih OK.

   > **Note**
   >
   > Menguji konfigurasi VMware HA Anda me-reboot VM gateway Anda dan mengganggu konektivitas ke gateway Anda. Tes mungkin memakan waktu beberapa menit untuk menyelesaikannya.

   Jika tes berhasil, status Verified muncul di tab detail gateway di konsol.
5. Pilih Keluar.

Anda dapat menemukan informasi tentang peristiwa VMware HA di grup CloudWatch log Amazon. Untuk informasi selengkapnya, lihat Mendapatkan log kesehatan 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)
- Linux (bash/zsh)
- Microsoft Windows PowerShell
- Menggunakan konsol lokal Anda

Linux (ikal)

Contoh berikut menunjukkan cara mendapatkan kunci aktivasi menggunakan Linux (curl).

> **Note**
>
> Ganti variabel yang disorot dengan nilai aktual untuk gateway Anda. Nilai yang dapat diterima adalah sebagai berikut:
>
> - *gateway_ip_address*- IPv4 Alamat gateway Anda, misalnya `172.31.29.201`
> - *gateway_type*- Jenis gateway yang ingin Anda aktifkan, seperti`STORED`,, `CACHEDVTL`,`FILE_S3`, atau`FILE_FSX_SMB`.
> - *region_code*- Wilayah tempat Anda ingin mengaktifkan gateway Anda. Lihat titik akhir Regional di Panduan Referensi AWS Umum. Jika parameter ini tidak ditentukan, atau jika nilai yang diberikan salah eja atau tidak cocok dengan wilayah yang valid, perintah akan default ke wilayah tersebut`us-east-1`.
> - *vpc_endpoint*- Nama titik akhir VPC untuk gateway Anda, misalnya. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Untuk mendapatkan kunci aktivasi untuk titik akhir publik:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Untuk mendapatkan kunci aktivasi untuk titik akhir VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

Contoh berikut menunjukkan cara menggunakan Linux (bash/zsh) untuk mengambil respons HTTP, mengurai header HTTP, dan mendapatkan kunci aktivasi.

```

```

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

Contoh berikut menunjukkan cara menggunakan Microsoft Windows PowerShell untuk mengambil respons HTTP, mengurai header HTTP, dan mendapatkan kunci aktivasi.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Menggunakan konsol lokal Anda

contoh menunjukkan cara menggunakan konsol lokal Anda untuk menghasilkan dan menampilkan kunci aktivasi.

Untuk mendapatkan kunci aktivasi untuk gateway Anda dari konsol lokal Anda

1. Masuk ke konsol lokal Anda sebagai admin.
2. Setelah Anda masuk dan melihat menu utama Aktivasi AWS Alat - Konfigurasi, pilih `0` untuk memilih Dapatkan kunci aktivasi.
3. Pilih Storage Gateway untuk opsi keluarga gateway.
4. Saat diminta, masukkan Wilayah AWS tempat Anda ingin mengaktifkan gateway Anda.
5. Masukkan 1 untuk Publik atau 2 untuk titik akhir VPC sebagai jenis jaringan.
6. Masukkan 1 Standard atau Federal 2 Information Processing Standard (FIPS) sebagai tipe endpoint.

Menggunakan Direct Connect dengan Storage Gateway

Direct Connect menautkan 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. 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 digunakan 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 sistem file 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:

- VMware tuan rumah: Mengakses Konsol Lokal Gateway dengan VMware ESXi
- Host HyperV: Akses Konsol Lokal Gateway dengan Microsoft Hyper-V
- Host Mesin Virtual (KVM) berbasis Kernel Linux: Mengakses Konsol Lokal Gateway dengan Linux KVM
- 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.

Memahami sumber daya dan sumber daya Storage Gateway IDs

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 (ARNs) 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`*
Berbagi-File ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

Bekerja dengan Sumber Daya IDs

Saat Anda membuat sumber daya, Storage Gateway menetapkan sumber daya ID sumber daya unik. ID sumber daya ini adalah bagian dari sumber daya ARN. ID sumber daya mengambil bentuk

pengenal sumber daya, diikuti oleh tanda hubung, dan kombinasi unik dari delapan huruf dan angka. Misalnya, ID gateway adalah bentuk `sgw-12A3456B` di mana `sgw` adalah pengenal sumber daya untuk gateway.

ID sumber daya Storage Gateway dalam huruf besar. Namun, saat Anda menggunakan ID sumber daya ini dengan Amazon EC2 API, Amazon EC2 mengharapkan ID sumber daya dalam huruf kecil. Anda harus mengubah ID sumber daya Anda menjadi huruf kecil untuk menggunakannya dengan EC2 API. Misalnya, di Storage Gateway ID untuk volume mungkin`vol-1122AABB`. Saat Anda menggunakan ID ini dengan EC2 API, Anda harus mengubahnya menjadi`vol-1122aabb`. Jika tidak, API EC2 mungkin tidak berperilaku seperti yang diharapkan.

> **Important**
>
> IDs untuk volume Storage Gateway dan snapshot Amazon EBS yang dibuat dari volume gateway berubah ke format yang lebih panjang. Mulai Desember 2016, semua volume dan snapshot baru akan dibuat dengan string 17 karakter. Mulai April 2016, Anda akan dapat menggunakan ini lebih lama IDs sehingga Anda dapat menguji sistem Anda dengan format baru. Untuk informasi selengkapnya, lihat Sumber Daya EC2 dan EBS yang Lebih Panjang. IDs
>
> Misalnya, ARN volume dengan format ID volume yang lebih panjang akan terlihat seperti ini: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
>
> ID snapshot dengan format ID yang lebih panjang akan terlihat seperti ini:`snap-78e226633445566ee`.
>
> Untuk informasi selengkapnya, lihat Pengumuman: Heads-up - Volume dan snapshot Storage Gateway yang lebih lama IDs akan hadir pada tahun 2016.

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 rekaman virtual yang ditandai, rekaman itu mempertahankan tagnya di arsip. Demikian pula, jika Anda mengambil rekaman dari arsip ke gateway lain, tag dipertahankan di gateway baru.

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 huruf dan angka UTF-8, spasi, dan karakter khusus + - =. _:/dan @.

Bekerja dengan tag

Anda dapat bekerja dengan tag dengan menggunakan konsol Storage Gateway, Storage Gateway API, atau Storage Gateway Command Line Interface (CLI). Prosedur berikut menunjukkan cara menambahkan, mengedit, dan menghapus tag di konsol.

Untuk menambahkan tag

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Di panel navigasi, pilih sumber daya yang ingin Anda tag.

   Misalnya, untuk menandai gateway, pilih Gateway, lalu pilih gateway yang ingin Anda tag dari daftar gateway.
3. Pilih Tag, lalu pilih Tambah/edit tag.

4. Dalam kotak dialog Tambah/edit tag, pilih Buat tag.
5. Ketik kunci untuk 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/rumah.
2. Pilih sumber daya yang tagnya ingin Anda edit.
3. Pilih Tag untuk membuka kotak dialog Tambah/edit tag.
4. Pilih ikon pensil di sebelah tag yang ingin Anda edit, lalu edit tag.
5. Setelah selesai mengedit tag, pilih Simpan.

Untuk menghapus tanda

1. Buka konsol Storage Gateway di https://console.aws.amazon.com/storagegateway/rumah.
2. Pilih sumber daya yang tagnya ingin Anda hapus.
3. Pilih Tag, lalu pilih Tambah/edit tag untuk membuka kotak dialog Tambah/edit tag.
4. Pilih ikon X di sebelah tag yang ingin Anda hapus, lalu pilih Simpan.

Bekerja dengan komponen sumber terbuka untuk AWS Storage Gateway

Bagian ini menjelaskan alat dan lisensi pihak ketiga yang kami andalkan untuk memberikan AWS Storage Gateway fungsionalitas.

Topik

Komponen open source 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 pada VMware ESXi: sources.tar
- Untuk peralatan Storage Gateway yang digunakan di Microsoft Hyper-V: sources_hyperv.tar
- Untuk peralatan Storage Gateway yang digunakan di Virtual Machine (KVM) berbasis Kernel Linux: sources_KVM.tar

Produk ini mencakup perangkat lunak yang dikembangkan oleh proyek OpenSSL untuk digunakan dalam OpenSSL Toolkit (http://www.openssl.org/). Untuk lisensi yang relevan untuk semua alat pihak ketiga yang bergantung, lihat Lisensi Pihak Ketiga.

Komponen sumber terbuka untuk Amazon FSx File Gateway

Beberapa alat dan lisensi pihak ketiga digunakan untuk memberikan fungsionalitas Amazon FSx File Gateway (FSx File Gateway).

Gunakan tautan berikut untuk mengunduh kode sumber untuk komponen perangkat lunak sumber terbuka tertentu yang disertakan dengan perangkat lunak FSx File Gateway:

- Untuk Amazon FSx File Gateway 2021-07-07 Rilis: -open-source.tgz sgw-file-fsx-smb
- Untuk Rilis Amazon FSx File Gateway 2021-04-06: -20210406-open-source.tgz sgw-file-fsx-smb

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 tautan berikut:

- Untuk Amazon FSx File Gateway 2021-07-07 Rilis: Lisensi Pihak Ketiga.
- Untuk Amazon FSx File Gateway 2021-04-06 Rilis: Lisensi Pihak Ketiga.

Batas dan kuota untuk

Kuota untuk sistem FSx file Amazon

Tabel berikut mencantumkan batas minimum dan maksimum dan kuota untuk sistem FSx file Amazon.

Sumber daya	Batas per sistem FSx file Amazon
Jumlah maksimum tag	50 tag
Periode penyimpanan maksimum untuk cadangan otomatis	90 hari
Jumlah maksimum permintaan salinan cadangan yang sedang berlangsung ke satu Wilayah tujuan per akun.	5 permintaan
Kapasitas penyimpanan minimum untuk sistem file SSD	32 GiB
Kapasitas penyimpanan minimum untuk sistem file HDD	2.000 GiB
Kapasitas penyimpanan maksimum untuk sistem file SSD dan HDD	64 TiB
Kapasitas throughput minimum	8 MBps
Kapasitas throughput maksimum	2,048 MBps
Jumlah maksimum pembagian FSx file Amazon	100.000

Ukuran disk lokal yang direkomendasikan untuk gateway Anda

Tabel berikut merekomendasikan ukuran untuk penyimpanan disk lokal untuk masing-masing AWS Storage Gateway dalam penerapan Anda.

Jenis Gateway	Cache (Minimum)	Cache (Maksimum)	
FSx Gerbang 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 File FSx yang ada, penting untuk membuat disk baru di host virtual Anda (hypervisor atau instans Amazon EC2). Jangan mengubah ukuran disk yang ada jika disk sebelumnya telah dialokasikan sebagai cache.

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
`MaximumVolumeCount Exceeded`	Jumlah volume maksimum terlampaui.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	Konfigurasi jaringan gateway telah berubah.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`NotSupported`	Operasi yang ditentukan tidak didukung.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	Gateway yang ditentukan sudah ketinggalan zaman.	ActivateGateway
`SnapshotInProgressException`	Snapshot yang ditentukan sedang berlangsung.	DeleteVolume
`SnapshotIdInvalid`	Snapshot yang ditentukan tidak valid.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`StagingAreaFull`	Area pementasan penuh.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetAlreadyExists`	Target yang ditentukan sudah ada.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	Target yang ditentukan tidak valid.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	Target yang ditentukan tidak ditemukan.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`UnsupportedOperationForGatewayType`	Operasi yang ditentukan tidak valid untuk jenis gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Volume yang ditentukan sudah ada.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	Volume yang ditentukan tidak valid.	DeleteVolume
`VolumeInUse`	Volume yang ditentukan sudah digunakan.	DeleteVolume

Kode Kesalahan Operasi	Pesan	Operasi yang Mengembalikan Kode Kesalahan ini
`VolumeNotFound`	Volume yang ditentukan tidak ditemukan.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	Volume yang ditentukan belum siap.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Respons Kesalahan

Ketika ada kesalahan, informasi header respons berisi:

- Tipe Konten: aplikasi/ -1.1 x-amz-json
- Kode status yang sesuai `4xx` atau `5xx` HTTP

Tubuh respons kesalahan berisi informasi tentang kesalahan yang terjadi. Contoh 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 Amazon FSx File Gateway

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
Pemberitahuan perubahan ketersediaan untuk FSx File Gateway	Amazon FSx File Gateway tidak lagi tersedia untuk pelanggan baru. Pelanggan FSx File Gateway yang ada dapat terus menggunakan layanan ini secara normal. Untuk kemampuan yang mirip dengan FSx File Gateway, kunjungi posting blog ini.	Oktober 28, 2024
Pemberitahuan perubahan ketersediaan untuk FSx File Gateway	AWS Storage Gateway FSx File Gateway tidak akan lagi tersedia untuk pelanggan baru mulai 10/28/24. Untuk menggunakan layanan ini, Anda harus mendaftar sebelum tanggal tersebut. Pelanggan FSx File Gateway yang ada dapat terus menggunakan layanan ini secara normal. Untuk kemampuan yang mirip dengan FSx File Gateway, kunjungi posting blog ini.	September 26, 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
CloudWatch Alarm yang direkomendasikan diperbarui	CloudWatch `HealthNotifications` Alarm sekarang berlaku untuk dan direkomendasikan untuk semua jenis gateway dan platform host. Pengaturan konfigurasi yang disarankan juga telah diperbarui untuk `HealthNotifications` dan`AvailabilityNotifications` . Untuk informasi selengkapnya lihat .	2 Oktober 2023

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 kiat pemecahan masalah Direktori Aktif Gabung Domain	Bagian Pemecahan Masalah: Masalah File Gateway sekarang menyertakan panduan pemecahan masalah untuk membantu mendiagnosis masalah yang mungkin Anda temui saat mencoba bergabung dengan gateway Anda ke domain Direktori Aktif. Untuk informasi selengkapnya, lihat Pemecahan masalah: Masalah domain Direktori Aktif.	Oktober 19, 2022
Prosedur pembuatan gateway yang diperbarui	Prosedur untuk membuat gateway baru telah diperbarui untuk mencerminkan perubahan di konsol Storage Gateway. Untuk informasi selengkapnya, lihat Membuat dan mengaktifkan Gateway File Amazon S3.	Oktober 12, 2021

Dukungan beberapa sistem file	Amazon FSx File Gateway sekarang mendukung hingga lima sistem FSx file Amazon terlampir. Untuk informasi selengkapnya, lihat Melampirkan sistem file Amazon FSx untuk Windows File Server.	7 Juli 2021
Dukungan kuota penyimpanan FSx lunak Amazon	Amazon FSx File Gateway sekarang mendukung kuota penyimpanan lunak (yang memperingatkan Anda ketika pengguna melampaui batas data mereka) saat menulis ke sistem FSx file Amazon terlampir di mana kuota penyimpanan dikonfigurasi. Kuota keras (yang memberlakukan batasan data dengan menolak akses tulis) tidak didukung. Kuota lunak berfungsi untuk semua pengguna kecuali pengguna FSx admin Amazon. Untuk informasi selengkapnya tentang mengatur kuota penyimpanan, lihat Kuota penyimpanan di Panduan Pengguna Amazon FSx untuk Windows File Server.	7 Juli 2021

Panduan baru	Selain File Gateway asli (sekarang dikenal sebagai Amazon S3 File Gateway), Storage Gateway menyediakan Amazon FSx File Gateway (FSx File Gateway). FSx File Gateway menyediakan latensi rendah dan akses efisien ke in-cloud FSx untuk berbagi file Windows File Server dari fasilitas lokal Anda. Untuk informasi selengkapnya, lihat Apa itu Amazon FSx File Gateway?	27 April 2021
Kepatuhan FedRAMP	Storage Gateway sekarang sesuai dengan FedRAMP. Untuk informasi selengkapnya, lihat Validasi kepatuhan untuk Storage Gateway.	24 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
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 selengkapnya, 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 Processing 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 File Gateway untuk otorisasi berbasis tag	File Gateway sekarang mendukung otorisasi berbasis tag. Anda dapat mengontro l akses ke sumber daya File Gateway berdasarkan tag pada sumber daya tersebut. Anda juga dapat mengontro l 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

Pembaruan lebih awal

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS Storage Gateway Pengguna sebelum Mei 2018.

Ubah	Deskripsi	Tanggal Diubah
Baru Wilayah AWS	Tape Gateway sekarang tersedia di Wilayah Asia Pasifik (Singapura). Untuk detail informasi, lihat Wilayah AWS yang mendukung Storage Gateway.	3 April 2018
Baru Wilayah AWS	Storage Gateway sekarang tersedia di Wilayah Eropa (Paris). Untuk detail informasi, lihat Wilayah AWS yang mendukung Storage Gateway.	18 Desember 2017
Support untuk VMware ESXi Hypervisor versi 6.5	AWS Storage Gateway sekarang mendukung VMware ESXi Hypervisor versi 6.5. Ini adalah tambahan untuk versi 4.1, 5.0, 5.1, 5.5, dan 6.0. Untuk informasi selengkapnya, lihat Hypervisor dan persyaratan host yang didukung.	13 September 2017
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 AWS yang mendukung Storage Gateway.	02 Mei 2017
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	Februari 08, 2017

Ubah	Deskripsi	Tanggal Diubah
	Amazon FSx File Gateway Untuk informasi tentang cara meluncurkan AMI File Gateway, lihatMenerapkan host FSx Amazon EC2 default untuk 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.	
Baru Wilayah AWS	Storage Gateway sekarang tersedia di Wilayah Eropa (London). Untuk detail informasi, lihat Wilayah AWS yang mendukung Storage Gateway.	13 Desember 2016
Baru Wilayah AWS	Storage Gateway sekarang tersedia di Wilayah Kanada (Tengah). Untuk detail informasi, lihat Wilayah AWS yang 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