aws

Panduan Pengguna Windows

Amazon FSx untuk Server File Windows

Amazon FSx untuk Server File Windows: Panduan Pengguna Windows

Table of Contents

Apa itu FSx untuk Windows File Server?

Amazon FSx untuk Windows File Server menyediakan server file Microsoft Windows yang dikelola sepenuhnya, didukung oleh sistem file Windows yang sepenuhnya asli. FSx untuk Windows File Server memiliki fitur, kinerja, dan kompatibilitas untuk dengan mudah mengangkat dan mengalihkan aplikasi perusahaan ke file AWS Cloud.

Amazon FSx mendukung serangkaian beban kerja Windows perusahaan yang luas dengan penyimpanan file yang dikelola sepenuhnya yang dibangun di Microsoft Windows Server. Amazon FSx memiliki dukungan asli untuk fitur sistem file Windows dan untuk protokol Server Message Block (SMB) standar industri untuk mengakses penyimpanan file melalui jaringan. Amazon FSx dioptimalkan untuk aplikasi perusahaan di AWS Cloud, dengan kompatibilitas Windows asli, kinerja dan fitur perusahaan, dan latensi sub-milidetik yang konsisten.

Dengan penyimpanan file di Amazon FSx, kode, aplikasi, dan alat yang digunakan pengembang dan administrator Windows saat ini dapat terus bekerja tanpa perubahan. Aplikasi dan beban kerja Windows yang ideal untuk Amazon FSx mencakup aplikasi bisnis, direktori rumah, penayangan web, manajemen konten, analitik data, pengaturan pembuatan perangkat lunak, dan beban kerja pemrosesan media.

Sebagai layanan yang dikelola sepenuhnya, FSx untuk Windows File Server menghilangkan overhead administratif pengaturan dan penyediaan server file dan volume penyimpanan. Selain itu, Amazon FSx terus memperbarui perangkat lunak Windows, mendeteksi dan mengatasi kegagalan perangkat keras, dan melakukan pencadangan. Ini juga menyediakan integrasi yang kaya dengan AWS layanan lain seperti AWS IAM, AWS Directory Service for Microsoft Active Directory, Amazon WorkSpaces AWS Key Management Service, dan AWS CloudTrail.

FSx untuk sumber daya Windows File Server: sistem file, backup, dan berbagi file

Sumber daya utama di Amazon FSx adalah sistem file dan cadangan. Sebuah sistem file adalah tempat Anda menyimpan dan mengakses file dan folder Anda. Sebuah sistem file terdiri dari satu atau beberapa server file Windows dan volume penyimpanan. Saat Anda membuat sistem file, Anda menentukan jumlah kapasitas penyimpanan (dalam GiB), IOPS SSD, dan kapasitas throughput (in). MBps Anda dapat mengubah properti ini saat kebutuhan Anda berubah setelah Anda membuat sistem file tersebut. Lihat informasi selengkapnya di Mengelola kapasitas penyimpanan, Mengelola SSD IOPS, dan Mengelola kapasitas throughput.

FSx untuk Windows File Server backup file-system-consistent, sangat tahan lama, dan inkremental. Untuk memastikan konsistensi sistem file, Amazon FSx menggunakan Volume Shadow Copy Service (VSS) di Microsoft Windows. Backup harian otomatis diaktifkan secara default saat Anda membuat sistem file, dan Anda juga dapat mengambil backup manual tambahan kapan saja. Untuk informasi selengkapnya, lihat Melindungi data Anda dengan backup.

Berbagi file Windows adalah folder tertentu (dan subfolder) dalam sistem file Anda yang Anda buat dapat diakses untuk instans komputasi dengan SMB. Sistem file Anda sudah dilengkapi dengan berbagi file Windows default yang disebut `\share`. Anda dapat membuat dan mengelola sebanyak berbagi file Windows lainnya sesuai keinginan Anda dengan menggunakan alat antarmuka pengguna grafis (GUI) Folder Bersama pada Windows. Untuk informasi selengkapnya, lihat Mengakses data menggunakan berbagi file.

Berbagi file diakses menggunakan nama DNS sistem file atau alias DNS yang Anda kaitkan dengan sistem file tersebut. Untuk informasi selengkapnya, lihat Mengelola alias DNS.

Mengakses berbagi file

Amazon dapat FSx diakses dari instans komputasi dengan protokol SMB (mendukung versi 2.0 hingga 3.1.1). Anda dapat mengakses berbagi Anda dari semua versi Windows mulai dari Windows Server 2008 dan Windows 7, dan juga dari versi Linux saat ini. Anda dapat memetakan pembagian FSx file Amazon di instans Amazon Elastic Compute Cloud (Amazon EC2), dan pada WorkSpaces instans, instans Amazon AppStream 2.0, dan Cloud on. VMware AWS VMs

Anda dapat mengakses berbagi file dari instans komputasi on-premise menggunakan AWS Direct Connect atau AWS VPN. Selain mengakses berbagi file yang berada di VPC AWS , akun, Wilayah AWS dan sistem file yang sama, Anda juga dapat mengakses saham Anda dari instance komputasi yang ada di VPC Amazon, akun, atau akun yang berbeda. Wilayah AWS Anda melakukannya dengan menggunakan peering VPC atau transit gateway. Untuk informasi selengkapnya, lihat Mengakses data dari dalam AWS Cloud.

Keamanan dan perlindungan data

Amazon FSx menyediakan berbagai tingkat keamanan dan kepatuhan untuk membantu memastikan bahwa data Anda terlindungi. Ini secara otomatis mengenkripsi data saat istirahat (untuk sistem file dan cadangan) menggunakan kunci yang Anda kelola di (). AWS Key Management Service AWS KMS Data in transit juga secara otomatis dienkripsi menggunakan kunci sesi Kerberos SMB. Ia telah dinilai untuk mematuhi sertifikasi ISO, PCI-DSS, dan SOC, dan telah memenuhi syarat HIPAA.

Amazon FSx menyediakan kontrol akses pada tingkat file dan folder dengan daftar kontrol akses Windows (ACLs). Ia menyediakan kontrol akses pada tingkat sistem file menggunakan grup keamanan Virtual Private Cloud (Amazon VPC) dari Amazon. Selain itu, ia juga menyediakan kontrol akses pada tingkat API menggunakan kebijakan akses AWS Identity and Access Management (IAM). Pengguna yang mengakses sistem file diautentikasi dengan Direktori Aktif Microsoft. Amazon FSx terintegrasi dengan AWS CloudTrail untuk memantau dan mencatat panggilan API Anda yang memungkinkan Anda melihat tindakan yang diambil oleh pengguna di FSx sumber daya Amazon Anda.

Selain itu, ia melindungi data Anda dengan mengambil backup yang sangat berdaya tahan dari sistem file Anda secara otomatis setiap hari dan memungkinkan Anda untuk mengambil backup tambahan di setiap titik. Untuk informasi selengkapnya, lihat Keamanan di Amazon FSx.

Ketersediaan dan daya tahan

FSx untuk Windows File Server menawarkan sistem file dengan dua tingkat ketersediaan dan daya tahan. File Single-AZ memastikan ketersediaan tinggi dalam Availability Zone tunggal (AZ) dengan mendeteksi dan menangani kegagalan komponen secara otomatis. Selain itu, sistem file multi-AZ menyediakan ketersediaan tinggi dan dukungan failover di beberapa Availability Zone dengan menyediakan dan memelihara server file siaga di Availability Zone terpisah dalam suatu Wilayah. AWS Untuk mempelajari lebih lanjut tentang deployment sistem file Single-AZ dan Multi-AZ, lihat Ketersediaan dan daya tahan: Sistem file Single-AZ dan Multi-AZ.

Mengelola sistem file

Anda dapat mengelola sistem file Windows File Server Anda FSx menggunakan PowerShell perintah manajemen jarak jauh kustom, atau menggunakan GUI asli Windows dalam beberapa kasus. Untuk mempelajari selengkapnya tentang mengelola sistem FSx file Amazon, lihatMengelola FSx untuk sistem file Windows.

Fleksibilitas harga dan performa

FSx untuk Windows File Server memberi Anda fleksibilitas harga dan kinerja dengan menawarkan jenis penyimpanan solid state drive (SSD) dan hard disk drive (HDD). Penyimpanan HDD dirancang untuk spektrum beban kerja yang luas, termasuk direktori beranda, berbagi pengguna dan departemen, dan sistem pengelolaan konten. Penyimpanan SSD dirancang untuk beban kerja

dengan performa tertinggi dan paling sensitif terhadap latensi, termasuk basis data, beban kerja pemrosesan media, dan aplikasi analitik data.

Dengan FSx Windows File Server, Anda dapat menyediakan penyimpanan sistem file, SSD IOPS, dan throughput secara independen untuk mencapai campuran biaya dan kinerja yang tepat. Anda dapat memodifikasi penyimpanan sistem file Anda, IOPS SSD, dan kapasitas throughput untuk memenuhi kebutuhan beban kerja yang berubah, sehingga Anda hanya membayar untuk apa yang Anda butuhkan.

Harga untuk Amazon FSx

Dengan Amazon FSx, tidak ada biaya perangkat keras atau perangkat lunak di muka. Anda hanya harus membayar sumber daya yang digunakan, tanpa komitmen minimum, biaya penyiapan, atau biaya tambahan. Untuk informasi tentang harga dan biaya yang terkait dengan layanan, lihat Harga Amazon FSx untuk Windows File Server.

Asumsi

Untuk menggunakan Amazon FSx, Anda memerlukan AWS akun dengan EC2 instans Amazon, WorkSpaces instance, instans AppStream 2.0, atau VM yang berjalan di VMware Cloud pada AWS lingkungan jenis yang didukung.

Dalam panduan ini, kami membuat asumsi sebagai berikut:

- Jika Anda menggunakan Amazon EC2, kami berasumsi bahwa Anda sudah familiar dengan Amazon EC2. Untuk informasi selengkapnya tentang cara menggunakan Amazon EC2, lihat dokumentasi Amazon Elastic Compute Cloud.
- Jika Anda menggunakan WorkSpaces, kami berasumsi bahwa Anda sudah familiar dengannya WorkSpaces. Untuk informasi selengkapnya tentang cara menggunakan WorkSpaces, lihat Panduan WorkSpaces Pengguna Amazon.
- Jika Anda menggunakan VMware Cloud AWS, kami berasumsi bahwa Anda sudah familiar dengannya. Untuk informasi selengkapnya, lihat VMware Cloud on AWS.
- Kami berasumsi bahwa Anda sudah familiar dengan konsep Direktori Aktif Microsoft.

Prasyarat

Untuk membuat sistem FSx file Amazon, Anda memerlukan yang berikut ini:

- AWS Akun dengan izin yang diperlukan untuk membuat sistem FSx file Amazon dan EC2 instance Amazon. Untuk informasi selengkapnya, lihat Menyiapkan Akun AWS.
- EC2 Instans Amazon yang menjalankan Microsoft Windows Server di cloud pribadi virtual (VPC) berdasarkan layanan Amazon VPC yang ingin Anda kaitkan dengan sistem file Amazon Anda. FSx Untuk informasi tentang cara membuatnya, lihat Memulai Instans Amazon EC2 Windows di Panduan EC2 Pengguna Amazon.
- Amazon FSx bekerja dengan Microsoft Active Directory untuk melakukan otentikasi pengguna dan kontrol akses. Anda bergabung dengan sistem FSx file Amazon Anda ke Microsoft Active Directory saat membuatnya. Untuk informasi selengkapnya, lihat Bekerja dengan Microsoft Active Directory.
- Panduan ini mengasumsikan bahwa Anda belum mengubah aturan di grup keamanan default untuk VPC Anda berdasarkan layanan Amazon VPC. Jika sudah, Anda perlu memastikan bahwa Anda menambahkan aturan yang diperlukan untuk mengizinkan lalu lintas jaringan dari EC2 instans Amazon Anda ke sistem FSx file Amazon Anda. Untuk detail selengkapnya, lihat Keamanan di Amazon FSx.
- Instal dan konfigurasikan AWS Command Line Interface (AWS CLI). Versi yang didukung adalah 1.9.12 dan yang lebih baru. Untuk informasi selengkapnya, lihat Menginstal, memperbarui, dan mencopot instalasi AWS CLI di Panduan Pengguna AWS Command Line Interface .

> **Note**
>
> Anda dapat memeriksa versi yang AWS CLI Anda gunakan dengan `aws --version` perintah.

Amazon FSx untuk forum Server File Windows

Jika Anda mengalami masalah saat menggunakan Amazon FSx, gunakan forum.

Apakah Anda pengguna Amazon FSx pertama kali?

Jika Anda adalah pengguna Amazon pertama kali FSx, kami sarankan Anda membaca bagian berikut secara berurutan:

1. Jika Anda siap untuk membuat sistem FSx file Amazon pertama Anda, cobaMemulai Amazon FSx untuk Windows File Server.
2. Untuk informasi tentang kinerja, lihatFSx untuk kinerja Windows File Server.

3. Untuk detail FSx keamanan Amazon, lihatKeamanan di Amazon FSx.
4. Untuk informasi tentang Amazon FSx API, lihat Referensi Amazon FSx API.

Praktik terbaik FSx untuk Windows File Server

Kami menyarankan Anda mengikuti praktik terbaik ini saat bekerja dengan Amazon FSx untuk Windows File Server.

Topik

Praktik terbaik umum

Membuat rencana pemantauan

Anda dapat menggunakan metrik sistem file untuk memantau penyimpanan dan penggunaan kinerja Anda, memahami pola penggunaan Anda, dan memicu pemberitahuan ketika penggunaan Anda mendekati batas penyimpanan atau kinerja sistem file Anda. Memantau sistem FSx file Amazon Anda bersama dengan lingkungan aplikasi lainnya memungkinkan Anda men-debug masalah apa pun yang dapat memengaruhi kinerja dengan cepat.

Memastikan bahwa sistem file Anda memiliki sumber daya yang memadai

Memiliki sumber daya yang tidak mencukupi dapat mengakibatkan peningkatan latensi dan antrian untuk permintaan I/O, yang mungkin tampak sebagai tidak tersedianya sistem file Anda secara lengkap atau sebagian. Untuk informasi selengkapnya tentang memantau kinerja dan mengakses peringatan dan rekomendasi kinerja, lihat. Peringatan dan rekomendasi kinerja

Praktik terbaik keamanan

Kami menyarankan Anda mengikuti praktik terbaik ini untuk mengelola keamanan dan kontrol akses sistem file Anda. Untuk informasi lebih rinci tentang mengonfigurasi Amazon FSx untuk memenuhi tujuan keamanan dan kepatuhan Anda, lihatKeamanan di Amazon FSx.

Keamanan jaringan

Jangan memodifikasi atau menghapus ENI yang terkait dengan sistem file Anda

Sistem FSx file Amazon Anda diakses melalui elastic network interface (ENI) yang berada di virtual private cloud (VPC) yang terkait dengan sistem file Anda. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan koneksi hilang permanen antara VPC dan sistem file Anda.

Menggunakan grup keamanan dan jaringan ACLs

Anda dapat menggunakan grup keamanan dan daftar kontrol akses jaringan (ACLs) untuk membatasi akses ke sistem file Anda. Untuk grup keamanan VPC, grup keamanan default sudah ditambahkan ke sistem file Anda di konsol. Pastikan bahwa grup keamanan dan jaringan ACLs untuk subnet tempat Anda membuat sistem file memungkinkan lalu lintas di port.

Direktori Aktif

Saat membuat sistem FSx file Amazon, Anda dapat menggabungkannya ke domain Microsoft Active Directory untuk memberikan autentikasi pengguna, dan otorisasi kontrol akses tingkat berbagi, file, dan folder. Pengguna Anda dapat menggunakan akun Active Directory yang ada untuk terhubung ke berbagi file dan mengakses file dan folder di dalamnya. Selain itu, Anda dapat memigrasikan konfigurasi ACL keamanan yang ada ke Amazon FSx tanpa modifikasi apa pun. Amazon FSx memberi Anda dua opsi untuk Active Directory: Microsoft Active Directory yang AWS dikelola atau Microsoft Active Directory yang dikelola sendiri.

Jika Anda menggunakan Microsoft Active Directory yang AWS dikelola, sebaiknya tinggalkan pengaturan default grup keamanan Active Directory Anda. Jika Anda mengubah pengaturan ini, pastikan Anda mempertahankan konfigurasi jaringan yang memenuhi persyaratan jaringan. Untuk informasi selengkapnya, lihat Prasyarat jaringan.

Jika Anda menggunakan Microsoft Active Directory yang dikelola sendiri, Anda memiliki opsi tambahan untuk mengonfigurasi sistem file Anda. Kami merekomendasikan praktik terbaik berikut untuk konfigurasi awal saat menggunakan Amazon FSx dengan Microsoft Active Directory yang dikelola sendiri:

- Tetapkan subnet ke satu situs Direktori Aktif: Jika lingkungan Direktori Aktif Anda memiliki sejumlah besar pengontrol domain, gunakan Situs dan Layanan Direktori Aktif untuk menetapkan subnet yang digunakan oleh sistem FSx file Amazon Anda ke satu situs Direktori Aktif dengan

ketersediaan dan keandalan tertinggi. Pastikan bahwa grup keamanan VPC, ACL jaringan VPC, aturan firewall Windows pada Anda DCs, dan kontrol perutean jaringan lainnya yang Anda miliki di infrastruktur Direktori Aktif memungkinkan komunikasi dari Amazon pada port yang diperlukan. FSx Ini memungkinkan Windows untuk kembali ke yang lain DCs jika tidak dapat menggunakan situs Active Directory yang ditetapkan. Untuk informasi selengkapnya, lihat Kontrol akses sistem file dengan Amazon VPC.

- Gunakan Unit Organisasi (OU) terpisah: Gunakan OU untuk sistem FSx file Amazon Anda yang terpisah dari unit organisasi lain yang mungkin Anda miliki.
- Konfigurasikan akun layanan Anda dengan hak istimewa minimum yang diperlukan: Konfigurasikan atau delegasikan akun layanan yang Anda berikan ke Amazon FSx dengan hak istimewa minimum yang diperlukan. Untuk informasi selengkapnya, lihat Menggunakan Microsoft Active Directory yang dikelola sendiri.
- Verifikasi konfigurasi Direktori Aktif Anda secara terus-menerus: Jalankan alat validasi Direktori Aktif Amazon FSx terhadap konfigurasi Direktori Aktif Anda sebelum membuat sistem FSx file Amazon Anda untuk memverifikasi bahwa konfigurasi Anda valid untuk digunakan dengan Amazon FSx, dan untuk menemukan peringatan dan kesalahan apa pun yang mungkin diekspos oleh alat tersebut.

Hindari kehilangan ketersediaan karena kesalahan konfigurasi Active Directory

Saat menggunakan Amazon FSx dengan Microsoft Active Directory yang dikelola sendiri, penting untuk memiliki konfigurasi Active Directory yang valid tidak hanya selama pembuatan sistem file Anda, tetapi juga untuk operasi dan ketersediaan yang sedang berlangsung. Selama peristiwa pemulihan kegagalan, peristiwa pemeliharaan rutin, dan tindakan pembaruan kapasitas throughput, Amazon FSx menggabungkan kembali sumber daya server file ke Direktori Aktif Anda. Jika konfigurasi Active Directory tidak valid selama peristiwa, sistem file Anda berubah menjadi status Salah Konfigurasi, dan berisiko menjadi tidak tersedia. Berikut adalah beberapa cara yang dapat Anda hindari kehilangan ketersediaan:

- Perbarui konfigurasi Direktori Aktif Anda dengan Amazon FSx: Jika Anda membuat perubahan, seperti mengatur ulang kata sandi akun layanan Anda, pastikan Anda memperbarui konfigurasi untuk sistem file apa pun yang menggunakan akun layanan ini.
- Monitor untuk kesalahan konfigurasi Active Directory: Setel pemberitahuan status yang salah konfigurasi untuk diri Anda sendiri sehingga Anda dapat mengatur ulang konfigurasi Active

Directory sistem file Anda, jika perlu. Untuk contoh yang menggunakan solusi berbasis Lambda untuk mencapai hal ini, lihat Memantau kesehatan sistem FSx file Amazon menggunakan Amazon EventBridge dan. AWS Lambda

- Validasi konfigurasi Active Directory Anda secara teratur: Jika Anda ingin secara proaktif mendeteksi kesalahan konfigurasi Active Directory, kami sarankan Anda menjalankan alat Validasi Direktori Aktif terhadap konfigurasi Direktori Aktif Anda secara berkelanjutan. Jika Anda menerima peringatan atau kesalahan saat menjalankan alat validasi, itu berarti sistem file Anda berisiko salah konfigurasi.
- Jangan memindahkan atau memodifikasi objek komputer yang dibuat oleh FSx: Amazon FSx membuat dan mengelola objek komputer di Direktori Aktif Anda, menggunakan akun layanan dan izin yang Anda berikan. Memindahkan atau memodifikasi objek komputer ini dapat mengakibatkan sistem file Anda menjadi salah konfigurasi.

Jendela ACLs

Dengan Amazon FSx, Anda menggunakan daftar kontrol akses Windows standar (ACLs) untuk kontrol akses tingkat berbagi, file, dan folder berbutir halus. Sistem FSx file Amazon secara otomatis memverifikasi kredensil pengguna yang mengakses data sistem file untuk menegakkan Windows ini. ACLs

- Jangan mengubah izin ACL NTFS untuk pengguna SYSTEM: Amazon FSx mengharuskan pengguna SYSTEM memiliki kontrol penuh izin NTFS ACL pada semua folder dalam sistem file Anda. Mengubah izin ACL NTFS untuk pengguna SYSTEM dapat mengakibatkan sistem file Anda menjadi tidak dapat diakses dan backup sistem file future mungkin menjadi tidak dapat digunakan.

Mengkonfigurasi dan mengukur sistem file Anda dengan benar

Memilih jenis penerapan

Amazon FSx menyediakan dua opsi penerapan: Single-AZ dan Multi-AZ. Sebaiknya gunakan sistem file Multi-AZ untuk sebagian besar beban kerja produksi yang memerlukan ketersediaan tinggi untuk data file Windows bersama. Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan: Sistem file Single-AZ dan Multi-AZ.

Memilih kapasitas throughput

Konfigurasikan sistem file Anda dengan kapasitas throughput yang cukup untuk memenuhi tidak hanya lalu lintas yang diharapkan dari beban kerja Anda, tetapi juga sumber daya kinerja tambahan yang diperlukan untuk mendukung fitur yang ingin Anda aktifkan pada sistem file Anda. Misalnya, jika Anda menjalankan deduplikasi data, kapasitas throughput yang Anda pilih harus menyediakan memori yang cukup untuk menjalankan deduplikasi berdasarkan penyimpanan yang Anda miliki. Jika Anda menggunakan salinan bayangan, tingkatkan kapasitas throughput ke nilai yang setidaknya tiga kali lipat dari nilai yang diharapkan didorong oleh beban kerja Anda untuk menghindari Windows Server menghapus salinan bayangan Anda. Untuk informasi selengkapnya, lihat Dampak kapasitas throughput terhadap performa.

Meningkatkan kapasitas penyimpanan dan kapasitas throughput

Tingkatkan kapasitas penyimpanan sistem file Anda ketika hampir habis pada penyimpanan gratis, atau ketika Anda mengharapkan kebutuhan penyimpanan Anda tumbuh lebih besar dari batas penyimpanan saat ini. Kami merekomendasikan untuk mempertahankan setidaknya 20% dari kapasitas penyimpanan gratis setiap saat di sistem file Anda. Kami juga merekomendasikan peningkatan kapasitas throughput setidaknya 20% sebelum meningkatkan kapasitas penyimpanan untuk mengimbangi dampak kinerja apa pun selama peningkatan penyimpanan. Anda dapat menggunakan FreeStorageCapacity CloudWatch metrik untuk memantau jumlah penyimpanan gratis yang tersedia dan memahami bagaimana trennya. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan.

Anda juga harus meningkatkan kapasitas throughput sistem file Anda jika beban kerja Anda dibatasi oleh batas kinerja saat ini. Anda dapat menggunakan halaman Pemantauan dan kinerja di FSx konsol untuk melihat kapan tuntutan beban kerja telah mendekati atau melampaui batas kinerja untuk menentukan apakah sistem file Anda kurang disediakan untuk beban kerja Anda.

Untuk meminimalkan durasi penskalaan penyimpanan dan menghindari pengurangan kinerja penulisan, kami sarankan untuk meningkatkan kapasitas throughput sistem file Anda sebelum meningkatkan kapasitas penyimpanan dan kemudian menskalakan kembali kapasitas throughput setelah peningkatan kapasitas penyimpanan selesai. Sebagian besar beban kerja mengalami dampak kinerja minimal selama penskalaan penyimpanan. Namun, sistem file dengan jenis penyimpanan HDD dan beban kerja yang melibatkan sejumlah besar pengguna akhir, I/O tingkat tinggi, atau kumpulan data dengan sejumlah besar file kecil untuk sementara dapat mengalami penurunan kinerja. Untuk informasi selengkapnya, lihat Kapasitas penyimpanan meningkat dan performa sistem file.

Memodifikasi kapasitas throughput selama periode idle

Memperbarui kapasitas throughput mengganggu ketersediaan selama beberapa menit untuk sistem file Single-AZ dan menyebabkan failover dan failback untuk sistem file multi-AZ. Untuk sistem file multi-AZ, jika ada lalu lintas yang sedang berlangsung selama failover dan failback, setiap perubahan data yang dibuat selama waktu ini perlu disinkronkan antara server file. Proses sinkronisasi data dapat memakan waktu hingga beberapa jam untuk beban kerja yang berat dan berat IOPS. Meskipun sistem file Anda akan terus tersedia selama waktu ini, kami merekomendasikan penjadwalan jendela pemeliharaan dan melakukan pembaruan kapasitas throughput selama periode idle ketika ada beban minimal pada sistem file Anda untuk mengurangi durasi sinkronisasi data. Untuk mempelajari informasi lebih lanjut, lihat Mengelola kapasitas throughput.

Memulai Amazon FSx untuk Windows File Server

Berikut ini, Anda dapat mempelajari cara mulai menggunakan FSx untuk Windows File Server. Latihan memulai ini mencakup langkah-langkah berikut.

1. Mendaftar untuk Akun AWS dan membuat pengguna administratif di akun.
2. Buat Direktori Aktif Microsoft AD AWS Terkelola menggunakan AWS Directory Service. Anda akan bergabung dengan sistem file Anda dan menghitung instance ke Active Directory.
3. Buat instans komputasi Amazon Elastic Compute Cloud yang menjalankan Microsoft Windows Server. Anda akan menggunakan contoh ini untuk mengakses sistem file Anda.
4. Buat sistem file Amazon FSx untuk Windows File Server menggunakan FSx konsol Amazon.
5. Petakan sistem file Anda ke EC2 instans Anda
6. Tulis data ke sistem file Anda.
7. Cadangkan sistem file Anda.
8. Bersihkan sumber daya yang Anda buat.

Topik

Menyiapkan Akun AWS

Sebelum Anda menggunakan Amazon FSx untuk pertama kalinya, selesaikan tugas-tugas berikut:

1. Mendaftar untuk Akun AWS
2. Buat pengguna dengan akses administratif

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.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah 1. Menyiapkan Direktori Aktif

Dengan Amazon FSx, Anda dapat mengoperasikan penyimpanan file yang dikelola sepenuhnya untuk beban kerja berbasis Windows. Demikian juga, AWS Directory Service menyediakan direktori

yang dikelola sepenuhnya untuk digunakan dalam penerapan beban kerja Anda. Jika Anda memiliki domain Active Directory perusahaan yang berjalan AWS di virtual private cloud (VPC) menggunakan EC2 instance, Anda dapat mengaktifkan autentikasi berbasis pengguna dan kontrol akses. Anda melakukannya dengan membangun hubungan kepercayaan antara Direktori Aktif Microsoft AWS Terkelola dan domain perusahaan Anda. Untuk otentikasi Windows di Amazon FSx, Anda hanya memerlukan kepercayaan hutan arah satu arah, di mana hutan AWS terkelola mempercayai hutan domain perusahaan.

Domain perusahaan Anda berperan sebagai domain tepercaya, dan domain AWS Directory Service terkelola berperan sebagai domain yang dipercaya. Permintaan autentikasi yang tervalidasi berpindah antar domain hanya dalam satu arah—yang memungkinkan akun di domain perusahaan Anda untuk melakukan autentikasi terhadap sumber daya yang dibagikan di domain terkelola. Dalam hal ini, Amazon hanya FSx berinteraksi dengan domain terkelola. Domain terkelola kemudian diteruskan pada permintaan autentikasi ke domain perusahaan Anda.

> **Note**
>
> Anda juga dapat menggunakan jenis kepercayaan eksternal dengan Amazon FSx untuk domain tepercaya.

Grup keamanan Active Directory Anda harus mengaktifkan akses masuk dari grup keamanan sistem FSx file Amazon.

Untuk membuat Layanan AWS Direktori untuk Microsoft Active Directory

- Jika Anda belum memilikinya, gunakan AWS Directory Service untuk membuat direktori Microsoft Active Directory AWS Terkelola. Untuk informasi selengkapnya, lihat Membuat Direktori Aktif Microsoft AWS Terkelola Anda di Panduan AWS Directory Service Administrasi.

  > **Important**
  >
  > Ingat kata sandi yang Anda tetapkan untuk pengguna Admin Anda; Anda memerlukannya nanti dalam latihan memulai ini. Jika Anda lupa kata sandi, Anda perlu mengulangi langkah-langkah dalam latihan ini dengan AWS Directory Service direktori baru dan pengguna Admin.

- Jika Anda memiliki Direktori Aktif yang ada, buat hubungan kepercayaan antara Direktori Aktif Microsoft AWS Terkelola dan Direktori Aktif yang ada. Untuk informasi lebih lanjut, lihat Kapan

Sebaiknya Menciptakan Hubungan Kepercayaan dalam Panduan Administrasi AWS Directory Service .

Langkah 2: Luncurkan instance Windows di EC2 konsol Amazon

Anda dapat meluncurkan instance Windows menggunakan AWS Management Console seperti yang dijelaskan dalam prosedur berikut. Peluncuran ini dimaksudkan untuk membantu Anda meluncurkan instans pertama dengan cepat, jadi tidak mencakup semua opsi yang memungkinkan. Untuk informasi selengkapnya tentang opsi lanjutan, lihat Meluncurkan sebuah instans.

Untuk meluncurkan sebuah instans

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Dari dasbor konsol, pilih Luncurkan Instans.
3. Halaman Choose an Amazon Machine Image (AMI) menampilkan daftar konfigurasi dasar, yang disebut Amazon Machine Images (AMIs), yang berfungsi sebagai template untuk instans Anda. Pilih AMI untuk Windows Server 2016 Base atau yang lebih baru. Perhatikan bahwa ini AMIs ditandai “Tingkat gratis memenuhi syarat.”
4. Pada halaman Pilih Jenis Instans, Anda dapat memilih konfigurasi perangkat keras instans Anda. Pilih jenis `t2.micro`, yang dipilih secara default. Perhatikan bahwa jenis instans ini memenuhi syarat untuk tingkat gratis.
5. Pilih Tinjau dan Luncurkan untuk memungkinkan wizard menyelesaikan pengaturan konfigurasi lainnya untuk Anda.
6. Pada halaman Tinjau Peluncuran Instans, di bawah Grup Keamanan, sebuah grup keamanan yang wizard buat dan pilihkan untuk Anda muncul. Anda dapat menggunakan grup keamanan ini, atau Anda dapat memilih grup keamanan yang Anda buat saat menyiapkan di awal dengan menggunakan langkah-langkah berikut ini:
   a. Pilih Sunting grup keamanan.
   b. Pada halaman Konfigurasi Grup Keamanan, pastikan bahwa Pilih grup keamanan yang sudah ada dipilih.
   c. Pilih grup keamanan Anda dari daftar grup keamanan yang sudah ada, lalu pilih Tinjau dan Luncurkan.
7. Pada halaman Tinjau Peluncuran Instans, pilih Luncurkan.

8. Saat dimintai pasangan kunci, pilih Pilih pasangan kunci yang sudah ada, kemudian pilih pasangan kunci yang Anda buat saat menyiapkannya.

   Sebagai gantinya, Anda dapat membuat pasangan kunci yang baru. Pilih Buat sebuah pasangan kunci yang baru, masukkan nama untuk pasangan kunci, lalu pilih Unduh Pasangan Kunci. Ini adalah satu-satunya kesempatan bagi Anda untuk menyimpan file kunci privat, jadi pastikan Anda mengunduhnya. Simpan file kunci privat di suatu tempat yang aman. Anda harus menyediakan nama pasangan kunci saat meluncurkan sebuah instans dan kunci privat yang sesuai setiap kali Anda terhubung dengan instans tersebut.

   > **Warning**
   >
   > Jangan pilih pilihan Lanjutkan tanpa pasangan kunci. Jika Anda meluncurkan instans Anda tanpa pasangan kunci, Anda tidak dapat terhubung dengan instans.

   Saat Anda siap, pilih kotak centang bahwa Anda telah mengetahuinya, lalu pilih Luncurkan Instans.

9. Halaman konfirmasi memberi tahu Anda bahwa instans Anda akan diluncurkan. Pilih Lihat Instans untuk menutup halaman konfirmasi dan kembali ke konsol.

10. Pada layar Instans, Anda dapat melihat status peluncuran. Hanya butuh waktu singkat untuk meluncurkan sebuah instans. Saat Anda meluncurkan sebuah instans, status awalnya adalah `pending`. Setelah instans dimulai, statusnya akan berubah menjadi `running` dan instans tersebut menerima sebuah nama DNS publik. (Jika kolom DNS Publik (IPv4) disembunyikan, pilih Tampilkan/Sembunyikan Kolom (ikon berbentuk roda gigi) di sudut kanan atas halaman dan kemudian pilih DNS Publik ().) IPv4

11. Proses ini mungkin memerlukan waktu beberapa menit sampai instans siap, sehingga Anda dapat terhubung dengannya. Periksa apakah instans Anda telah lulus pemeriksaan statusnya; Anda dapat melihat informasi ini di kolom Pemeriksaan Status.

> **Important**
>
> Buatlah sebuah catatan ID grup keamanan yang tercipta ketika Anda meluncurkan instans ini. Anda akan membutuhkannya saat membuat sistem FSx file Amazon Anda.

Setelah instans Anda diluncurkan, Anda dapat terhubung ke instans Anda.

Langkah 3: Connect ke instans Anda

Untuk menyambungkan ke instans Windows, Anda harus mengambil sandi administrator awal dan kemudian menentukan sandi ini saat Anda menyambungkan ke instans Anda menggunakan Desktop Jarak Jauh.

Nama akun administrator tergantung pada bahasa sistem operasi. Misalnya, untuk bahasa Inggris, maka Administrator, untuk bahasa Perancis maka Administrateur, dan untuk bahasa Portugis maka Administrador. Untuk informasi lebih lanjut, lihat Nama Lokal untuk Akun Administrator di Windows dalam Microsoft TechNet Wiki.

Jika Anda telah menggabungkan instans Anda ke suatu domain, Anda dapat ter-connect ke instans Anda menggunakan kredensial domain yang telah Anda tentukan di AWS Directory Service. Pada layar masuk Remote Desktop, jangan gunakan nama komputer lokal dan kata sandi yang dihasilkan. Sebaliknya, gunakan nama pengguna yang memenuhi syarat untuk administrator dan kata sandi untuk akun ini. Contohnya adalah **`corp.example.com\Admin`**.

Lisensi untuk sistem operasi (OS) Windows Server mengizinkan dua koneksi jarak jauh secara simultan untuk tujuan administratif. Lisensi untuk Windows Server sudah termasuk dalam harga instans Windows Anda. Jika Anda membutuhkan lebih dari dua koneksi jarak jauh secara bersamaan, Anda harus membeli lisensi Remote Desktop Services (RDS). Jika Anda mencoba koneksi ketiga, terjadi kesalahan. Untuk informasi selengkapnya, lihat Mengonfigurasi Jumlah Sambungan Jarak Jauh Simultan yang Diizinkan untuk Koneksi.

Untuk menyambungkan ke instans Windows Anda menggunakan RDP client

1. Di EC2 konsol Amazon, pilih instance, lalu pilih Connect.
2. Di kotak dialog Connect ke Instans Anda, pilih Dapatkan Kata Sandi (akan memakan waktu beberapa menit setelah instans diluncurkan sebelum kata sandi tersedia).
3. Pilih Jelajahi dan navigasi ke file kunci privat yang Anda buat saat meluncurkan instans tersebut. Pilih file dan pilih Buka untuk menyalin seluruh isi file ke dalam bidang Isi.
4. Pilih Dekripsi Kata Sandi. Konsol tersebut menampilkan kata sandi administrator default untuk instans dalam kotak dialog Connect ke Instans Anda, yang menggantikan tautan ke Dapatkan Kata Sandi yang ditunjukkan sebelumnya dengan kata sandi yang sebenarnya.
5. Catat kata sandi administrator default, atau salin ke clipboard. Anda memerlukan kata sandi ini untuk terhubung ke instans.

6. Pilih Unduh File Desktop Jarak Jauh. Peramban Anda meminta untuk membuka atau menyimpan file .rdp. Anda dapat memilih opsi mana saja. Setelah selesai, Anda bisa memilih Tutup untuk menutup kotak dialog Connect ke Instans Anda.

   - Jika Anda membuka file .rdp, Anda akan melihat kotak dialog Koneksi Desktop Jarak Jauh.
   - Jika Anda menyimpan file .rdp, arahkan ke direktori unduhan Anda, dan buka file .rdp untuk menampilkan kotak dialog.

7. Anda mungkin mendapatkan peringatan bahwa penerbit koneksi jarak jauh tidak diketahui. Anda dapat terus terhubung ke instans Anda.

8. Saat diminta, masuk ke instans, dengan menggunakan akun administrator untuk sistem operasi dan kata sandi yang Anda catat atau salin sebelumnya. Jika Koneksi Desktop Jarak Jauh telah menyiapkan akun administrator, Anda mungkin harus memilih opsi Gunakan akun lain dan ketik nama pengguna dan kata sandi secara manual.

   > **Note**
   >
   > Terkadang menyalin dan menempelkan konten dapat merusak data. Jika Anda menemukan kesalahan "Kata Sandi Gagal" saat Anda log in masuk, coba ketikkan kata sandi secara manual.

9. Karena sifat dari sertifikat yang ditandatangani sendiri, Anda mungkin mendapatkan peringatan bahwa sertifikat keamanan tidak dapat diautentikasi. Gunakan langkah-langkah berikut untuk memverifikasi identitas komputer jarak jauh, atau cukup pilih Ya atau Lanjutkan untuk melanjutkan jika Anda memercayai sertifikat tersebut.

   a. Jika Anda menggunakan Koneksi Desktop Jarak Jauh dari PC Windows, pilih Tampilkan sertifikat. Jika Anda menggunakan Desktop Jarak Jauh Microsoft di Mac, pilih Tampilkan Sertifikat.

   b. Pilih tab Detail, dan gulir ke bawah ke entri Sidik Jari pada PC Windows, atau entri SHA1Sidik Jari di Mac. Ini adalah pengidentifikasi unik untuk sertifikat keamanan komputer jarak jauh.

   c. Di EC2 konsol Amazon, pilih instance, pilih Tindakan, lalu pilih Dapatkan Log Sistem.

   d. Dalam output log sistem, cari entri berlabel `RDPCERTIFICATE-THUMBPRINT`. Jika nilai ini cocok dengan sidik jari sertifikat, Anda telah memverifikasi identitas komputer jarak jauh.

e. Jika Anda menggunakan Koneksi Desktop Jarak Jauh dari sebuah PC Windows, kembali ke kotak dialog Sertifikat dan pilih OK. Jika Anda menggunakan Desktop Jarak Jauh Microsoft di Mac, kembali ke bagian Verifikasi Sertifikat dan pilih Lanjutkan.

f. [Windows] Pilih Ya pada jendela Koneksi Remote Desktop untuk terhubung ke instans Anda.

Setelah Anda terhubung ke instans Anda, Anda dapat menggabungkan instans Anda ke direktori AWS Directory Service Anda.

Langkah 4: Bergabunglah dengan instans Anda ke AWS Directory Service direktori Anda

Prosedur berikut menunjukkan kepada Anda cara menggabungkan instans Amazon EC2 Windows yang ada secara manual ke AWS Directory Service direktori Anda.

Untuk menggabungkan instance Windows ke AWS Directory Service direktori Anda

1. Connect ke instans menggunakan klien Remote Desktop Protocol.
2. Buka kotak dialog IPv4 TCP/properties pada instance.

   a. Buka Koneksi Jaringan.

   > **Tip**
   >
   > Anda dapat membuka Koneksi Jaringan secara langsung dengan menjalankan berikut ini dari command prompt pada instans.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Buka menu konteks (klik kanan) untuk koneksi jaringan aktif mana pun dan pilih Properti.

   c. Dalam kotak dialog properti koneksi, buka (klik dua kali) Protokol Internet Versi 4.
3. (Opsional) Pilih Gunakan alamat server DNS berikut, ubah server DNS pilihan dan alamat server DNS alternatif ke alamat IP server DNS yang AWS Directory Service disediakan, dan pilih OK.
4. Buka kotak dialog Properti sistem untuk instans, pilih tab Nama Komputer, dan pilih Ubah.

> **Tip**
>
> Anda dapat membuka kotak dialog Properti Sistem secara langsung dengan menjalankan yang berikut ini dari command prompt pada instans.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Di kotak Anggota, pilih Domain, masukkan nama AWS Directory Service direktori Anda yang sepenuhnya memenuhi syarat, dan pilih OK.
6. Saat diminta untuk nama dan kata sandi untuk administrator domain, masukkan nama pengguna dan kata sandi akun Admin.

> **Note**
>
> Anda dapat memasukkan nama domain atau nama yang sepenuhnya memenuhi syarat, diikuti dengan garis miring terbalik (\), dan kemudian nama pengguna, dalam hal ini, Admin. NetBios Misalnya, corp.example.com\ Admin atau corp\ Admin.

7. Setelah Anda menerima pesan yang menyambut Anda ke domain, mulai ulang instans agar perubahan berlaku.
8. Sambungkan kembali ke instans Anda melalui RDP, dan masuk ke instance menggunakan nama pengguna dan kata sandi untuk pengguna Admin AWS Directory Service direktori Anda.

Sekarang instans Anda telah bergabung ke domain, Anda siap untuk membuat sistem FSx file Amazon Anda.

Langkah 5. Buat sistem file Anda

Untuk membuat sistem file Anda (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Pada dasbor, pilih Buat sistem file untuk memulai wizard pembuatan sistem file.
3. Pada halaman Pilih jenis sistem file, pilih FSx untuk Windows File Server, lalu pilih Berikutnya. Halaman Buat sistem file muncul.
4. Untuk metode Creation pilih Standard create.

Rincian sistem file

1. Di bagian Detail sistem file, berikan nama untuk sistem file Anda. Lebih mudah untuk menemukan dan mengelola sistem file Anda ketika Anda menamainya. Anda dapat menggunakan maksimal 256 huruf Unicode, spasi, dan angka, serta karakter khusus + - = . _ : /
2. Untuk Jenis Deployment Pilih Multi-AZ atau Single-AZ.

   - Pilih Multi-AZ untuk men-deploy sistem file yang toleran pada ketidaktersediaan Availability Zone. Opsi ini men-support penyimpanan SSD dan HDD.
   - Pilih Single-AZ untuk men-deploy sistem file yang digunakan di Availability Zone tunggal. Single-AZ 2 adalah generasi terbaru dari sistem file Availability Zone tunggal, dan Single-AZ 2 men-support penyimpanan SSD dan HDD.

   Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan: Sistem file Single-AZ dan Multi-AZ.
3. Untuk Jenis penyimpanan, Anda dapat memilih SSD atau HDD.

   FSx untuk Windows File Server menawarkan jenis penyimpanan solid state drive (SSD) dan hard disk drive (HDD). Penyimpanan SSD dirancang untuk performa tertinggi dan beban kerja yang paling peka latensi, termasuk basis data, beban kerja pemrosesan media, dan aplikasi analitik data. Penyimpanan HDD dirancang untuk spektrum beban kerja yang luas, termasuk direktori beranda, berbagi file pengguna dan departemen, dan sistem manajemen konten. Untuk informasi selengkapnya, lihat Tentang jenis penyimpanan.
4. Untuk IOPS SSD yang Disediakan, Anda dapat memilih mode Otomatis atau yang disediakan pengguna.

   Jika Anda memilih mode Otomatis, FSx untuk Windows File Server secara otomatis menskalakan IOPS SSD Anda untuk mempertahankan 3 IOPS SSD per GiB kapasitas penyimpanan. Jika Anda memilih mode yang disediakan pengguna, masukkan bilangan bulat apa pun dalam kisaran 96—400.000. Penskalaan SSD IOPS di atas 80.000 tersedia di AS Timur (Virginia N.), AS Barat (Oregon), AS Timur (Ohio), Eropa (Irlandia), Asia Pasifik (Tokyo), dan Asia Pasifik (Singapura). Untuk informasi selengkapnya, lihat Mengelola SSD IOPS.
5. Untuk Kapasitas penyimpanan, masukkan kapasitas dari sistem file Anda, dalam GiB. Jika Anda menggunakan penyimpanan SSD, masukkan bilangan bulat berapa pun dalam kisaran 32–65,536. Jika Anda menggunakan penyimpanan HDD, masukkan bilangan bulat berapa pun dalam kisaran 2,000–65,536. Anda dapat meningkatkan jumlah kapasitas penyimpanan sesuai

kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan.

6. Pertahankan Kapasitas throughput pada pengaturan default-nya. Kapasitas throughput adalah kecepatan berkelanjutan di mana server file yang menyimpan sistem file Anda dapat melayani data. Pengaturan Kapasitas throughput yang disarankan didasarkan pada jumlah kapasitas penyimpanan yang Anda pilih. Jika Anda membutuhkan lebih dari kapasitas throughput yang disarankan, pilih Tentukan kapasitas throughput, dan kemudian pilih nilai. Untuk informasi selengkapnya, lihat FSx untuk kinerja Windows File Server.

   > **Note**
   >
   > Jika Anda akan mengaktifkan audit akses file, Anda harus memilih kapasitas throughput 32 MBps atau lebih besar. Untuk informasi selengkapnya, lihat Mencatat akses pengguna akhir dengan audit akses file.

   Anda dapat mengubah kapasitas throughput sesuai kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Jaringan & keamanan

1. Di bagian Jaringan & keamanan, pilih Amazon VPC yang ingin Anda associate-kan dengan sistem file Anda. Untuk latihan memulai ini, pilih VPC Amazon yang sama yang Anda pilih untuk AWS Directory Service direktori dan instans Amazon EC2 Anda.
2. Untuk Grup Keamanan VPC, grup keamanan default untuk Amazon VPC default Anda sudah ditambahkan ke sistem file Anda di konsol. Jika Anda tidak menggunakan grup keamanan default, pastikan grup keamanan yang Anda pilih Wilayah AWS sama dengan sistem file Anda. Untuk memastikan bahwa Anda dapat menghubungkan EC2 instance dengan sistem file Anda, Anda perlu menambahkan aturan berikut ke grup keamanan yang Anda pilih:

   a. Tambahkan aturan jalur masuk dan jalur keluar berikut ini untuk mengizinkan port berikut.

Aturan	Port
UDP	53, 88, 123, 389, 464

Aturan	Port
TCP	53, 88, 135, 389, 445, 464, 636, 3268, 3269, 5985, 9389, 49152-65535

Tambahkan dari dan ke alamat IP atau grup keamanan IDs yang terkait dengan instance komputasi klien yang ingin Anda akses ke sistem file Anda.

b. Tambahkan aturan jalur keluar untuk mengizinkan semua lalu lintas ke Direktori Aktif tempat Anda menggabungkan sistem file Anda. Untuk melakukannya, lakukan salah satu hal berikut:

- Izinkan lalu lintas jalur keluar ke ID grup keamanan yang ter-associate dengan direktori AD yang dikelola AWS .
- Izinkan lalu lintas jalur keluar menuju alamat IP yang ter-associate dengan pengendali domain Direktori Aktif yang dikelola sendiri.

> **Note**
>
> Dalam beberapa kasus, Anda mungkin telah mengubah aturan grup AWS Managed Microsoft AD keamanan Anda dari pengaturan default. Jika demikian, pastikan grup keamanan ini memiliki aturan masuk yang diperlukan untuk mengizinkan lalu lintas dari sistem FSx file Amazon Anda. Untuk informasi selengkapnya tentang aturan jalur masuk yang diperlukan, lihat Prasyarat AWS Managed Microsoft AD dalam Panduan Administrasi AWS Directory Service .

Untuk informasi selengkapnya, lihat Kontrol akses sistem file dengan Amazon VPC.

3. Sistem file multi-AZ memiliki server file primer dan siaga, masing-masing di Availability Zone dan subnet.Jika Anda membuat sistem file multi-AZ (lihat langkah 5), pilih nilai subnet Preferred untuk server file utama dan nilai subnet Siaga untuk server file siaga.

   Jika Anda membuat sistem file Single-AZ, pilih Subnet untuk sistem file Anda.

Otentikasi Windows

- Untuk autentikasi Windows, Anda memiliki opsi berikut:

  Pilih Direktori Aktif Microsoft AWS Terkelola jika Anda ingin menggabungkan sistem file Anda ke domain Microsoft Active Directory yang dikelola oleh AWS, lalu pilih AWS Directory Service direktori Anda dari daftar. Untuk informasi selengkapnya, lihat Bekerja dengan Microsoft Active Directory.

  Pilih Microsoft Active Directory yang dikelola sendiri jika Anda ingin menggabungkan sistem file Anda ke domain Microsoft Active Directory yang dikelola sendiri, dan berikan detail berikut untuk Active Directory Anda. Untuk mengetahui informasi selengkapnya, lihat Menggunakan Microsoft Active Directory yang dikelola sendiri.

  - Nama domain yang memenuhi syarat dari Direktori Aktif Anda.

    > **Important**
    >
    > Untuk sistem file Single-AZ 2 dan semua sistem file Multi-AZ, nama domain Direktori Aktif tidak boleh melebihi 47 karakter. Batasan ini berlaku untuk nama domain Active Directory AWS Directory Service dan yang dikelola sendiri.
    > Amazon FSx memerlukan koneksi langsung untuk lalu lintas internal ke alamat IP DNS Anda. Koneksi melalui gateway internet tidak didukung. Sebagai gantinya, gunakan AWS Virtual Private Network, mengintip VPC, AWS Direct Connect, atau asosiasi. AWS Transit Gateway

  - Alamat IP server DNS — IPv4 alamat server DNS untuk domain Anda

    > **Note**
    >
    > Server DNS Anda harus memiliki EDNS (ekstensi mekanisme untuk DNS) yang aktif. Jika EDNS dinonaktifkan, sistem file Anda mungkin gagal dibuat.

  - Nama pengguna akun layanan—nama pengguna akun layanan di Direktori Aktif yang sudah ada milik Anda . Jangan masukkan sebuah prefiks atau sufiks domain.
  - Kata sandi akun layanan—kata sandi untuk akun layanan.
  - (Opsional) Unit Organisasi (OU)—nama jalur yang berbeda dari unit organisasi tempat Anda menggabungkan sistem file Anda.

- (Opsional) Grup administrator sistem file terdelegasi— nama grup di Direktori Aktif Anda yang dapat mengelola sistem file Anda. Grup default adalah 'Admin domain'. Untuk informasi selengkapnya, lihat Akun FSx layanan Amazon.

Enkripsi, Audit, dan Akses (alias DNS)

1. Untuk Enkripsi, pilih kunci AWS KMS key Enkripsi yang digunakan untuk mengenkripsi data pada sistem file Anda saat istirahat. Anda dapat memilih aws/fsx default (default) yang dikelola oleh AWS KMS, kunci yang ada, atau kunci yang dikelola pelanggan dengan menentukan ARN untuk kunci tersebut. Untuk informasi selengkapnya, lihat Enkripsi data saat tidak digunakan.
2. Untuk Audit - opsional, audit akses file dinonaktifkan secara default. Untuk informasi tentang mengaktifkan dan mengkonfigurasi audit akses file, lihat Mencatat akses pengguna akhir dengan audit akses file.
3. Untuk Akses - opsional, masukkan alias DNS yang ingin Anda associate-kan dengan sistem file. Setiap nama alias harus diformat sebagai sebuah nama domain yang sepenuhnya memenuhi syarat (FQDN). Untuk informasi selengkapnya, lihat Mengelola alias DNS.

Backup dan pemeliharaan

Untuk informasi selengkapnya tentang pencadangan harian otomatis dan pengaturan di bagian ini, lihat. Melindungi data Anda dengan backup

1. Pencadangan otomatis harian diaktifkan secara default. Anda dapat menonaktifkan pengaturan ini jika Anda tidak FSx ingin Amazon mengambil cadangan sistem file Anda secara otomatis setiap hari.
2. Jika backup otomatis diaktifkan, mereka terjadi dalam periode waktu yang dikenal sebagai jendela cadangan. Anda dapat menggunakan jendela default, atau memilih waktu mulai jendela pencadangan otomatis yang terbaik untuk alur kerja Anda.
3. Untuk periode retensi cadangan otomatis, Anda dapat menggunakan pengaturan default 30 hari, atau menetapkan nilai antara 1 dan 90 hari yang Amazon FSx akan menyimpan cadangan harian otomatis sistem file Anda. Pengaturan ini tidak berlaku untuk pencadangan yang dimulai pengguna, atau cadangan yang diambil oleh. AWS Backup
4. Untuk Tag - opsional, masukkan kunci dan nilai untuk menambahkan tag ke sistem file Anda. Tag adalah pasangan nilai-kunci yang peka huruf besar-kecil yang membantu Anda mengelola, mem-filter, dan mencari sistem file Anda. Untuk informasi selengkapnya, lihat Menandai sumber daya Amazon FSx Anda.

Pilih Berikutnya.

Tinjau konfigurasi Anda dan buat

1. Tinjau konfigurasi sistem file yang ditampilkan pada halaman Buat sistem file. Untuk referensi Anda, Anda dapat melihat pengaturan sistem file mana yang dapat dan tidak dapat Anda ubah setelah sistem file dibuat. Pilih Buat sistem file.
2. Setelah Amazon FSx membuat sistem file, pilih ID sistem file dari daftar di dasbor Sistem File untuk melihat detailnya. Pilih Lampirkan, dan catat nama DNS untuk sistem file Anda tab Jaringan & keamanan. Anda akan membutuhkannya dalam prosedur berikut untuk memetakan bagian ke sebuah EC2 instance.

Langkah 6. Memetakan berbagi file Anda ke EC2 instance yang menjalankan Windows Server

Sekarang Anda dapat memasang sistem FSx file Amazon ke EC2 instans Amazon berbasis Microsoft Windows yang bergabung dengan direktori Anda AWS Directory Service . Nama Berbagi file Anda tidak sama dengan nama sistem file Anda.

Untuk memetakan file share pada instance Amazon EC2 Windows menggunakan GUI

1. Sebelum Anda dapat me-mount file share pada instance Windows, Anda harus meluncurkan EC2 instance dan menggabungkannya dengan sistem file Anda AWS Directory Service for Microsoft Active Directory yang telah bergabung. Untuk melakukan tindakan ini, pilih salah satu prosedur berikut dari Panduan AWS Directory Service Administrasi:
   - Bergabunglah dengan instans Windows EC2 dengan mulus
   - Bergabunglah dengan instance Windows secara manual
2. Terhubung ke instans Anda. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
3. Saat tersambung, buka File Explorer.
4. Dari panel navigasi, buka menu konteks (klik kanan) untuk Jaringan dan pilih Drive Jaringan Peta.
5. Pilih drive letter pilihan anda untuk Drive.

6. Anda dapat memetakan sistem file Anda menggunakan nama DNS default yang ditetapkan oleh Amazon FSx, atau menggunakan alias DNS yang Anda pilih. Prosedur ini menjelaskan pemetaan Berbagi file menggunakan nama DNS default. Jika Anda ingin memetakan Berbagi file menggunakan alias DNS, lihat Mengakses data menggunakan alias DNS.

   Untuk Folder, masukkan nama DNS sistem file dan nama Berbagi. FSx Bagikan Amazon default disebut`\share`. Anda dapat menemukan nama DNS di FSx konsol Amazon https://console.aws.amazon.com/fsx/, Windows File Server > Jaringan & Keamanan bagian, atau dalam respons CreateFileSystem atau perintah DescribeFileSystems API.

   - Untuk sistem file Single-AZ yang bergabung dengan Direktori Aktif Microsoft AWS Terkelola, nama DNS terlihat seperti berikut ini.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - Untuk sistem file Single-AZ yang tergabung ke Direktori Aktif yang dikelola sendiri, dan sistem file Multi-AZ, nama DNS terlihat seperti berikut ini.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   Misalnya, masukkan `\\fs-0123456789abcdef0.ad-domain.com\share`.
7. Tentukan apakah Berbagi file harus Menyambung kembali saat masuk, lalu pilih Selesai.

Langkah 7. Menulis data ke berbagi file Anda

Sekarang setelah Anda memetakan Berbagi file Anda ke instans Anda, Anda dapat menggunakan akses berbagi file seperti direktori lain di lingkungan Windows Anda.

Untuk menulis data ke Berbagi file Anda

1. Buka editor teks Notepad.
2. Tulis beberapa konten di editor teks. Misalnya: *`Hello, World!`*
3. Simpan file tersebut ke drive letter berbagi file Anda.
4. Menggunakan File Explorer, arahkan ke Berbagi file Anda dan temukan file teks yang baru saja Anda simpan.

Langkah 8. Cadangkan sistem file Anda

Sekarang setelah Anda memiliki kesempatan untuk menggunakan sistem FSx file Amazon dan berbagi filenya, Anda dapat mencadangkannya. Secara default, backup harian dibuat secara otomatis selama jendela backup 30 menit dari sistem file Anda. Namun Anda dapat membuat backup yang dikerjakan pengguna kapan saja. Backup memiliki biaya tambahan yang ter-asosiasi dengannya. Untuk informasi lebih lanjut tentang harga backup, lihat Penetapan Harga.

Untuk membuat backup dari sistem file Anda dari konsol

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Dari dasbor konsol, pilih nama sistem file yang Anda buat untuk latihan ini.
3. Dari tab gambaran umum untuk sistem file Anda, pilih Buat backup.
4. Di kotak dialog Buat cadangan yang terbuka, berikan nama untuk backup Anda. Nama ini dapat berisikan maksimal 256 huruf Unicode sudah termasuk spasi, angka, dan karakter khusus berikut: + - = . _ : /
5. Pilih Buat backup.
6. Untuk melihat semua backup dalam daftar, agar Anda dapat memulihkan sistem file atau menghapus backup, pilih Backup.

Saat Anda membuat backup yang baru, statusnya diatur menjadi MEMBUAT Saat sedang dibuat. Hal ini dapat menghabiskan waktu beberapa menit. Ketika backup tersedia untuk digunakan, statusnya berubah menjadi TERSEDIA.

Langkah 9. Pembersihan sumber daya

Setelah Anda menyelesaikan latihan ini, Anda harus mengikuti langkah-langkah ini untuk membersihkan sumber daya Anda dan melindungi AWS akun Anda.

Untuk membersihkan sumber daya

1. Di EC2 konsol Amazon, hentikan instans Anda. Untuk informasi selengkapnya, lihat Menghentikan Instans Anda di Panduan EC2 Pengguna Amazon.
2. Di FSx konsol Amazon, hapus sistem file Anda. Semua backup otomatis dihapus secara otomatis. Walau bagaimanapun, anda masih perlu menghapus backup yang dibuat secara manual. Langkah-langkah berikut menjelaskan proses ini:

a. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.

b. Dari dasbor konsol, pilih nama sistem file yang Anda buat untuk latihan ini.

c. Untuk Tindakan, pilih Hapus sistem file.

d. Di kotak dialog Hapus sistem file yang terbuka, tentukan apakah Anda ingin membuat backup akhir. Jika Anda melakukannya, beri nama untuk backup akhir. Backup yang dibuat secara otomatis juga akan dihapus.

> **Important**
>
> Sistem file yang baru dapat dibuat dari backup. Kami merekomendasikan Anda membuat backup akhir sebagai praktik terbaik. Jika Anda merasa tidak membutuhkannya setelah jangka waktu tertentu, Anda dapat menghapus backup akhir dan backup lainnya yang dibuat secara manual.

e. Masukkan ID sistem file yang ingin Anda hapus di kotak ID sistem file.

f. Pilih Hapus sistem file.

g. Sistem file sekarang sedang dihapus, dan statusnya di dasbor berubah menjadi MENGHAPUS. Ketika sistem file telah dihapus, maka tidak akan lagi muncul di dasbor.

h. Sekarang Anda dapat menghapus backup apa pun yang dibuat secara manual untuk sistem file Anda. Dari navigasi sisi kiri, pilih Backup.

i. Dari dasbor, pilih backup apa pun yang memiliki ID sistem file yang sama dengan sistem file yang Anda hapus, dan pilih Hapus backup.

j. Kotak dialog Hapus backup terbuka. Biarkan kotak centang dicentang untuk ID backup yang Anda pilih, dan pilih Hapus backup.

Sistem FSx file Amazon Anda dan cadangan otomatis terkait sekarang dihapus.

3. Untuk menghapus AWS Directory Service direktori yang Anda buat untuk latihan ini, lihat Menghapus direktori Anda di Panduan AWS Directory Service Administrasi.

Mengakses data Anda

Anda dapat mengakses sistem FSx file Amazon menggunakan berbagai klien dan metode yang didukung baik dari lingkungan AWS Cloud maupun lokal.

Topik

Klien yang didukung

FSx untuk Windows File Server mendukung protokol Server Message Block (SMB) versi 2.0 hingga 3.1.1, memberi Anda fleksibilitas untuk terhubung ke sistem file Anda menggunakan berbagai macam instans komputasi dan sistem operasi.

Instans AWS komputasi berikut didukung untuk digunakan dengan Amazon: FSx

- Instans Amazon Elastic Compute Cloud (Amazon EC2), termasuk instans Microsoft Windows, Mac, Amazon Linux, dan Amazon Linux 2. Untuk informasi selengkapnya, lihat Memetakan berbagi file.
- Kontainer Amazon Elastic Container Service (Amazon ECS). Untuk informasi selengkapnya, lihat FSx volume Server File Windows di Panduan Pengembang Layanan Amazon Elastic Container.
- WorkSpaces contoh - Untuk mempelajari lebih lanjut, lihat posting AWS blog Menggunakan FSx untuk Windows File Server dengan Amazon WorkSpaces.
- Instans Amazon AppStream 2.0 - Untuk mempelajari lebih lanjut, lihat posting AWS blog Menggunakan Amazon FSx dengan Amazon AppStream 2.0.
- VMs berjalan di VMware Cloud di AWS lingkungan — Untuk mempelajari lebih lanjut, lihat posting AWS blog Menyimpan dan FSx Berbagi File dengan Windows File Server di VMware Cloud di AWS Lingkungan.

Sistem operasi berikut didukung untuk digunakan dengan Amazon FSx:

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, dan Windows Server 2022.
- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (termasuk pengalaman desktop Windows 7 dan Windows 10 WorkSpaces), dan Windows 11.
- Linux, menggunakan alat `cifs-utils`.
- macOS

Mengakses data dari dalam AWS Cloud

Setiap sistem FSx file Amazon dikaitkan dengan Virtual Private Cloud (VPC). Anda dapat mengakses sistem file Windows File Server Anda FSx dari mana saja di VPC sistem file, terlepas dari Availability Zone. Anda juga dapat mengakses sistem file Anda dari VPCs yang berbeda Akun AWS atau Wilayah AWS dari sistem file. Selain persyaratan yang dijelaskan di bagian berikut FSx untuk mengakses sumber daya Windows File Server, Anda juga perlu memastikan bahwa grup keamanan VPC sistem file Anda dikonfigurasi sehingga lalu lintas data dan manajemen dapat mengalir antara sistem file dan klien Anda. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan dengan port yang diperlukan, lihatKontrol akses sistem file dengan Amazon VPC.

Anda dapat mengakses FSx sistem file Windows File Server dari klien yang didukung yang berada di VPC yang sama dengan sistem file Anda.

Tabel berikut menggambarkan lingkungan dari mana Amazon FSx mendukung akses dari klien di setiap lingkungan yang didukung, tergantung pada kapan sistem file dibuat.

Klien yang berlokasi di...	Akses ke sistem file yang dibuat sebelum tanggal 22 Februari 2019	Akses ke sistem file yang dibuat sebelum tanggal 17 Desember 2020	Akses ke sistem file yang dibuat setelah tanggal 17 Desember 2020
Subnet tempat sistem file dibuat	✓	✓	✓
Blok CIDR primer dari VPC	✓	✓	✓

Klien yang berlokasi di...	Akses ke sistem file yang dibuat sebelum tanggal 22 Februari 2019	Akses ke sistem file yang dibuat sebelum tanggal 17 Desember 2020	Akses ke sistem file yang dibuat setelah tanggal 17 Desember 2020
tempat sistem file dibuat			
Sekunder CIDRs dari VPC di mana sistem file dibuat		Klien dengan alamat IP di rentang alamat IP privat RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Klien dengan alamat IP di luar rentang blok CIDR berikut: 198.19.0.0/16
Jaringan lain CIDRs atau peered			

> **Note**
>
> Dalam beberapa kasus, Anda mungkin ingin mengakses sistem file yang dibuat sebelum 17 Desember 2020 dari on-premise menggunakan rentang alamat IP non-privat. Untuk melakukan ini, buat sistem file baru dari backup sistem file. Untuk informasi selengkapnya, lihat Melindungi data Anda dengan backup.

Mengakses data dari VPC Akun AWS yang berbeda,, atau Wilayah AWS

Anda dapat mengakses sistem file Windows File Server Anda FSx dari klien pendukung yang terletak di VPC yang berbeda, Akun AWS, atau Wilayah AWS dari apa yang terkait dengan sistem file Anda menggunakan gateway peering atau transit VPC. Saat Anda menggunakan koneksi peering VPC atau gateway transit untuk terhubung VPCs, instance komputasi yang ada di satu VPC dapat mengakses sistem file FSx Amazon yang ada di VPC lain. Akses ini dimungkinkan bahkan jika VPCs milik yang berbeda Akun AWS, dan bahkan jika VPCs tinggal di berbeda Wilayah AWS.

Koneksi peering VPC adalah koneksi jaringan antara dua VPCs yang dapat Anda gunakan untuk merutekan lalu lintas di antara mereka menggunakan alamat pribadi IPv4 atau IP versi 6 ()IPv6. Anda dapat menggunakan VPC peering untuk terhubung VPCs dalam AWS Wilayah yang sama atau antar Wilayah. AWS Untuk informasi selengkapnya tentang peering VPC, lihat Apa yang dimaksud dengan peering VPC? dalam Panduan Peering Amazon VPC.

Gateway transit adalah hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya tentang menggunakan VPC transit gateway, lihat Memulai dengan Transit Gateway dalam Transit Gateway Amazon VPC.

Setelah Anda menyiapkan koneksi peering VPC atau transit gateway, Anda dapat mengakses sistem file Anda menggunakan nama DNS-nya. Cara melakukannya sama seperti saat Anda melakukannya dari instans komputasi dalam VPC yan dikaitkan.

Mengakses data dari lokal

FSx untuk Windows File Server mendukung penggunaan AWS Direct Connect atau AWS VPN untuk mengakses sistem file Anda dari instans komputasi lokal Anda. Dengan dukungan untuk AWS Direct Connect, FSx untuk Windows File Server memungkinkan Anda mengakses sistem file Anda melalui koneksi jaringan khusus dari lingkungan lokal Anda. Dengan dukungan untuk AWS VPN, FSx untuk Windows File Server memungkinkan Anda mengakses sistem file dari perangkat lokal Anda melalui terowongan yang aman dan pribadi.

Setelah menghubungkan lingkungan lokal ke VPC yang terkait dengan sistem file FSx Amazon, Anda dapat mengakses sistem file menggunakan nama DNS atau alias DNS. Cara melakukannya sama seperti saat Anda melakukannya dari instans komputasi dalam VPC. Untuk informasi selengkapnya tentang AWS Direct Connect, lihat Panduan Pengguna AWS Direct Connect. Untuk informasi lebih lanjut tentang pengaturan koneksi AWS VPN , lihat Koneksi VPN dalam Panduan Pengguna Amazon VPC.

> **Note**
>
> Dalam beberapa kasus, Anda mungkin ingin mengakses sistem file yang dibuat sebelum 17 Desember 2020 dari on-premise menggunakan rentang alamat IP non-privat. Untuk melakukan ini, buat sistem file baru dari backup sistem file. Untuk informasi selengkapnya, lihat Melindungi data Anda dengan backup.

FSx untuk Windows File Server juga mendukung penggunaan Amazon FSx File Gateway untuk memberikan latensi rendah, akses mulus ke in-cloud FSx Anda untuk berbagi file Windows File Server dari instans komputasi lokal Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon FSx File Gateway.

> **Note**
>
> 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.

Mengakses data menggunakan nama DNS default

FSx untuk Windows File Server menyediakan nama Domain Name System (DNS) untuk setiap sistem file. Anda FSx mengakses sistem file Windows File Server Anda dengan memetakan huruf drive pada instance komputasi Anda ke FSx file share Amazon Anda menggunakan nama DNS ini. Untuk mempelajari selengkapnya, lihat Mengakses data menggunakan berbagi file.

> **Important**
>
> Amazon FSx hanya mendaftarkan catatan DNS untuk sistem file jika Anda menggunakan Microsoft DNS sebagai DNS default. Jika Anda menggunakan DNS pihak ketiga, Anda harus mengatur entri DNS secara manual untuk sistem file Amazon FSx Anda. Untuk informasi lebih lanjut tentang cara memilih alamat IP yang benar untuk digunakan untuk sistem file, lihat Mendapatkan alamat IP sistem file yang benar untuk digunakan untuk entri DNS manual.

Untuk mencari nama DNS:

- Di FSx konsol Amazon, pilih Sistem file, lalu pilih Detail. Lihat nama DNS di bagian Jaringan & Keamanan.
- Atau, lihat dalam respon CreateFileSystem atau perintah API DescribeFileSystems.

Untuk semua sistem file Single-AZ yang bergabung dengan Direktori Aktif Microsoft AWS Terkelola, nama DNS memiliki format berikut: `fs-0123456789abcdef0.`*`ad-dns-domain-name`*

Untuk semua sistem file Single-AZ yang bergabung dengan Active Directory yang dikelola sendiri, dan sistem file Multi-AZ apa pun, nama DNS memiliki format berikut: `amznfsxaa11bb22.`*`ad-domain`*`.com`

Menggunakan otentikasi Kerberos dengan nama DNS

Kami menyarankan Anda menggunakan otentikasi dan enkripsi berbasis Kerberos dalam perjalanan dengan Amazon. FSx Kerberos menyediakan autentikasi paling aman untuk klien yang mengakses sistem file Anda. Untuk mengaktifkan otentikasi berbasis Kerberos dan enkripsi data dalam perjalanan untuk sesi SMB Anda, gunakan nama DNS sistem file yang disediakan oleh FSx Amazon untuk mengakses sistem file Anda.

Jika Anda memiliki kepercayaan eksternal yang dikonfigurasi antara Direktori Aktif Microsoft AWS Terkelola dan Direktori Aktif lokal, untuk menggunakan autentikasi Amazon FSx Remote PowerShell dengan Kerberos, Anda harus mengonfigurasi kebijakan grup lokal pada klien untuk urutan pencarian hutan. Untuk informasi selengkapnya, lihat Konfigurasi Urutan Pencarian Forest Kerberos (KFSO) dalam dokumentasi Microsoft.

Support untuk ruang nama Distributed File System (DFS)

FSx untuk Windows File Server mendukung penggunaan Microsoft DFS Namespaces. Gunakan Ruang Nama DFS untuk mengatur berbagi file yang terletak di beberapa sistem file ke dalam satu struktur folder umum (namespace) yang Anda gunakan untuk mengakses seluruh kumpulan data file. Anda dapat menggunakan nama di Namespace DFS Anda untuk mengakses sistem FSx file Amazon Anda dengan mengonfigurasi target tautannya menjadi nama DNS sistem file. Untuk informasi selengkapnya, lihat Kelompokkan beberapa FSx untuk sistem file Windows File Server dengan Ruang Nama DFS.

Mengakses data menggunakan alias DNS

FSx untuk Windows File Server menyediakan nama DNS untuk setiap sistem file yang dapat Anda gunakan untuk mengakses berbagi file Anda. Anda juga dapat mengakses berbagi file Anda menggunakan nama DNS selain nama DNS default dengan mendaftarkan alias DNS untuk sistem file Windows File FSx Server Anda.

Dengan menggunakan alias DNS, Anda dapat memindahkan data berbagi file Windows ke FSx Windows File Server dan terus menggunakan nama DNS yang ada untuk mengakses data di

Amazon. FSx Alias DNS juga memungkinkan Anda untuk menggunakan nama yang berarti yang membuatnya lebih mudah untuk mengelola alat dan aplikasi untuk terhubung ke sistem file Amazon FSx Anda. Anda dapat mengasosiasikan hingga 50 alias DNS dengan sistem file pada satu waktu. Untuk informasi selengkapnya tentang mengaitkan dan memisahkan alias DNS dengan sistem file Windows File Server FSx untuk Windows, lihat. Mengelola alias DNS

Untuk mengonfigurasi akses ke sistem file Windows File Server Anda FSx menggunakan alias DNS, Anda harus melakukan langkah-langkah berikut:

1. Kaitkan alias DNS dengan sistem file Anda.
2. Buat catatan DNS CNAME untuk sistem file dan alias DNS yang terkait dengannya.

Untuk informasi selengkapnya tentang penggunaan alias DNS FSx untuk sistem file Windows File Server, lihat. Mengelola alias DNS

Menggunakan otentikasi dan enkripsi Kerberos dengan alias DNS

Kami menyarankan Anda menggunakan otentikasi dan enkripsi berbasis Kerberos dalam perjalanan dengan Amazon. FSx Kerberos menyediakan autentikasi paling aman untuk klien yang mengakses sistem file Anda. Untuk mengaktifkan otentikasi Kerberos untuk klien yang mengakses Amazon FSx menggunakan alias DNS, Anda harus menambahkan nama utama layanan (SPNs) yang sesuai dengan alias DNS pada objek komputer Active Directory sistem file FSx Amazon Anda.

Untuk mengatur otentikasi dan enkripsi Kerberos saat mengakses sistem file Anda menggunakan alias DNS, lihat. Konfigurasikan nama utama layanan (SPNs) untuk Kerberos

Anda dapat secara opsional menegakkan klien yang mengakses sistem file menggunakan alias DNS untuk menggunakan otentikasi dan enkripsi Kerberos dengan menyetel Objek Kebijakan Grup berikut () di Direktori Aktif Anda: GPOs

- Membatasi NTLM: Lalu lintas NTLM keluar menuju server jarak jauh - Gunakan pengaturan kebijakan ini untuk menolak atau meng-audit lalu lintas NTLM keluar dari sebuah komputer ke server jarak jauh yang menjalankan sistem operasi Windows.
- Membatasi NTLM: Menambahkan pengecualian server jarak jauh untuk autentikasi NTLM - Gunakan pengaturan kebijakan ini untuk membuat daftar pengecualian server jarak jauh yang padanya perangkat klien diperbolehkan untuk menggunakan autentikasi NTLM jika pengaturan kebijakan Keamanan jaringan: Membatasi NTLM: Lalu lintas NTLM keluar menuju server jarak jauh dikonfigurasi.

Untuk menerapkan otentikasi dan enkripsi Kerberos saat mengakses sistem file Anda menggunakan alias DNS, lihat. Menegakkan otentikasi Kerberos menggunakan Objek Kebijakan Grup () GPOs

Untuk informasi selengkapnya tentang mengkonfigurasi sistem file Anda untuk menggunakan alias DNS, lihat prosedur berikut:

- Kaitkan alias DNS dengan sistem file Anda
- Konfigurasikan nama utama layanan (SPNs) untuk Kerberos
- Memperbarui atau membuat catatan DNS CNAME
- Menegakkan otentikasi Kerberos menggunakan Objek Kebijakan Grup () GPOs

Kaitkan alias DNS dengan sistem file Anda

Anda dapat mengaitkan alias DNS dengan sistem file Windows File Server yang ada FSx , saat Anda membuat sistem file baru, dan saat Anda membuat sistem file baru dari cadangan menggunakan FSx konsol Amazon, CLI, dan API. Jika Anda membuat alias dengan nama domain yang berbeda, masukkan nama lengkap, termasuk domain induk, untuk mengaitkan alias.

Prosedur ini menjelaskan cara mengaitkan alias DNS saat membuat sistem file baru menggunakan konsol Amazon FSx . Untuk informasi tentang cara mengaitkan alias DNS dengan sistem file yang ada, dan detail tentang cara menggunakan CLI dan API, lihat Mengelola alias DNS.

Untuk mengaitkan alias DNS saat membuat sebuah sistem file baru

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat sistem file baru seperti yang dijelaskan di Langkah 5. Buat sistem file Anda dari bagian Memulai.
3. Di bagian Akses - opsional dari penuntun Buat sistem file, masukkan alias DNS yang ingin Anda kaitkan dengan sistem file Anda.

   Gunakan pedoman berikut saat menentukan alias DNS:

   - Harus diformat sebagai fully qualified domain name (FQDN) *`hostname.domain`*, misalnya, `accounting.example.com`.
   - Dapat berisi karakter alfanumerik dan tanda hubung ().
   - Tidak dapat meluncurkan atau mengakhiri dengan tanda hubung.
   - Dapat memulai dengan angka.

Untuk nama alias DNS, Amazon FSx menyimpan karakter alfabet sebagai huruf kecil (a-z), terlepas dari bagaimana Anda menentukannya: sebagai huruf besar, huruf kecil, atau huruf yang sesuai dalam kode pelarian.

4. Untuk Preferensi pemeliharaan, buat perubahan apa pun yang Anda inginkan.
5. Di bagian Tag - opsional, tambahkan tag yang Anda butuhkan, dan kemudian pilih Selanjutnya.
6. Tinjau konfigurasi sistem file yang ditampilkan pada halaman Buat sistem file. Pilih Buat sistem file untuk membuat sistem file.

Konfigurasikan nama utama layanan (SPNs) untuk Kerberos

Kami menyarankan Anda menggunakan otentikasi dan enkripsi berbasis Kerberos dalam perjalanan dengan Amazon. FSx Kerberos menyediakan autentikasi paling aman untuk klien yang mengakses sistem file Anda.

Untuk mengaktifkan otentikasi Kerberos untuk klien yang mengakses Amazon FSx menggunakan alias DNS, Anda harus menambahkan nama utama layanan (SPNs) yang sesuai dengan alias DNS pada objek komputer Active Directory sistem file FSx Amazon Anda. SPN hanya dapat dikaitkan dengan objek komputer direktori aktif tunggal pada satu waktu. Jika Anda memiliki nama SPNs DNS yang dikonfigurasi untuk objek komputer Active Directory sistem file asli Anda, Anda harus menghapusnya terlebih dahulu.

Ada dua yang diperlukan SPNs untuk otentikasi Kerberos:

```
HOST/alias
HOST/alias.domain
```

Jika aliasnya`finance.domain.com`, berikut ini adalah dua yang diperlukan SPNs:

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> Anda harus menghapus HOST yang ada SPNs yang sesuai dengan alias DNS pada objek komputer Active Directory sebelum Anda membuat HOST baru SPNs untuk objek komputer

Active Directory (AD) sistem FSx file Amazon Anda. Upaya SPNs untuk mengatur sistem FSx file Amazon Anda akan gagal jika SPN untuk alias DNS ada di AD.

Prosedur berikut menjelaskan cara melakukan hal berikut:

- Temukan alias DNS yang ada SPNs pada objek komputer Active Directory sistem file asli.
- Hapus yang ada SPNs ditemukan, jika ada.
- Buat alias DNS baru SPNs untuk objek komputer Active Directory sistem FSx file Amazon Anda.

Untuk menginstal modul PowerShell Active Directory yang diperlukan

1. Masuk ke instance Windows yang bergabung dengan Active Directory tempat sistem FSx file Amazon Anda bergabung.
2. Buka PowerShell sebagai administrator.
3. Instal modul PowerShell Active Directory menggunakan perintah berikut.

```
Install-WindowsFeature RSAT-AD-PowerShell
```

Untuk menemukan dan menghapus alias DNS yang ada SPNs pada objek komputer Active Directory sistem file asli

Jika Anda telah SPNs mengonfigurasi alias DNS yang telah ditetapkan ke sistem file lain pada objek komputer di Active Directory, Anda harus terlebih dahulu menghapusnya SPNs sebelum menambahkan SPNs ke objek komputer sistem file Anda.

1. Temukan yang ada SPNs dengan menggunakan perintah berikut. Ganti *alias_fqdn* dengan alias DNS yang Anda kaitkan dengan sistem file di Langkah 1:.

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. Hapus HOST yang ada SPNs kembali pada langkah sebelumnya dengan menggunakan contoh script berikut.

- Ganti *alias_fqdn* dengan alias DNS penuh yang Anda kaitkan dengan sistem file di Langkah 1:.
- Ganti *file_system_DNS_name* dengan nama DNS sistem file yang semula.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Ulangi langkah-langkah sebelumnya untuk setiap alias DNS yang telah dikaitkan dengan sistem file di Langkah 1:.

Untuk mengatur SPNs objek komputer Active Directory sistem FSx file Amazon Anda

1. Tetapkan baru SPNs untuk sistem FSx file Amazon Anda dengan menjalankan perintah berikut.

   - Ganti *file_system_DNS_name* dengan nama DNS yang FSx ditetapkan Amazon ke sistem file.

     Untuk menemukan nama DNS sistem file Anda di FSx konsol Amazon, pilih Sistem file, pilih sistem file Anda, lalu pilih panel Jaringan & keamanan pada halaman detail sistem file.

     Anda juga bisa mendapatkan nama DNS sebagai respons operasi DescribeFileSystemsAPI.
   - Ganti *alias_fqdn* dengan alias DNS penuh yang Anda kaitkan dengan sistem file di Langkah 1:.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)
```

```
##Use the following command to set both the full FQDN and Alias SPNs
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname" =
 @($Alias, $Alias.Split(".")[0])}
```

> **Note**
>
> Menyetel SPN untuk sistem FSx file Amazon Anda akan gagal jika SPN untuk alias DNS ada di AD untuk objek komputer sistem file asli. Untuk informasi tentang menemukan dan menghapus yang ada SPNs, lihatUntuk menemukan dan menghapus alias DNS yang ada SPNs pada objek komputer Active Directory sistem file asli.

2. Verifikasi bahwa SPNs yang baru dikonfigurasi untuk alias DNS menggunakan contoh skrip berikut. Pastikan bahwa respons mencakup dua HOST SPNs, `HOST/`*`alias`* dan`HOST/`*`alias_fqdn`*, seperti yang dijelaskan sebelumnya dalam prosedur ini.

   Ganti *`file_system_DNS_name`* dengan nama DNS yang FSx ditetapkan Amazon ke sistem file Anda. Untuk menemukan nama DNS sistem file Anda di FSx konsol Amazon, pilih Sistem file, pilih sistem file Anda, lalu pilih panel Jaringan & keamanan pada halaman detail sistem file.

   Anda juga bisa mendapatkan nama DNS sebagai respons operasi DescribeFileSystemsAPI.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Ulangi langkah-langkah sebelumnya untuk setiap alias DNS yang telah dikaitkan dengan sistem file di Langkah 1:.

Memperbarui atau membuat catatan DNS CNAME

Setelah Anda mengkonfigurasi dengan benar SPNs untuk sistem file Anda, Anda dapat memotong ke Amazon FSx dengan mengganti setiap catatan DNS yang diselesaikan ke sistem file asli dengan catatan DNS yang menyelesaikan ke nama DNS default sistem file Amazon. FSx

Modul `dnsserver` dan modul Windows `activedirectory` diperlukan untuk menjalankan perintah yang disajikan di bagian ini.

Untuk menginstal PowerShell modul yang diperlukan

1. Masuk ke instans Windows yang bergabung dengan Active Directory yang sama dengan sistem FSx file Amazon Anda bergabung sebagai pengguna yang merupakan anggota grup yang memiliki izin administrasi DNS (Administrator Sistem Nama Domain AWS Delegasi AWS Managed Microsoft AD, dan Admin Domain atau grup lain tempat Anda telah mendelegasikan izin administrasi DNS di Direktori Aktif yang dikelola sendiri).

   Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
2. Buka PowerShell sebagai administrator.
3. Modul PowerShell DNS Server diperlukan untuk melakukan instruksi dalam prosedur ini. Instal modul tersebut perintah berikut.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Untuk memperbarui atau membuat nama DNS khusus ke sistem FSx file Amazon Anda

1. Connect ke EC2 instans Amazon Anda sebagai pengguna yang merupakan anggota grup yang memiliki izin administrasi DNS (Administrator Sistem Nama Domain AWS Delegasi di Direktori Aktif AWS Terkelola, dan Admin Domain atau grup lain tempat Anda telah mendelegasikan izin administrasi DNS di Direktori Aktif yang dikelola sendiri).

   Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
2. Pada command prompt, jalankan skrip berikut. Skrip ini memigrasikan catatan DNS CNAME yang ada ke sistem file Amazon FSx Anda. Jika tidak ada yang ditemukan, itu membuat catatan CNAME DNS baru untuk alias DNS *alias_fqdn* yang menyelesaikan nama DNS default untuk sistem file Amazon Anda. FSx

   Untuk menjalankan skrip tersebut:

   - Ganti *alias_fqdn* dengan alias DNS yang Anda kaitkan dengan sistem file.
   - Ganti *file_system_DNS_name* dengan nama DNS yang FSx telah ditetapkan Amazon ke sistem file.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

3. Ulangi langkah-langkah sebelumnya untuk setiap alias DNS yang Anda kaitkan dengan sistem file di Langkah 1:.

Anda sekarang telah menambahkan nilai DNS CNAME untuk sistem FSx file Amazon Anda dengan alias DNS. Sekarang Anda dapat menggunakan alias DNS untuk mengakses data Anda.

> **Note**
>
> Saat memperbarui catatan DNS CNAME untuk menunjuk ke sistem FSx file Amazon yang sebelumnya menunjuk ke sistem file lain, klien mungkin tidak dapat terhubung dengan sistem file untuk jangka waktu yang singkat. Ketika cache DNS klien menyegarkan kembali, mereka harus dapat terhubung menggunakan alias DNS. Untuk informasi selengkapnya, lihat Tidak dapat mengakses sistem file menggunakan alias DNS.

Menegakkan otentikasi Kerberos menggunakan Objek Kebijakan Grup () GPOs

Anda dapat menerapkan otentikasi Kerberos saat mengakses sistem file dengan menyetel Objek Kebijakan Grup (GPOs) berikut di Direktori Aktif Anda:

- Membatasi NTLM: Lalu lintas NTLM keluar menuju server jarak jauh - Gunakan pengaturan kebijakan ini untuk menolak atau meng-audit lalu lintas NTLM keluar dari sebuah komputer ke server jarak jauh yang menjalankan sistem operasi Windows.
- Membatasi NTLM: Menambahkan pengecualian server jarak jauh untuk autentikasi NTLM - Gunakan pengaturan kebijakan ini untuk membuat daftar pengecualian server jarak jauh yang padanya perangkat klien diperbolehkan untuk menggunakan autentikasi NTLM jika pengaturan

kebijakan Keamanan jaringan: Membatasi NTLM: Lalu lintas NTLM keluar menuju server jarak jauh dikonfigurasi.

1. Masuk ke instance Windows yang bergabung dengan Active Directory tempat sistem FSx file Amazon Anda bergabung sebagai administrator. Jika Anda mengonfigurasi Active Directory yang dikelola sendiri, terapkan langkah-langkah ini langsung ke Active Directory Anda.
2. Pilih Mulai, pilih Alat Administrasi, lalu pilih Manajemen Kebijakan Grup.
3. Pilih Objek Kebijakan Grup.
4. Jika Objek Kebijakan Grup Anda belum ada, buat itu.
5. Temukan Keamanan Jaringan yang ada: Batasi NTLM: Lalu lintas NTLM keluar ke kebijakan server jarak jauh. (Jika tidak ada kebijakan yang ada, buat kebijakan baru.) Di tab Pengaturan keamanan lokal, buka menu konteks (klik kanan), dan pilih Properti.
6. Pilih Tolak semua.
7. Pilih Terapkan untuk menyimpan pengaturan keamanan.
8. Untuk mengatur pengecualian untuk koneksi NTLM ke server jarak jauh tertentu untuk klien, cari Keamanan jaringan: Membatasi NTLM: Tambahkan pengecualian server jarak jauh.

   Buka menu konteks (klik kanan), dan pilih Properti di tab Pengaturan keamanan lokal.
9. Masukkan nama server yang akan ditambahkan ke daftar pengecualian.
10. Pilih Terapkan untuk menyimpan pengaturan keamanan.

Mengakses data menggunakan berbagi file

Berbagi file Microsoft Windows adalah folder atau direktori tertentu pada sistem file Anda. Ini termasuk setiap sub folder yang mungkin ada. Klien mengakses berbagi file di sistem file Anda menggunakan protokol Server Message Block (SMB). Sistem file Server File Windows Anda FSx untuk Windows dilengkapi dengan berbagi file Windows default, bernama`share`. Anda dapat membuat dan mengelola sebanyak mungkin berbagi file lain yang Anda inginkan dengan menggunakan alat antarmuka pengguna grafis (GUI) Windows Shared Folder.

Microsoft Windows Continuously Available (CA) berbagi memberikan manfaat utama mempertahankan akses tanpa gangguan ke file bersama bahkan ketika node server dalam cluster gagal. Menggunakan berbagi file CA dapat meminimalkan gangguan ke aplikasi server yang menyimpan file data mereka pada berbagi file ini selama jendela pemeliharaan sistem file.

Untuk informasi selengkapnya tentang membuat dan mengelola berbagi file pada sistem file Windows File Server Anda FSx , termasuk berbagi CA, lihatMembuat, memperbarui, menghapus berbagi file.

Memetakan berbagi file

Untuk mengakses berbagi file Anda, gunakan fungsionalitas Windows Map Network Drive untuk memetakan huruf drive pada instance komputasi Anda ke berbagi FSx file Amazon Anda. Proses pemetaan sebuah Berbagi file ke drive pada instans komputasi dikenal sebagai pemasangan Berbagi file di Linux. Proses ini berbeda-beda tergantung pada jenis instans komputasi dan sistem operasi. Setelah Berbagi file Anda dipetakan, aplikasi Anda dan para pengguna dapat mengakses file dan folder pada Berbagi file milik Anda seolah-olah semuanya adalah file dan folder lokal.

Untuk informasi selengkapnya tentang pemetaan dan pemasangan berbagi file untuk mengakses data pada sistem file Anda, lihat prosedur berikut:

- Memetakan berbagi file di instans Amazon EC2 Windows.
- Memasang berbagi file di instans Amazon EC2 Mac
- Memasang berbagi file di instans Amazon EC2 Linux

Memetakan berbagi file di instans Amazon EC2 Windows

Anda dapat memetakan file share pada instance EC2 Windows untuk mengakses sistem file Windows File Server Anda FSx dengan menggunakan Windows File Explorer atau command prompt.

Untuk memetakan file share pada instance Amazon EC2 Windows (File Explorer)

1. Luncurkan instance EC2 Windows dan sambungkan ke Microsoft Active Directory tempat Anda bergabung dengan sistem FSx file Amazon Anda. Untuk melakukannya, pilih salah satu berikut dari Panduan Administrasi AWS Directory Service :
   - Bergabunglah dengan instans Windows EC2 dengan mulus
   - Bergabunglah dengan instance Windows secara manual
2. Connect ke instance EC2 Windows Anda. Untuk informasi selengkapnya, lihat Menyambungkan ke instans Windows Anda di Panduan EC2 Pengguna Amazon.
3. Setelah tersambung, buka File Explorer.
4. Di panel navigasi, buka menu konteks (klik kanan) untuk Jaringan, dan pilih Drive Jaringan Peta.
5. Untuk Drive, pilih drive letter.

6. Untuk Folder, masukkan nama DNS dari sistem file atau alias DNS yang ter-associate dengan sistem file, dan nama Berbagi.

> **Important**
>
> Menggunakan alamat IP alih-alih nama DNS dapat mengakibatkan tidak tersedianya selama proses failover sistem file Multi-AZ. Juga, nama DNS atau alias DNS terkait diperlukan untuk otentikasi berbasis Kerberos dalam sistem file multi-AZ dan Single-AZ.

Anda dapat menemukan nama DNS sistem file dan alias DNS terkait di FSx konsol Amazon dengan memilih Windows File Server, Jaringan & keamanan. Atau, Anda dapat menemukan mereka dalam respon Operasi API CreateFileSystem atau DescribeFileSystems. Untuk informasi selengkapnya tentang menggunakan alias DNS, lihat Mengelola alias DNS.

- Untuk sistem file Single-AZ yang bergabung dengan Direktori Aktif Microsoft AWS Terkelola, nama DNS terlihat seperti berikut ini.

```
fs-0123456789abcdef0.ad-domain.com
```

- Untuk sistem file Single-AZ yang tergabung ke Direktori Aktif yang dikelola sendiri, dan sistem file Multi-AZ, nama DNS terlihat seperti berikut ini.

```
amznfsxaa11bb22.ad-domain.com
```

Contohnya, untuk menggunakan nama DNS sistem file Single-AZ, masukkan yang berikut untuk Folder.

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

Untuk menggunakan nama DNS sistem file Multi-AZ, masukkan yang berikut ini untuk Folder.

```
\\amznfsxaa11bb22.ad-domain.com\share
```

Untuk menggunakan alias DNS yang ter-associate dengan sistem file, masukkan yang berikut ini untuk Folder.

```
\\fqdn-dns-alias\share
```

7. Pilih sebuah opsi untuk Sambungkan kembali saat masuk, yang menunjukkan apakah Berbagi file harus menyambung kembali saat masuk, dan kemudian pilih Selesai.

Untuk memetakan file share pada instance Amazon EC2 Windows (command prompt)

1. Luncurkan instance EC2 Windows dan sambungkan ke Microsoft Active Directory tempat Anda bergabung dengan sistem FSx file Amazon Anda. Untuk melakukannya, pilih salah satu berikut dari Panduan Administrasi AWS Directory Service :
   - Bergabunglah dengan instans Windows EC2 dengan mulus
   - Bergabunglah dengan instance Windows secara manual
2. Connect ke instance EC2 Windows Anda sebagai pengguna di AWS Managed Microsoft AD direktori Anda. Untuk informasi selengkapnya, lihat Menyambungkan ke instans Windows Anda di Panduan EC2 Pengguna Amazon.
3. Setelah terhubung, buka jendela command prompt.
4. Pasang Berbagi file menggunakan drive letter pilihan Anda, nama DNS sistem file, dan nama Berbagi. Anda dapat menemukan nama DNS menggunakan FSx konsol Amazon dengan memilih Windows File Server, Jaringan & keamanan. Atau, Anda dapat menemukan mereka dalam respon Operasi API `CreateFileSystem` atau `DescribeFileSystems`.
   - Untuk sistem file Single-AZ yang bergabung dengan Direktori Aktif Microsoft AWS Terkelola, nama DNS terlihat seperti berikut ini.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```
   - Untuk sistem file Single-AZ yang tergabung ke Direktori Aktif yang dikelola sendiri, dan sistem file Multi-AZ, nama DNS terlihat seperti berikut ini.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   Berikut ini adalah contoh perintah untuk memasang Berbagi file.

   ```
   $ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
   ```

Alih-alih `net use` perintah, Anda juga dapat menggunakan PowerShell perintah yang didukung untuk me-mount file share.

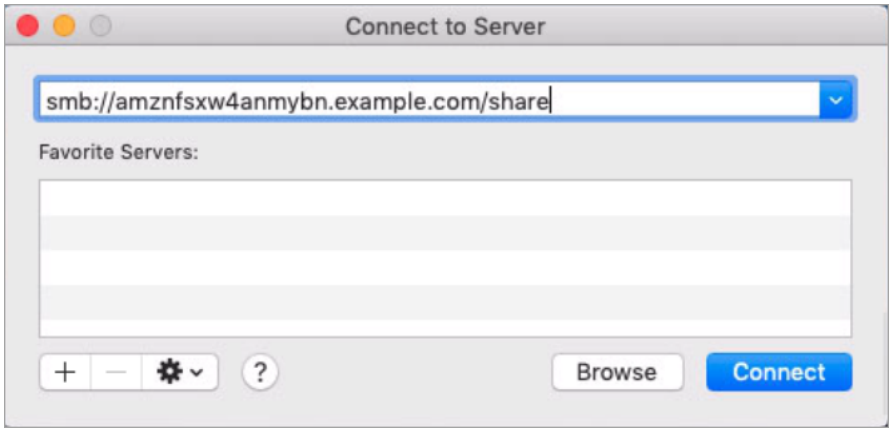
Memasang berbagi file di instans Amazon EC2 Mac

Anda dapat memasang berbagi file di instans Amazon EC2 Mac yang digabungkan ke Active Directory atau tidak bergabung untuk mengakses sistem file Windows File Server Anda FSx . Jika instans tidak tergabung ke Direktori Aktif Anda, pastikan untuk memperbarui kumpulan opsi DHCP untuk Amazon Virtual Private Cloud (Amazon VPC) tempat instans berdiam untuk memasukkan server nama DNS untuk domain Direktori Aktif Anda. Kemudian luncurkan kembali instans.

Untuk me-mount file share pada instans Amazon EC2 Mac (GUI)

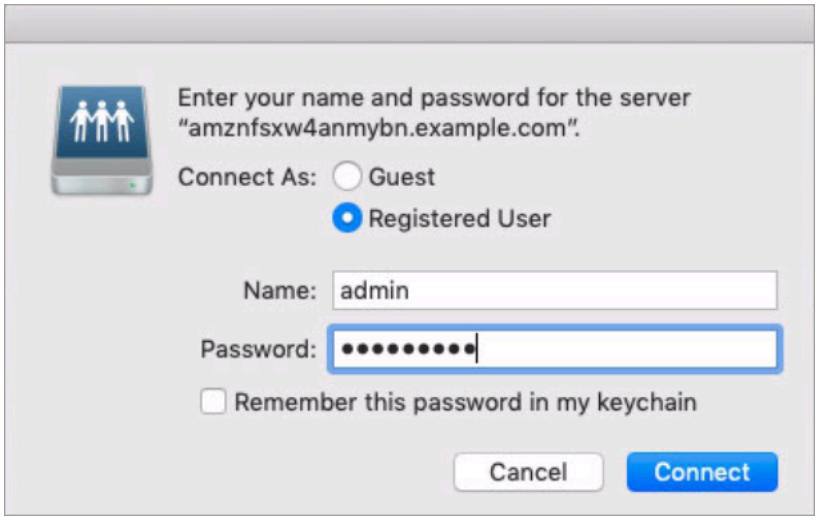
1. Luncurkan instance EC2 Mac. Untuk melakukan ini, pilih salah satu prosedur berikut dari Panduan EC2 Pengguna Amazon:
   - Luncurkan instance Mac menggunakan konsol
   - Luncurkan instance Mac menggunakan AWS CLI
2. Connect ke instans EC2 Mac menggunakan Virtual Network Computing (VNC). Untuk informasi selengkapnya, lihat Connect ke instans menggunakan VNC di Panduan EC2 Pengguna Amazon.
3. Pada instance EC2 Mac Anda, sambungkan ke berbagi FSx file Amazon Anda, sebagai berikut:
   a. Buka Finder, pilih Go, lalu pilih Connect ke Server.
   b. Di kotak dialog Connect ke Server, masukkan nama DNS sistem file atau alias DNS yang dikaitkan dengan sistem file, dan nama Berbagi. Kemudian pilih Connect.

      Anda dapat menemukan nama DNS sistem file dan alias DNS terkait di FSx konsol Amazon dengan memilih Windows File Server, Jaringan & keamanan. Atau, Anda dapat menemukan mereka dalam respon Operasi API CreateFileSystem atau DescribeFileSystems. Untuk informasi selengkapnya tentang penggunaan alias DNS, lihat Mengelola alias DNS.



c. Pada layar berikutnya, pilih Connect untuk melanjutkan.

d. Masukkan kredensyal Microsoft Active Directory (AD) untuk akun FSx layanan Amazon, seperti yang ditunjukkan pada contoh berikut. Kemudian pilih Connect.



e. Jika koneksi berhasil, Anda dapat melihat FSx bagian Amazon, di bawah Lokasi di jendela Finder Anda.

Untuk me-mount file share pada instance Amazon EC2 Mac (baris perintah)

1. Luncurkan instance EC2 Mac. Untuk melakukan ini, pilih salah satu prosedur berikut dari Panduan EC2 Pengguna Amazon:

   - Luncurkan instance Mac menggunakan konsol
   - Luncurkan instance Mac menggunakan AWS CLI

2. Connect ke instans EC2 Mac menggunakan Virtual Network Computing (VNC). Untuk informasi selengkapnya, lihat Connect ke instans menggunakan VNC di Panduan EC2 Pengguna Amazon.

3. Pasang Berbagi file dengan perintah berikut.

```
mount_smbfs //file_system_dns_name/file_share mount_point
```

Anda dapat menemukan nama DNS di FSxkonsol Amazon dengan memilih Windows File Server, Jaringan & keamanan. Atau, Anda dapat menemukan mereka dalam respon Operasi API `CreateFileSystem` atau `DescribeFileSystems`.

- Untuk sistem file Single-AZ yang bergabung dengan Direktori Aktif Microsoft AWS Terkelola, nama DNS terlihat seperti berikut ini.

```
fs-0123456789abcdef0.ad-domain.com
```

- Untuk sistem file Single-AZ yang tergabung ke Direktori Aktif yang dikelola sendiri, dan sistem file Multi-AZ, nama DNS terlihat seperti berikut ini.

```
amznfsxaa11bb22.ad-domain.com
```

Perintah pemasangan yang digunakan dalam prosedur ini melakukan hal berikut pada titik-titik berikut:

- *//file_system_dns_name/file_share* — Tentukan nama DNS dan nama Berbagi sistem file untuk memasang.
- *mount_point*— Direktori pada EC2 contoh tempat Anda memasang sistem file.

Memasang berbagi file di instans Amazon EC2 Linux

Anda dapat memasang file share FSx untuk Windows File Server pada instance Amazon EC2 Linux yang digabungkan ke Active Directory atau tidak bergabung untuk mengakses sistem file Windows File Server Anda FSx .

> **Note**
>
> - Perintah berikut menentukan parameter seperti protokol SMB, caching, dan ukuran buffer baca dan tulis sebagai contoh saja. Pilihan parameter untuk `cifs` perintah Linux, serta

versi kernel Linux yang digunakan, dapat memengaruhi throughput dan latensi untuk operasi jaringan antara klien dan sistem FSx file Amazon. Untuk informasi selengkapnya, lihat `cifs` dokumentasi untuk lingkungan Linux yang Anda gunakan.

- Klien Linux tidak mendukung failover berbasis DNS otomatis. Untuk informasi selengkapnya, lihat Pengalaman failover pada klien Linux.

Untuk me-mount file share pada instance Amazon EC2 Linux yang digabungkan ke Active Directory

1. Jika Anda belum memiliki instance EC2 Linux yang sedang berjalan bergabung dengan Microsoft Active Directory, lihat Menggabungkan instance Linux secara manual di Panduan AWS Directory Service Administrasi untuk petunjuk melakukannya.
2. Connect ke instans EC2 Linux Anda. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda di Panduan EC2 Pengguna Amazon.
3. Jalankan perintah berikut untuk menginstal paket `cifs-utils`. Paket ini digunakan untuk me-mount sistem file jaringan seperti Amazon FSx di Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Buat **`/mnt/fsx`** direktori titik pasang. Di sinilah Anda akan memasang sistem FSx file Amazon.

   ```
   $ sudo mkdir -p /mnt/fsx
   ```

5. Autentikasi dengan kerberos menggunakan perintah berikut.

   ```
   $ kinit
   ```

6. Pasang Berbagi file dengan perintah berikut.

   ```
   $ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
    vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
   file-server-Ip
   ```

   Anda dapat menemukan nama DNS di FSxkonsol Amazon dengan memilih Windows File Server, Jaringan & keamanan. Atau, Anda dapat menemukan mereka dalam respon operasi API `CreateFileSystem` atau `DescribeFileSystems`.

- Untuk sistem file Single-AZ yang bergabung dengan Direktori Aktif Microsoft AWS Terkelola, nama DNS terlihat seperti berikut ini.

```
fs-0123456789abcdef0.ad-domain.com
```

- Untuk sistem file Single-AZ yang tergabung ke Direktori Aktif yang dikelola sendiri, dan sistem file Multi-AZ, nama DNS terlihat seperti berikut ini.

```
amznfsxaa11bb22.ad-domain.com
```

Ganti *CIFSMaxBufSize* dengan nilai terbesar yang diizinkan oleh kernel Anda. Jalankan perintah berikut untuk mendapatkan nilai ini.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Hasilnya menunjukkan bahwa ukuran buffer maksimum adalah 130048.

7. Verifikasikan bahwa sistem file dipasang dengan menjalankan perintah berikut, yang menghasilkan hanya sistem file jenis Sistem File Internet Umum (CIFS).

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

Perintah pemasangan yang digunakan dalam prosedur ini melakukan hal berikut pada titik-titik berikut:

- *//file_system_dns_name/file_share* — Tentukan nama DNS dan nama Berbagi sistem file untuk memasang.
- *mount_point*— Direktori pada EC2 contoh tempat Anda memasang sistem file.
- `-t cifs vers=`*SMB_version*— Menentukan jenis sistem file sebagai CIFS dan versi protokol SMB. Amazon FSx untuk Windows File Server mendukung SMB versi 2.0 hingga 3.1.1.
- `sec=krb5` — Tentukan untuk autentikasi menggunakan Kerberos versi 5.

- `cache=cache_mode`— Mengatur mode cache. Opsi untuk cache CIFS ini dapat memengaruhi kinerja, dan Anda harus menguji pengaturan mana yang paling sesuai (dan meninjau dokumentasi Linux) untuk kernel dan beban kerja Anda. Pilihan `strict` dan `none` direkomendasikan, karena `loose` dapat menyebabkan inkonsistensi data karena semantik protokol longgar.
- `cruid=ad_user` — Atur uid dari pemilik cache kredensial ke administrator direktori AD.
- `/mnt/fsx`— Menentukan titik pemasangan untuk berbagi FSx file Amazon pada EC2 instans Anda.
- `rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize` — Tentukan ukuran buffer baca dan tulis sebagai ukuran maksimum yang diizinkan oleh protokol CIFS. Ganti `CIFSMaxBufSize` dengan nilai terbesar yang diizinkan oleh kernel Anda. Tentukan `CIFSMaxBufSize` dengan menjalankan perintah berikut.

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  Hasilnya menunjukkan bahwa ukuran buffer maksimum adalah 130048.
- `ip=preferred-file-server-Ip` — Mengatur alamat IP tujuan ke server file pilihan sistem file.

  Anda dapat mengambil alamat IP server file pilihan dari sistem file sebagai berikut:

  - Menggunakan FSx konsol Amazon, pada tab Jaringan & keamanan pada halaman detail sistem File.
  - Sebagai tanggapan dari perintah `describe-file-systems` CLI atau perintah DescribeFileSystemsAPI yang setara.

Untuk me-mount file share pada instance Amazon EC2 Linux yang tidak digabungkan ke Active Directory

Prosedur berikut memasang FSx file share Amazon ke instans Amazon EC2 Linux yang tidak bergabung dengan Active Directory (AD) Anda. Untuk instance EC2 Linux yang tidak bergabung dengan AD Anda, Anda hanya dapat memasang file share FSx untuk Windows File Server dengan menggunakan alamat IP pribadinya. Anda bisa mendapatkan alamat IP pribadi sistem file menggunakan FSx konsol Amazon, di tab Jaringan & keamanan, di Alamat IP Server File Pilihan.

Contoh ini menggunakan autentikasi NTLM. Untuk melakukan ini, Anda memasang sistem file sebagai pengguna yang merupakan anggota domain Microsoft Active Directory FSx yang bergabung

dengan sistem file Windows File Server. Kredensyal untuk akun pengguna disediakan dalam file teks yang Anda buat pada EC2 instance Anda,. `creds.txt` File ini berisikan nama pengguna, kata sandi, dan domain untuk pengguna.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Untuk meluncurkan dan mengkonfigurasi EC2 instans Amazon Linux

1. Luncurkan EC2 instans Amazon Linux menggunakan EC2konsol Amazon. Untuk informasi selengkapnya, lihat Meluncurkan instance di Panduan EC2 Pengguna Amazon.
2. Connect ke EC2 instans Amazon Linux Anda. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda di Panduan EC2 Pengguna Amazon.
3. Jalankan perintah berikut untuk menginstal paket `cifs-utils`. Paket ini digunakan untuk me-mount sistem file jaringan seperti Amazon FSx di Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Buat titik pemasangan **`/mnt/fsxx`** tempat Anda berencana memasang sistem FSx file Amazon.

   ```
   $ sudo mkdir -p /mnt/fsx
   ```

5. Buat file kredensial `creds.txt` di direktori `/home/ec2-user`, menggunakan format yang ditampilkan sebelumnya.
6. Atur izin file `creds.txt` sehingga hanya Anda (sang pemilik) yang dapat membaca dan menulis ke file dengan menjalankan perintah berikut.

   ```
   $ chmod 700 creds.txt
   ```

Untuk memasang sistem file

1. Anda memasang Berbagi file yang tidak tergabung ke Direktori Aktif Anda dengan menggunakan alamat IP privat-nya. Anda bisa mendapatkan alamat IP pribadi sistem file menggunakan FSx konsol Amazon, di tab Jaringan & keamanan, di Alamat IP Server File Pilihan.
2. Pasang sistem file menggunakan perintah berikut:

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

Ganti *CIFSMaxBufSize* dengan nilai terbesar yang diizinkan oleh kernel Anda. Jalankan perintah berikut untuk mendapatkan nilai ini.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Hasilnya menunjukkan bahwa ukuran buffer maksimum adalah 130048.

3. Verifikasi bahwa sistem file dipasang dengan menjalankan perintah berikut, yang menghasilkan hanya sistem file CIFS.

```
$ mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
```

Perintah pemasangan yang digunakan dalam prosedur ini melakukan hal berikut pada titik-titik berikut:

- *//file-system-IP-address/file_share*— Menentukan alamat IP dan berbagi sistem file yang Anda pasang.
- `-t cifs vers=`*SMB_version*— Menentukan jenis sistem file sebagai CIFS dan versi protokol SMB. Amazon FSx untuk Windows File Server mendukung SMB versi 2.0 hingga 3.1.1.
- `sec=ntlmsspi` - Tentukan untuk menggunakan Antarmuka Penyedia Support Keamanan Manajer NT LAN (NTLMSSPI) untuk autentikasi .
- `cache=`*cache_mode*— Mengatur mode cache. Opsi untuk cache CIFS ini dapat memengaruhi kinerja, dan Anda harus menguji pengaturan mana yang paling sesuai (dan meninjau dokumentasi Linux) untuk kernel dan beban kerja Anda. Pilihan `strict` dan `none` direkomendasikan, karena `loose` dapat menyebabkan inkonsistensi data karena semantik protokol longgar.
- `cred=/home/ec2-user/creds.txt` — Tentukan tempat untuk mendapatkan kredensial pengguna.

- */mnt/fsx*— Menentukan titik pemasangan untuk berbagi FSx file Amazon pada EC2 instans Anda.
- `rsize=`*`CIFSMaxBufSize`*`,wsize=`*`CIFSMaxBufSize`* — Tentukan ukuran buffer baca dan tulis sebagai ukuran maksimum yang diizinkan oleh protokol CIFS. Ganti *`CIFSMaxBufSize`* dengan nilai terbesar yang diizinkan oleh kernel Anda. Tentukan `CIFSMaxBufSize` dengan menjalankan perintah berikut.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Secara otomatis memasang berbagi file pada instans Amazon EC2 Linux

Anda dapat secara otomatis me-mount file share Windows File Server Anda FSx untuk mengakses sistem file Windows File Server Anda setiap kali instance Amazon EC2 Linux yang dipasang reboot. FSx Untuk melakukannya, tambahkan entri ke `/etc/fstab` file pada EC2 instance. File `/etc/fstab` berisi informasi tentang sistem file. Perintah mount -a, yang berjalan selama startup instans, memasang sistem file yang tercantum dalam file `/etc/fstab`.

Untuk instance Amazon EC2 Linux yang tidak bergabung dengan Active Directory, Anda hanya dapat memasang file share FSx untuk Windows File Server dengan menggunakan alamat IP pribadinya. Anda bisa mendapatkan alamat IP pribadi sistem file menggunakan FSx konsol Amazon, di tab Jaringan & keamanan, di Alamat IP Server File Pilihan.

Prosedur berikut menggunakan autentikasi Microsoft NTLM. Anda memasang sistem file sebagai pengguna yang merupakan anggota domain Microsoft Active Directory yang FSx bergabung dengan sistem file Windows File Server. Anda dapat mengambil kredensyal untuk akun pengguna dari `creds.txt` file menggunakan perintah berikut.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Untuk secara otomatis me-mount file share pada EC2 instans Amazon Linux yang tidak tergabung ke Active Directory

Untuk meluncurkan dan mengkonfigurasi EC2 instans Amazon Linux

1. Luncurkan EC2 instans Amazon Linux menggunakan EC2konsol Amazon. Untuk informasi selengkapnya, lihat Meluncurkan instance di Panduan EC2 Pengguna Amazon.
2. Terhubung ke instans Anda. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda di Panduan EC2 Pengguna Amazon.
3. Jalankan perintah berikut untuk menginstal paket `cifs-utils`. Paket ini digunakan untuk me-mount sistem file jaringan seperti Amazon FSx di Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Buatlah direktori `/mnt/fsx`. Di sinilah Anda akan memasang sistem FSx file Amazon.

   ```
   $ sudo mkdir /mnt/fsx
   ```

5. Buat file kredensial `creds.txt` di direktori `/home/ec2-user`.
6. Atur izin file sehingga hanya Anda (sang pemilik) yang dapat membaca file dengan menjalankan perintah berikut.

   ```
   $ sudo chmod 700 creds.txt
   ```

Untuk memasang sistem file secara otomatis

1. Anda secara otomatis memasang sebuah berbagi file yang tidak tergabung ke Direktori Aktif Anda dengan menggunakan alamat IP privat. Anda bisa mendapatkan alamat IP pribadi sistem file menggunakan FSx konsol Amazon, di tab Jaringan & keamanan, di Alamat IP Server File Pilihan.
2. Untuk secara otomatis memasang berbagi file menggunakan alamat IP privat, tambahkan baris berikut ke file `/etc/fstab`.

   ```
   //file-system-IP-address/file_share /mnt/fsx cifs
    vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
   creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none 0 0
   ```

Ganti *CIFSMaxBufSize* dengan nilai terbesar yang diizinkan oleh kernel Anda. Jalankan perintah berikut untuk mendapatkan nilai ini.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Hasilnya menunjukkan bahwa ukuran buffer maksimum adalah 130048.

3. Ujilah entri `fstab` dengan menggunakan perintah `mount` dengan opsi 'palsu' dalam hubungannya dengan opsi 'semua' dan 'verbose'.

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. Untuk me-mount file share, reboot EC2 instance Amazon.
5. Ketika instans sudah tersedia lagi, verifikasi bahwa sistem file telah terpasang dengan menjalankan perintah berikut.

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

Baris yang ditambahkan ke file `/etc/fstab` dalam prosedur ini melakukan hal berikut pada titik-titik berikut:

- *//file-system-IP-address/file_share*— Menentukan alamat IP dan berbagi sistem FSx file Amazon yang Anda pasang.
- `/mnt/fsx`— Menentukan titik pemasangan untuk sistem FSx file Amazon pada EC2 instans Anda.
- `cifs vers=`*SMB_version*— Menentukan jenis sistem file sebagai CIFS dan versi protokol SMB. Amazon FSx untuk Windows File Server mendukung SMB versi 2.0 hingga 3.1.1.
- `sec=ntlmsspi` — Tentukan menggunakan Antarmuka Penyedia Support Keamanan Manajer NT LAN untuk memfasilitasi autentikasi respon tantangan NTLM.
- `cache=`*cache_mode*— Mengatur mode cache. Opsi untuk cache CIFS ini dapat memengaruhi kinerja, dan Anda harus menguji pengaturan mana yang paling sesuai (dan meninjau dokumentasi Linux) untuk kernel dan beban kerja Anda. Pilihan `strict` dan none

direkomendasikan, karena `loose` dapat menyebabkan inkonsistensi data karena semantik protokol longgar.

- `cred=/home/ec2-user/creds.txt` — Tentukan tempat untuk mendapatkan kredensial pengguna.
- `_netdev` — Beritahu sistem operasi bahwa sistem file berdiam di sebuah perangkat yang memerlukan akses jaringan. Menggunakan opsi ini mencegah instans dari pemasangan sistem file sampai layanan jaringan diaktifkan pada client.
- `0` — Menunjukkan bahwa sistem file harus didukung oleh dump, jika itu nilainya bukan nol. Untuk Amazon FSx, nilai ini seharusnya`0`.
- `0` — Tentukan urutan tempat `fsck` memeriksa sistem file pada boot. Untuk sistem FSx file Amazon, nilai ini `0` harus menunjukkan bahwa tidak `fsck` boleh berjalan saat start up.

Membuat, memperbarui, menghapus berbagi file

Topik ini menjelaskan bagaimana Anda dapat mengelola berbagi file dengan melakukan tugas-tugas berikut.

- Membuat pembagian file baru
- Ubah berbagi file yang ada
- Hapus berbagi file yang ada

Anda dapat menggunakan GUI Folder Bersama Windows-native dan FSx CLI Amazon untuk manajemen jarak jauh PowerShell untuk mengelola berbagi file pada sistem file Windows File Server Anda FSx . Anda mungkin mengalami penundaan saat menggunakan GUI Folder Bersama (fsmgmt.msc) saat pertama kali membuka menu konteks untuk berbagi yang terletak di sistem file yang berbeda. Untuk menghindari penundaan ini, gunakan PowerShell untuk mengelola berbagi file yang terletak di beberapa sistem file.

Microsoft Windows memberlakukan aturan dan batasan untuk penamaan file dan direktori. Untuk memastikan bahwa Anda berhasil membuat dan mengakses data Anda, Anda harus memberi nama file dan direktori Anda sesuai dengan pedoman Windows ini. Untuk informasi selengkapnya, lihat Konvensi Penamaan.

> **Warning**
>
> Amazon FSx mengharuskan pengguna SYSTEM memiliki izin NTFS ACL kontrol penuh pada setiap folder tempat Anda membuat file berbagi SMB. Jangan mengubah izin NTFS ACL untuk pengguna ini pada folder Anda, karena dapat membuat file Anda berbagi tidak dapat diakses.

Mengelola berbagi file dengan GUI Folder Bersama

Untuk mengelola berbagi file di sistem FSx file Amazon Anda, Anda dapat menggunakan GUI Folder Bersama. GUI Folder Bersama menyediakan lokasi pusat untuk mengelola semua folder bersama pada server Windows. Prosedur berikut menjelaskan cara mengelola berbagi file Anda.

Untuk menghubungkan folder bersama ke sistem file Windows File Server Anda FSx

1. Luncurkan EC2 instans Amazon Anda dan sambungkan ke Microsoft Active Directory tempat sistem FSx file Amazon Anda bergabung. Untuk melakukannya, pilih salah satu berikut dari Panduan Administrasi AWS Directory Service :

   - Bergabunglah dengan instans Windows EC2 dengan mulus
   - Bergabung dengan instance Windows secara manual

2. Connect ke instans Anda sebagai pengguna yang merupakan anggota dari grup administrator sistem file. Di Direktori Aktif Microsoft AWS Terkelola, grup ini disebut FSx Administrator AWS Delegasi. Di Direktori Aktif Microsoft yang dikelola sendiri, grup ini disebut Admin Domain atau nama kustom untuk grup administrator yang Anda berikan selama pembuatan. Untuk informasi selengkapnya, lihat Connect ke instans Windows Anda di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Windows.
3. Buka menu start dan jalankan fsmgmt.msc menggunakan Jalankan sebagai Administrator. Tindakan ini akan membuka alat GUI Folder Bersama.
4. Untuk Tindakan, pilih Connect ke komputer lain.
5. Untuk komputer lain, masukkan nama Domain Name System (DNS) untuk sistem FSx file Amazon Anda, misalnya**`amznfsxabcd0123.corp.example.com`**.

   Untuk menemukan nama DNS sistem file Anda di FSx konsol Amazon, pilih Sistem file, pilih sistem file Anda, lalu periksa bagian Jaringan & Keamanan pada halaman detail sistem file. Anda juga bisa mendapatkan nama DNS sebagai respons operasi DescribeFileSystemsAPI.

6. Pilih OKE. Entri untuk sistem FSx file Amazon Anda kemudian muncul dalam daftar untuk alat Folder Bersama.

Sekarang Folder Bersama terhubung ke sistem FSx file Amazon Anda, Anda dapat mengelola berbagi file Windows pada sistem file. Pembagian default disebut `\share`. Anda dapat melakukannya dengan tindakan berikut:

- Buat berbagi file baru — Di alat Folder Bersama, pilih Berbagi di panel kiri untuk melihat pembagian aktif untuk sistem FSx file Amazon Anda. Pilih Pembagian Baru dan selesaikan wizard Buat Folder Bersama.

  Anda harus membuat folder lokal sebelum membuat pembagian file baru. Anda dapat melakukannya sebagai berikut:

  - Menggunakan alat Folder Bersama: klik "Browse" saat menentukan jalur folder lokal dan klik "Buat folder baru" untuk membuat folder lokal.
  - Menggunakan baris perintah:

    ```
    New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
    \MyNewShare
    ```

- Mengubah pembagian file — Di alat Folder Bersama, buka menu konteks (klik kanan) untuk pembagian file yang ingin Anda ubah dalam panel kanan, lalu pilih Properti. Ubah properti dan pilih OKE.
- Menghapus pembagian file — Di alat Folder Bersama, buka menu konteks (klik kanan) untuk pembagian file yang ingin Anda hapus di panel kanan, lalu pilih Berhenti Berbagi.

> **Note**
>
> Untuk sistem file Single-AZ 2 dan Multi-AZ, menghapus berbagi file atau memodifikasi berbagi file (termasuk memperbarui izin, batas pengguna, dan properti lainnya) menggunakan alat GUI Folder Bersama hanya dimungkinkan jika Anda terhubung ke fsmgmt.msc menggunakan Nama DNS dari sistem file Amazon. FSx Alat GUI Folder Bersama tidak mendukung tindakan ini jika Anda terhubung menggunakan alamat IP atau nama alias DNS dari sistem file.

> **Note**
>
> Jika Anda menggunakan alat GUI Fsmgmt.msc Folder Bersama untuk mengakses berbagi yang terletak di beberapa FSx untuk sistem file Windows File Server, Anda mungkin mengalami penundaan saat pertama kali membuka menu konteks berbagi file untuk berbagi yang terletak di sistem file yang berbeda. Untuk menghindari penundaan ini, Anda dapat mengelola berbagi file menggunakan PowerShell seperti yang dijelaskan di bawah ini.

Mengelola berbagi file dengan PowerShell

Anda dapat mengelola berbagi file menggunakan kustom FSx untuk perintah manajemen jarak jauh Windows File Server untuk. PowerShell Perintah ini dapat membantu Anda mengotomatiskan pengelolaan tugas berbagi file seperti:

- Memigrasi berbagi file dari server file yang ada ke Amazon FSx
- Menyinkronkan berbagi file Wilayah AWS untuk pemulihan bencana
- Mengelola alur kerja berbagi file yang sedang berlangsung secara terprogram, seperti penyediaan berbagi file tim

Untuk mempelajari cara menggunakan Amazon FSx CLI untuk manajemen jarak jauh PowerShell, lihat. Menggunakan Amazon FSx CLI untuk PowerShell

Tabel berikut mencantumkan PowerShell perintah manajemen jarak jauh Amazon FSx CLI yang dapat Anda gunakan untuk mengelola berbagi file FSx untuk sistem file Windows File Server.

Perintah Pengelolaan Pembagian	Deskripsi
New-FSxSmbShare	Membuat pembagian file baru.
Remove-FSxSmbShare	Menghapus pembagian file.
Get-FSxSmbShare	Mengambil pembagian file yang ada.

Perintah Pengelolaan Pembagian	Deskripsi
Set-FSxSmbShare	Mengatur properti untuk pembagian.
Get-FSxSmbShareAccess	Mengambil daftar kontrol akses (ACL) pembagian.
Grant-FSxSmbShareAccess	Menambahkan entri kontrol akses (ACE) izinkan untuk trustee ke descriptor keamanan pembagian.
Revoke-FSxSmbShareAccess	Menghapus semua izin ACEs untuk wali amanat dari deskriptor keamanan saham.
Block-FSxSmbShareAccess	Menambahkan ACE tolak untuk trustee ke descriptor keamanan pembagian.
Unblock-FSxSmbShareAccess	Menghapus semua penolakan ACEs untuk wali amanat dari deskriptor keamanan saham.

Bantuan online untuk setiap perintah memberikan referensi dari semua opsi perintah. Untuk mengakses bantuan ini, jalankan perintah dengan `-?`, misalnya `New-FSxSmbShare -?`.

Meneruskan kredensil ke New- FSx SmbShare

Anda dapat meneruskan kredensil ke New- FSx SmbShare sehingga Anda dapat menjalankannya dalam satu lingkaran untuk membuat ratusan atau ribuan saham tanpa harus memasukkan kembali kredensi setiap kali.

Siapkan objek kredensi yang diperlukan untuk membuat berbagi file di server file Windows File Server Anda FSx menggunakan salah satu opsi berikut.

- Untuk membuat objek kredensial secara interaktif, gunakan perintah berikut.

```
$credential = Get-Credential
```

- Untuk menghasilkan objek kredensi menggunakan AWS Secrets Manager sumber daya, gunakan perintah berikut.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
```

```
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

Untuk membuat share yang terus tersedia (CA)

Anda dapat membuat saham yang tersedia terus menerus (CA) menggunakan Amazon FSx CLI untuk Manajemen Jarak Jauh di. PowerShell Saham CA yang dibuat pada sistem file multi-AZ FSx untuk Windows File Server sangat tahan lama dan sangat tersedia. Sistem file Amazon FSx Single-AZ dibangun di atas kluster simpul tunggal. Akibatnya, pembagian CA yang dibuat pada sistem file Single-AZ sangat berdaya tahan, tetapi tidak selalu tersedia. Gunakan `New-FSxSmbShare` perintah dengan `-ContinuouslyAvailable` opsi yang diatur `$True` untuk menentukan bahwa share adalah share yang terus tersedia. Berikut ini adalah contoh perintah untuk membuat pembagian CA.

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

Anda dapat memodifikasi `-ContinuouslyAvailable` opsi pada berbagi file yang ada menggunakan `Set-FSxSmbShare` perintah.

Tentukan apakah berbagi file yang ada terus tersedia

Gunakan perintah berikut untuk melihat nilai properti Continuous Available untuk berbagi file yang ada.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

Jika CA diaktifkan, output akan mencakup baris berikut:

```
[...]
ContinuouslyAvailable : True
[...]
```

Jika CA tidak diaktifkan, output akan mencakup baris berikut:

```
[...]
ContinuouslyAvailable : False
[...]
```

Untuk mengaktifkan Continuous Available pada file share yang ada, gunakan perintah berikut:

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

FSxSmbShare Perintah baru gagal dengan kepercayaan satu arah

Amazon FSx tidak mendukung eksekusi `New-FSxSmbShare` PowerShell perintah dalam kasus di mana Anda memiliki kepercayaan satu arah dan domain tempat pengguna berada tidak dikonfigurasi untuk mempercayai domain yang terkait dengan sistem FSx file Amazon.

Anda dapat mengatasi keadaan ini menggunakan salah satu solusi berikut:

- Pengguna yang menjalankan `New-FSxSmbShare` perintah harus berada dalam domain yang sama dengan sistem FSx file.
- Anda dapat menggunakan fsmgmt.msc GUI untuk membuat pembagian pada sistem file Anda. Untuk informasi selengkapnya, lihat Mengelola berbagi file dengan GUI Folder Bersama.

Ketersediaan dan daya tahan: Sistem file Single-AZ dan Multi-AZ

Amazon FSx untuk Windows File Server menawarkan dua jenis penyebaran sistem file: Single-AZ dan Multi-AZ. Bagian berikut memberikan informasi untuk membantu Anda memilih jenis penerapan yang tepat untuk beban kerja Anda. Untuk informasi tentang ketersediaan layanan SLA (Perjanjian Tingkat Layanan), lihat Perjanjian Tingkat FSx Layanan Amazon.

Sistem file Single-AZ terdiri dari satu instance server file Windows dan satu set volume penyimpanan dalam satu Availability Zone (AZ). Dengan sistem file Single-AZ, data secara otomatis direplikasi untuk melindunginya dari kegagalan satu komponen dalam banyak kasus. Amazon FSx terus memantau kegagalan perangkat keras, dan secara otomatis pulih dari peristiwa kegagalan dengan mengganti komponen infrastruktur yang gagal. Sistem file single-AZ biasanya mengalami sekitar 30 menit downtime selama peristiwa pemulihan kegagalan, dan selama jendela pemeliharaan yang direncanakan yang Anda konfigurasikan untuk sistem file Anda. Dengan sistem file Single-AZ, kegagalan sistem file mungkin tidak dapat dipulihkan dalam kasus yang jarang terjadi, seperti karena kegagalan beberapa komponen atau karena kegagalan non-anggun dari server file tunggal yang membuat sistem file dalam keadaan tidak konsisten, dalam hal ini Anda dapat memulihkan sistem file Anda dari cadangan terbaru.

Sistem file multi-AZ terdiri dari klaster server file Windows dengan ketersediaan tinggi yang tersebar di dua AZs (AZ pilihan dan AZ siaga), memanfaatkan teknologi Windows Server Failover Clustering (WSFC) dan satu set volume penyimpanan pada masing-masing dari keduanya. AZs Data direplikasi secara sinkron dalam setiap AZ individu dan di antara keduanya. AZs Sehubungan dengan penerapan Single-AZ, penerapan multi-AZ memberikan peningkatan daya tahan dengan mereplikasi data lebih lanjut AZs, dan meningkatkan ketersediaan selama pemeliharaan sistem yang direncanakan dan gangguan layanan yang tidak direncanakan dengan gagal secara otomatis ke AZ siaga. Hal ini memungkinkan Anda untuk terus mengakses data Anda, dan membantu melindungi data Anda dari kegagalan instans dan gangguan AZ.

Memilih tipe penyebaran sistem file Single-AZ atau Multi-AZ

Kami merekomendasikan penggunaan sistem file Multi-AZ untuk sebagian besar beban kerja produksi mengingat ketersediaan tinggi dan model daya tahan yang disediakannya. Penyebaran single-AZ dirancang sebagai solusi hemat biaya untuk beban kerja pengujian dan pengembangan, beban kerja produksi tertentu yang memiliki replikasi yang dibangun ke dalam lapisan aplikasi dan

tidak memerlukan redundansi tingkat penyimpanan tambahan, dan beban kerja produksi yang memiliki ketersediaan santai dan kebutuhan Recovery Point Objective (RPO). Beban kerja dengan ketersediaan yang santai dan kebutuhan RPO dapat mentolerir hilangnya ketersediaan sementara hingga 20 menit jika terjadi pemeliharaan sistem file yang direncanakan atau gangguan layanan yang tidak direncanakan dan, dalam kasus yang jarang terjadi, hilangnya pembaruan data sejak pencadangan terbaru.

Kami juga merekomendasikan untuk meninjau model ketersediaan untuk sistem file Anda dan memastikan bahwa beban kerja Anda tahan terhadap perilaku pemulihan yang diharapkan untuk jenis penerapan yang Anda pilih selama peristiwa seperti pemeliharaan sistem file, perubahan kapasitas throughput, dan gangguan layanan yang tidak direncanakan.

Dukungan fitur berdasarkan jenis penyebaran

Tabel berikut merangkum fitur yang didukung oleh FSx jenis penyebaran sistem file Windows File Server:

Jenis deployment	Penyimpanan SSD	Penyimpanan HDD	Namespace DFS	Replikasi DFS	Nama DNS kustom	Berbagi CA
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * Meskipun Anda dapat membuat pembagian yang tersedia secara berkelanjutan (CA) pada sistem file Single-AZ 2, Anda harus menggunakan saham CA pada sistem file multi-AZ untuk penerapan SQL Server HA.

Gagal dalam proses

Sistem file Multi-AZ secara otomatis melakukan failover dari server file pilihan ke server file siaga jika salah satu dari kondisi berikut terjadi:

- Terjadi gangguan Availability Zone.
- Server file pilihan menjadi tidak tersedia.
- Server file pilihan menjalani pemeliharaan yang direncanakan.

Ketika beralih dari satu server file ke server file yang lain, server file yang baru aktif secara otomatis mulai melayani semua permintaan baca dan tulis sistem file. Ketika sumber daya di subnet pilihan tersedia, Amazon FSx secara otomatis gagal kembali ke server file pilihan di subnet pilihan. Sebuah failover biasanya selesai dalam waktu kurang dari 30 detik sejak deteksi kegagalan pada server file aktif hingga promosi server file siaga ke status aktif. Proses failback ke konfigurasi Multi-AZ asli juga akan selesai dalam waktu kurang dari 30 detik, dan hanya terjadi setelah file server di subnet pilihan telah sepenuhnya pulih.

Selama periode singkat di mana sistem file Anda gagal dan gagal kembali, I/O mungkin dijeda dan metrik CloudWatch Amazon mungkin sementara tidak tersedia. Untuk sistem file multi-AZ, aktivitas baca dan tulis file apa pun yang terjadi selama failover dan failback perlu disinkronkan antara server file primer dan sekunder. Proses ini dapat memakan waktu hingga beberapa jam untuk sistem file dengan penyimpanan HDD, dan untuk beban kerja yang berat tulis dan berat IOPS. Sebaiknya uji dampak failover pada aplikasi Anda saat sistem file Anda berada di bawah beban yang lebih ringan.

Pengalaman failover pada klien Windows

Ketika gagal dari satu server file ke server lain, server file aktif baru secara otomatis mulai melayani semua permintaan baca dan tulis sistem file. Setelah sumber daya di subnet pilihan tersedia, Amazon FSx secara otomatis gagal kembali ke server file pilihan di subnet pilihan. Karena nama DNS sistem file tetap sama, failover bersifat transparan ke aplikasi Windows, yang melanjutkan operasi sistem file tanpa intervensi manual. Sebuah failover biasanya selesai dalam waktu kurang dari 30 detik sejak deteksi kegagalan pada server file aktif hingga promosi server file siaga ke status aktif. Proses failback ke konfigurasi Multi-AZ asli juga akan selesai dalam waktu kurang dari 30 detik, dan hanya terjadi setelah file server di subnet pilihan telah sepenuhnya pulih.

Pengalaman failover pada klien Linux

Klien Linux tidak mendukung failover berbasis DNS otomatis. Oleh karena itu, mereka tidak secara otomatis terhubung ke server file siaga selama terjadi failover. Mereka akan secara otomatis melanjutkan operasi sistem file setelah sistem file Multi-AZ telah beralih kembali ke server file yang ada di subnet pilihan.

Menguji failover pada sebuah sistem file

Anda dapat menguji failover sistem file Multi-AZ Anda dengan memodifikasi kapasitas throughput-nya. Saat Anda memodifikasi kapasitas throughput sistem file Anda, Amazon akan FSx mengganti server file sistem file. Sistem file multi-AZ secara otomatis gagal ke server sekunder sementara Amazon FSx menggantikan server file server pilihan terlebih dahulu. Kemudian sistem file secara otomatis gagal kembali ke server utama baru dan Amazon FSx menggantikan server file sekunder.

Anda dapat memantau kemajuan permintaan pembaruan kapasitas throughput di FSx konsol Amazon, CLI, dan API. Setelah pembaruan berhasil diselesaikan, sistem file Anda telah beralih ke server sekunder, dan beralih kembali ke server primer. Untuk informasi lebih lanjut tentang memodifikasi kapasitas throughput sistem file Anda dan memantau kemajuan permintaan, lihat Mengelola kapasitas throughput.

Sumber daya sistem file single-AZ dan Multi-AZ

Sistem file single-AZ dan multi-AZ mengkonsumsi subnet dan antarmuka jaringan elastis secara berbeda, seperti yang dijelaskan di bagian berikut.

Subnet

Saat Anda membuat virtual private cloud (VPC), itu mencakup semua Availability Zones (AZs) di. Wilayah AWS Availability Zone berada di lokasi yang berjauhan yang ditata sedemikian rupa agar terisolasi dari kegagalan Availability Zone lain. Setelah membuat VPC, Anda dapat menambahkan satu atau beberapa subnet di setiap Availability Zone. VPC default memiliki subnet di setiap Availability Zone. Subnet adalah serangkaian alamat IP di VPC. Subnet harus berada di Availability Zone tunggal.

FSx untuk Windows File Server Sistem file Single-AZ memerlukan satu subnet yang Anda tentukan saat pembuatan. Subnet yang Anda pilih mendefinisikan Availability Zone di mana sistem file akan dibuat.

Sistem file multi-AZ membutuhkan dua subnet, satu untuk server file pilihan dan satu untuk server file siaga. Dua subnet yang Anda pilih harus berada di Availability Zone yang berbeda dalam AWS Wilayah yang sama.

Untuk AWS aplikasi in-, kami menyarankan Anda meluncurkan klien Anda di Availability Zone yang sama dengan server file pilihan Anda untuk meminimalkan latensi.

Antarmuka jaringan elastis sistem file

Antarmuka jaringan elastis adalah komponen jaringan logis dalam VPC yang mewakili kartu jaringan virtual. Saat Anda membuat sistem FSx file Amazon, Amazon menyediakan FSx satu atau lebih elastic network interface di VPC yang Anda kaitkan dengan sistem file Anda. Elastic network interface memungkinkan klien untuk berkomunikasi dengan dan me-mount sistem file. Elastic network interface dianggap berada dalam lingkup layanan Amazon FSx, meskipun itu menjadi bagian dari VPC akun Anda. Sistem file Multi-AZ memiliki dua antarmuka jaringan elastis, satu untuk setiap server file. Sistem file Single-AZ memiliki satu antarmuka jaringan elastis.

> **Warning**
>
> Jangan memodifikasi atau menghapus antarmuka jaringan elastis yang terkait dengan sistem file Anda. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan koneksi hilang permanen antara VPC dan sistem file Anda.

Tabel berikut merangkum pemanfaatan sumber daya FSx untuk sistem file Windows File Server Single-AZ dan Multi-AZ:

Jenis deployment sistem file	Jumlah subnet	Jumlah antarmuka jaringan elastis	Jumlah alamat IP
Single-AZ 2	1	1	2
Single-AZ 1	1	1	1
Multi-AZ	2	2	4

Setelah sistem file dibuat, alamat IP-nya tidak berubah sampai sistem file dihapus.

Important

Amazon FSx tidak mendukung akses sistem file dari, atau mengekspos sistem file ke Internet publik. Jika alamat IP Elastic, yang merupakan alamat IP publik yang dapat dijangkau dari Internet, dilampirkan ke elastic network interface sistem file, Amazon FSx secara otomatis melepaskannya.

Bekerja dengan Microsoft Active Directory

Saat Anda membuat sistem file Windows File Server FSx untuk Windows, Anda menggabungkannya ke domain Active Directory untuk memberikan otentikasi pengguna dan kontrol akses tingkat file dan folder. Amazon FSx bekerja dengan Microsoft Active Directory untuk berintegrasi dengan lingkungan Microsoft Windows yang ada. Amazon FSx menyediakan dua opsi menggunakan sistem file Windows File Server Anda FSx dengan Active Directory: Menggunakan Amazon FSx dengan AWS Directory Service for Microsoft Active Directory danMenggunakan Microsoft Active Directory yang dikelola sendiri.

Direktori Aktif adalah directory service Microsoft yang digunakan untuk menyimpan informasi tentang objek pada jaringan dan membuat informasi ini mudah ditemukan dan digunakan oleh administrator dan pengguna. Objek ini biasanya mencakup sumber daya bersama seperti server file dan pengguna jaringan dan akun komputer.

Pengguna Anda kemudian dapat menggunakan identitas pengguna yang ada di Active Directory untuk mengautentikasi diri mereka sendiri dan mengakses sistem file Windows File Server FSx untuk Windows. Pengguna juga dapat menggunakan identitas mereka yang ada untuk mengontrol akses ke masing-masing file dan folder. Selain itu, Anda dapat memigrasikan file dan folder yang ada bersama dengan konfigurasi daftar kontrol akses keamanan (ACL) mereka ke Amazon FSx tanpa modifikasi apa pun.

> **Note**
>
> Amazon FSx mendukung Microsoft Azure Active Directory Domain Services, yang dapat Anda gabungkan ke Microsoft Azure Active Directory.

Setelah Anda membuat konfigurasi Direktori Aktif yang tergabung untuk sistem file, Anda dapat memperbarui hanya properti berikut:

- Kredensial pengguna layanan
- Alamat IP server DNS

Anda tidak dapat mengubah properti berikut untuk Microsoft AD yang bergabung setelah membuat sistem file:

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

Namun, Anda dapat membuat sistem file baru dari cadangan dan mengubah properti ini dalam konfigurasi integrasi Microsoft Active Directory sistem file baru. Untuk informasi selengkapnya, lihat Memulihkan backup ke sistem file baru.

> **Note**
>
> Amazon FSx tidak mendukung Konektor Direktori Aktif dan Direktori Aktif Sederhana.

Server File Windows Anda FSx dapat menjadi salah konfigurasi jika ada perubahan dalam konfigurasi Active Directory yang mengganggu koneksi ke sistem file Anda. Untuk mengembalikan sistem file Anda ke status Tersedia, pilih tombol Percobaan Pemulihan di FSx konsol Amazon, atau gunakan `StartMisconfiguredStateRecovery` perintah di Amazon FSx API atau konsol. Untuk informasi selengkapnya, lihat Sistem file dalam keadaan salah konfigurasi.

Topik

- Menggunakan Amazon FSx dengan AWS Directory Service for Microsoft Active Directory
- Menggunakan Microsoft Active Directory yang dikelola sendiri

Menggunakan Amazon FSx dengan AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) menyediakan direktori Active Directory aktual yang dikelola sepenuhnya, sangat tersedia di cloud. Anda dapat menggunakan direktori Active Directory ini dalam penerapan beban kerja Anda.

Jika organisasi Anda menggunakan AWS Managed Microsoft AD untuk mengelola identitas dan perangkat, kami sarankan Anda mengintegrasikan sistem FSx file Amazon Anda. AWS Managed Microsoft AD Dengan melakukan ini, Anda mendapatkan solusi turnkey menggunakan Amazon FSx dengan AWS Managed Microsoft AD. AWS menangani penyebaran, operasi, ketersediaan tinggi, keandalan, keamanan, dan integrasi yang mulus dari kedua layanan, memungkinkan Anda untuk fokus pada pengoperasian beban kerja Anda sendiri secara efektif.

Untuk menggunakan Amazon FSx dengan AWS Managed Microsoft AD pengaturan Anda, Anda dapat menggunakan FSx konsol Amazon. Saat Anda membuat sistem file Server File Windows baru FSx di konsol, pilih Direktori Aktif AWS Terkelola di bawah bagian Otentikasi Windows. Anda juga memilih direktori khusus yang ingin Anda gunakan. Untuk informasi selengkapnya, lihat Langkah 5. Buat sistem file Anda.

Organisasi Anda mungkin mengelola identitas dan perangkat di domain Direktori Aktif yang dikelola sendiri (on-premise atau di cloud). Jika demikian, Anda dapat bergabung dengan sistem FSx file Amazon langsung ke domain Active Directory yang sudah ada dan dikelola sendiri. Untuk informasi selengkapnya, lihat Menggunakan Microsoft Active Directory yang dikelola sendiri.

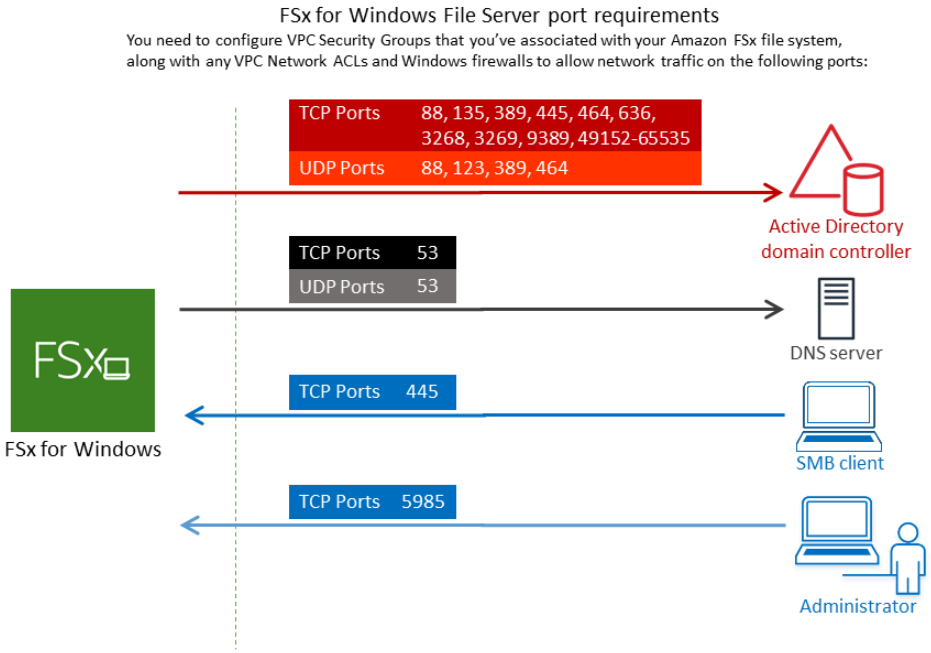
Selain itu, Anda juga dapat mengatur sistem Anda untuk mendapatkan manfaat dari model isolasi forest sumber daya. Dalam model ini, Anda mengisolasi sumber daya Anda, termasuk sistem FSx file Amazon Anda, ke dalam hutan Direktori Aktif yang terpisah dari tempat pengguna Anda berada.

> **Important**
>
> Untuk sistem file Single-AZ 2 dan semua sistem file Multi-AZ, nama domain yang memenuhi syarat (FQDN) Active Directory tidak dapat melebihi 47 karakter.

Prasyarat jaringan

Sebelum Anda membuat FSx sistem file Windows File Server yang bergabung dengan domain AWS Microsoft Managed Active Directory, pastikan bahwa Anda telah membuat dan mengatur konfigurasi jaringan berikut:

- Untuk Grup keamanan VPC, grup keamanan default untuk Amazon VPC Anda sudah ditambahkan ke sistem file Anda di konsol. Harap pastikan bahwa grup keamanan dan Jaringan VPC ACLs untuk subnet tempat Anda membuat sistem FSx file memungkinkan lalu lintas di port dan petunjuk yang ditunjukkan pada diagram berikut.



Tabel berikut mengidentifikasi peran masing-masing port.

Protokol	Port	Peran
TCP/UDP	53	Sisten Nama Doma (DNS)
TCP/UDP	88	Auten si Kerbe
TCP/UDP	464	Ubah/ Atur kata sandi

Protokol	Port	Peran
TCP/UDP	389	Protok Akses Direkt Ringa (LDAP
UDP	123	Protok Waktu Jaring (NTP)
TCP	135	Lingku n Komp Terdis busi/ Peme ta Titik Akhir (DCE/ EPMA P)
TCP	445	Pemb file SMB Layan Direkt

Protokol	Port	Peran
TCP	636	Protok Akses Direkt Ringa melalu TLS/ SSL (LDAP
TCP	3268	Katalo Globa Micros
TCP	3269	Katalo Globa Micros melalu SSL
TCP	5985	WinRI 2.0 (Peng aan Jarak Jauh Micros Windo
TCP	9389	Layan Web Micros AD DS, Power l

Protokol	Port	Peran
TCP	49152 - 65535	Port ephen untuk RPC

> **Important**
>
> Mengizinkan lalu lintas keluar pada TCP port 9389 diperlukan untuk single-AZ 2 dan semua deployment sistem file Multi-AZ.

> **Note**
>
> Jika Anda menggunakan jaringan VPC ACLs, Anda juga harus mengizinkan lalu lintas keluar pada port dinamis (49152-65535) dari sistem file Anda. FSx

- Jika Anda menghubungkan sistem FSx file Amazon Anda ke Direktori Aktif Microsoft AWS Terkelola di VPC atau akun yang berbeda, pastikan konektivitas antara VPC tersebut dan VPC Amazon tempat Anda ingin membuat sistem file. Untuk informasi selengkapnya, lihat Menggunakan Amazon FSx dengan AWS Managed Microsoft AD VPC atau akun yang berbeda.

> **Important**
>
> Sementara grup keamanan Amazon VPC mengharuskan port dibuka hanya ke arah lalu lintas jaringan dimulai, jaringan VPC ACLs memerlukan port untuk dibuka di kedua arah.

Gunakan alat Validasi FSx Jaringan Amazon untuk memvalidasi konektivitas ke pengontrol domain Direktori Aktif Anda.

Menggunakan model isolasi forest sumber daya

Anda bergabung dengan sistem file Anda ke pengaturan AWS Managed Microsoft AD . Anda kemudian membangun hubungan kepercayaan hutan satu arah antara AWS Managed Microsoft AD domain yang Anda buat dan domain Direktori Aktif yang dikelola sendiri yang ada. Untuk otentikasi

Windows di Amazon FSx, Anda hanya memerlukan kepercayaan hutan arah satu arah, di mana hutan AWS terkelola mempercayai hutan domain perusahaan.

Domain perusahaan Anda berperan sebagai domain tepercaya, dan domain AWS Directory Service terkelola berperan sebagai domain yang dipercaya. Permintaan autentikasi yang tervalidasi berpindah antar domain hanya dalam satu arah—yang memungkinkan akun di domain perusahaan Anda untuk melakukan autentikasi terhadap sumber daya yang dibagikan di domain terkelola. Dalam hal ini, Amazon hanya FSx berinteraksi dengan domain AWS terkelola. Dalam skenario otentikasi Kerberos, permintaan otentikasi yang berasal dari klien perusahaan divalidasi oleh domain perusahaan, yang kemudian merujuknya ke AWS Managed Microsoft AD, dan akhirnya klien menyajikan tiket layanannya ke sistem file Windows File Server Anda FSx untuk Windows. Untuk informasi lebih lanjut tentang kepercayaan, lihat posting Segala sesuatu yang ingin Anda ketahui tentang kepercayaan AWS Managed Microsoft AD di Blog AWS Keamanan.

Menguji konfigurasi Direktori Aktif Anda

Sebelum membuat sistem FSx file Amazon, kami sarankan Anda memvalidasi konektivitas ke pengontrol domain Active Directory menggunakan alat Validasi FSx Jaringan Amazon. Untuk informasi selengkapnya, lihat Memvalidasi konektivitas ke pengontrol domain Direktori Aktif Anda.

Sumber daya terkait berikut dapat membantu Anda saat Anda menggunakan AWS Directory Service for Microsoft Active Directory FSx untuk Windows File Server:

- Apa yang ada AWS Directory Service di Panduan AWS Directory Service Administrasi
- Buat Direktori Aktif AWS Terkelola Anda di Panduan AWS Directory Service Administrasi
- Kapan Membuat Hubungan Kepercayaan di Panduan Administrasi AWS Directory Service

Menggunakan Amazon FSx dengan AWS Managed Microsoft AD VPC atau akun yang berbeda

Anda dapat bergabung dengan sistem file Windows File Server Anda FSx ke AWS Managed Microsoft AD direktori yang ada di VPC berbeda dalam akun yang sama dengan menggunakan pengintip VPC. Anda juga dapat menggabungkan sistem file Anda ke AWS Managed Microsoft AD direktori yang ada di AWS akun yang berbeda dengan menggunakan berbagi direktori.

> **Note**
>
> Anda hanya dapat memilih AWS Managed Microsoft AD dalam yang Wilayah AWS sama dengan sistem file Anda. Jika Anda ingin menggunakan pengaturan peering VPC lintas wilayah, Anda harus menggunakan Microsoft Active Directory yang dikelola sendiri. Untuk informasi selengkapnya, lihat Menggunakan Microsoft Active Directory yang dikelola sendiri.

Alur kerja untuk menggabungkan sistem file Anda ke VPC yang berbeda melibatkan langkah-langkah berikut: AWS Managed Microsoft AD

1. Siapkan lingkungan jaringan Anda.
2. Bagikan direktori Anda.
3. Bergabunglah dengan sistem file Anda ke direktori bersama.

Untuk informasi selengkapnya, lihat Berbagi direktori Anda di Panduan AWS Directory Service Administrasi.

Untuk mengatur lingkungan jaringan Anda, Anda dapat menggunakan AWS Transit Gateway atau Amazon VPC dan membuat koneksi peering VPC. Selain itu, pastikan bahwa lalu lintas jaringan diperbolehkan di antara keduanya VPCs.

Gateway transit adalah hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya tentang menggunakan VPC transit gateway, lihat Memulai dengan Transit Gateway dalam Panduan Transit Gateway Amazon VPC.

Koneksi peering VPC adalah koneksi jaringan antara dua. VPCs Koneksi ini memungkinkan Anda untuk merutekan lalu lintas di antara mereka menggunakan alamat Internet Protocol pribadi versi 4 (IPv4) atau Internet Protocol versi 6 (IPv6). Anda dapat menggunakan VPC peering untuk terhubung VPCs dalam hal yang sama Wilayah AWS atau di antara keduanya. Wilayah AWS Untuk informasi selengkapnya tentang peering VPC, lihat Apa yang dimaksud dengan peering VPC? dalam Panduan Peering Amazon VPC.

Ada prasyarat lain ketika Anda bergabung dengan sistem file Anda ke AWS Managed Microsoft AD direktori di akun yang berbeda dari sistem file Anda. Anda juga perlu membagikan Microsoft Active Directory Anda dengan akun lain. Untuk melakukan ini, Anda dapat menggunakan fitur berbagi direktori Microsoft Active Directory yang AWS dikelola. Untuk mempelajari selengkapnya, lihat Berbagi direktori Anda di Panduan AWS Directory Service Administrasi.

Memvalidasi konektivitas ke pengontrol domain Direktori Aktif Anda

Sebelum Anda membuat sistem file FSx untuk Windows File Server yang bergabung dengan Active Directory Anda, gunakan alat Validasi Direktori FSx Aktif Amazon untuk memvalidasi konektivitas ke domain Active Directory Anda. Anda dapat menggunakan pengujian ini apakah Anda menggunakan FSx untuk Windows File Server dengan Direktori Aktif Microsoft AWS Terkelola atau dengan konfigurasi Direktori Aktif yang dikelola sendiri. Tes Konektivitas Jaringan Pengontrol Domain (Test- FSx ADController Connection) tidak menjalankan rangkaian lengkap pemeriksaan konektivitas jaringan terhadap setiap pengontrol domain di domain. Sebaliknya, gunakan tes ini untuk menjalankan validasi konektivitas jaringan terhadap serangkaian pengontrol domain tertentu.

Untuk memvalidasi konektivitas ke pengontrol domain Direktori Aktif

1. Luncurkan instance Amazon EC2 Windows di subnet yang sama dan dengan grup keamanan Amazon VPC yang sama yang akan Anda gunakan untuk sistem file Windows File Server FSx Anda. Untuk jenis deployment Multi-AZ, gunakan subnet untuk server file aktif pilihan.
2. Bergabunglah dengan instance EC2 Windows Anda ke Active Directory Anda. Untuk informasi lebih lanjut, lihat Menggabungkan Instans Windows Secara Manual dalam Panduan Administrasi AWS Directory Service .
3. Connect ke EC2 instans Anda. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
4. Buka PowerShell jendela Windows (menggunakan Run as Administrator) pada EC2 instance.

   Untuk menguji apakah modul Active Directory yang diperlukan untuk Windows PowerShell diinstal, gunakan perintah pengujian berikut.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Jika hasil pengujian menunjukkan kesalahan, instasl menggunakan perintah berikut.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. Unduh alat validasi jaringan menggunakan perintah berikut.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/WindowsGuide/
samples/AmazonFSxADValidation.zip" -OutFile "AmazonFSxADValidation.zip"
```

6. Buka file zip dengan menggunakan perintah berikut.

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. Tambahkan FSx ADValidation modul Amazon ke sesi saat ini.

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. Tetapkan nilai untuk alamat IP pengendali domain Direktori Aktif dan jalankan tes konektivitas menggunakan perintah berikut:

```
$ADControllerIp = '10.0.75.243'
$Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
```

9. Contoh berikut menunjukkan pengambilan output tes, dengan hasil tes konektivitas sukses.

```
PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
```

```
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

Contoh berikut menunjukkan menjalankan tes dan mendapatkan hasil yang gagal.

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs

PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        False
FailedTcpPorts                 {9389}


PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

```
Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx
```

> **Note**
>
> Sebagai alternatif dari prosedur di atas, Anda dapat menggunakan `AWSSupport-ValidateFSxWindowsADConfig` runbook untuk memvalidasi konfigurasi Active Directory yang dikelola sendiri. Untuk informasi selengkapnya, lihat AWSSupport-

`ValidateFSxWindowsADConfig` di referensi buku runbook Otomatisasi AWS Systems Manager .

Menggunakan Microsoft Active Directory yang dikelola sendiri

Jika organisasi Anda mengelola identitas dan perangkat menggunakan Active Directory yang dikelola sendiri di tempat atau di cloud, Anda dapat menggabungkan sistem file Windows File Server FSx untuk Windows ke domain Active Directory saat pembuatan.

Saat Anda menggabungkan sistem file ke Active Directory yang dikelola sendiri, sistem file Windows File Server Anda FSx berada di hutan Active Directory yang sama (wadah logis teratas dalam konfigurasi Active Directory yang berisi domain, pengguna, dan komputer) dan dalam domain Active Directory yang sama dengan pengguna dan sumber daya yang ada (termasuk server file yang ada).

> **Note**
>
> Anda dapat mengisolasi sumber daya Anda—termasuk sistem file FSx Amazon Anda—ke dalam hutan Direktori Aktif terpisah dari hutan tempat pengguna Anda tinggal. Untuk melakukannya, gabungkan sistem file Anda ke Direktori Aktif Microsoft AWS Terkelola dan buat hubungan kepercayaan hutan satu arah antara Direktori Aktif Microsoft AWS Terkelola yang Anda buat dan Direktori Aktif yang dikelola sendiri yang ada.

- Nama pengguna dan kata sandi untuk akun layanan di domain Active Directory Anda, yang FSx dapat digunakan Amazon untuk bergabung dengan sistem file ke domain Active Directory Anda.
- (Opsional) Unit Organisasi (OU) di domain Anda di mana Anda ingin sistem file Anda bergabung.
- (Opsional) Grup domain yang Anda ingin delegasikan otoritas untuk melakukan tindakan administratif pada sistem file Anda. Misalnya, grup domain ini mungkin mengelola berbagi file Windows, mengelola Daftar Kontrol Akses (ACLs) pada folder root sistem file, mengambil kepemilikan file dan folder, dan sebagainya. Jika Anda tidak menentukan grup ini, Amazon FSx mendelegasikan otoritas ini ke grup Admin Domain di domain Active Directory Anda secara default.

  > **Note**
  >
  > Nama grup domain yang Anda berikan harus unik di Direktori Aktif Anda. FSx untuk Windows File Server tidak akan membuat grup domain dalam keadaan berikut:

- Jika grup sudah ada dengan nama yang Anda tentukan
- Jika Anda tidak menentukan nama, dan grup bernama “Domain Admin” sudah ada di Active Directory Anda.

Untuk informasi selengkapnya, lihat Bergabung dengan sistem FSx file Amazon ke domain Microsoft Active Directory yang dikelola sendiri.

Topik

Prasyarat

Sebelum Anda bergabung dengan sistem file Windows File Server ke domain Microsoft Active Directory yang dikelola sendiri, tinjau prasyarat berikut untuk membantu memastikan bahwa Anda berhasil bergabung dengan sistem FSx file Amazon ke Active Directory yang dikelola sendiri. FSx

Konfigurasi lokal

Ini adalah prasyarat untuk Microsoft Active Directory yang dikelola sendiri, baik lokal maupun berbasis cloud, tempat Anda akan bergabung dengan sistem file Amazon. FSx

- Pengontrol domain Direktori Aktif:
  - Harus memiliki tingkat fungsional domain pada Windows Server 2008 R2 atau lebih tinggi.

  - Harus bisa ditulis.
  - Setidaknya salah satu pengontrol domain yang dapat dijangkau harus berupa Katalog Global hutan.
- Server DNS harus dapat menyelesaikan nama sebagai berikut:
  - Di domain tempat Anda bergabung dengan sistem file
  - Di domain akar hutan
- Server DNS dan alamat IP pengontrol domain Direktori Aktif harus memenuhi persyaratan berikut, yang bervariasi tergantung pada kapan sistem FSx file Amazon Anda dibuat:

Untuk sistem file yang dibuat sebelum 17 Desember 2020	Untuk sistem file yang dibuat setelah 17 Desember 2020
Alamat IP harus dalam kisaran alamat IP pribadi RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Alamat IP dapat berada dalam kisaran apa pun, kecuali: • Alamat IP yang bertentangan dengan alamat IP milik Amazon Web Services di Wilayah AWS mana sistem file berada. Untuk daftar alamat IP yang AWS dimiliki menurut wilayah, lihat rentang alamat AWS IP. • Alamat IP dalam rentang blok CIDR 198.19.0.0/16

  Jika Anda perlu mengakses sistem file Windows File Server FSx untuk Windows yang dibuat sebelum 17 Desember 2020 menggunakan rentang alamat IP non-pribadi, Anda dapat membuat sistem file baru dengan memulihkan cadangan sistem file. Untuk informasi selengkapnya, lihat Memulihkan cadangan ke sistem file baru.
- Nama domain Direktori Aktif yang dikelola sendiri harus memenuhi persyaratan berikut:
  - Nama domain tidak dalam format Single Label Domain (SLD). Amazon FSx tidak mendukung domain SLD.
  - Untuk Single-AZ 2 dan semua sistem file Multi-AZ, nama domain tidak boleh melebihi 47 karakter.
- Setiap situs Active Directory yang telah Anda tetapkan harus memenuhi prasyarat berikut:

- Subnet di VPC yang terkait dengan sistem file Anda harus didefinisikan di situs Active Directory.
- Tidak ada konflik antara subnet VPC dan subnet situs Active Directory mana pun.

Amazon FSx memerlukan konektivitas ke pengontrol domain atau situs Direktori Aktif yang telah Anda tentukan di lingkungan Direktori Aktif Anda. Amazon FSx akan mengabaikan pengontrol domain apa pun dengan TCP dan UDP yang diblokir pada port 389. Untuk pengontrol domain yang tersisa di Direktori Aktif Anda, pastikan bahwa mereka memenuhi persyaratan FSx konektivitas Amazon. Selain itu, verifikasi bahwa setiap perubahan pada akun layanan Anda disebarkan ke semua pengontrol domain ini.

> **Important**
>
> Jangan pindahkan objek komputer yang FSx dibuat Amazon di OU setelah sistem file Anda dibuat. Dengan melakukannya, sistem file Anda akan mengalami kesalahan konfigurasi.

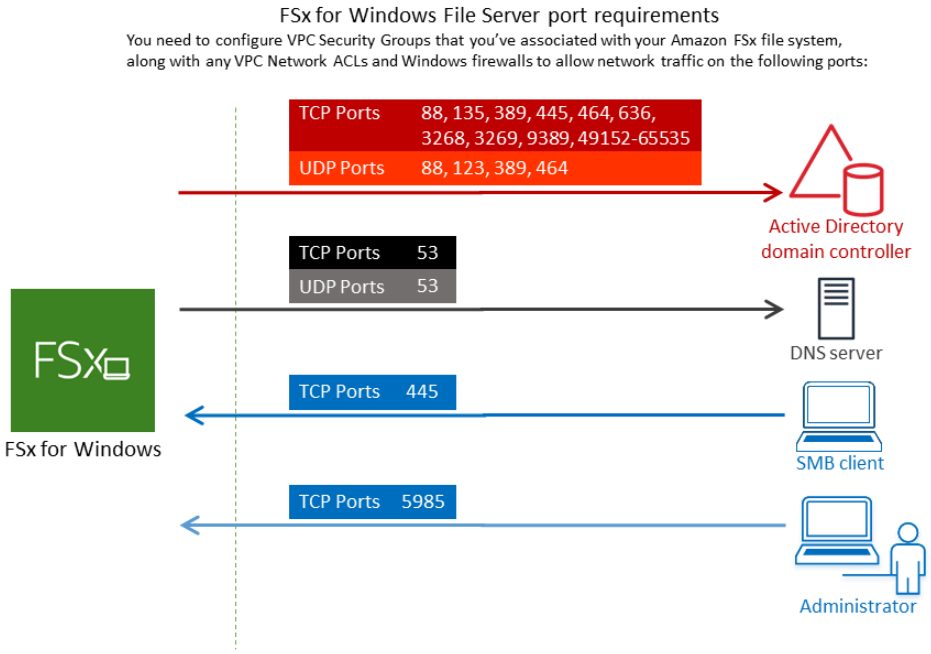
Anda dapat memvalidasi konfigurasi Direktori Aktif, termasuk menguji konektivitas beberapa pengontrol domain, menggunakan alat Validasi Direktori FSx Aktif Amazon. Untuk membatasi jumlah pengontrol domain yang memerlukan konektivitas, Anda juga dapat membangun hubungan kepercayaan antara pengontrol domain lokal dan pengontrol domain. AWS Managed Microsoft AD Untuk informasi selengkapnya, lihat Menggunakan model isolasi forest sumber daya.

> **Important**
>
> Amazon FSx hanya mendaftarkan catatan DNS untuk sistem file jika Anda menggunakan Microsoft DNS sebagai layanan DNS default. Jika Anda menggunakan DNS pihak ketiga, Anda perlu mengatur entri catatan DNS secara manual untuk sistem file Anda setelah Anda membuatnya.

Konfigurasi jaringan

Bagian ini menjelaskan persyaratan konfigurasi jaringan untuk menggabungkan sistem file ke Active Directory yang dikelola sendiri. Kami sangat menyarankan agar Anda menggunakan alat validasi Amazon FSx Active Directory untuk menguji pengaturan jaringan Anda sebelum mencoba menggabungkan sistem file Anda ke Active Directory yang dikelola sendiri.

- Pastikan bahwa aturan firewall Anda akan memungkinkan lalu lintas ICMP antara pengontrol domain Active Directory dan Amazon. FSx
- Konektivitas harus dikonfigurasi antara VPC Amazon tempat Anda ingin membuat sistem file dan Direktori Aktif yang dikelola sendiri. Anda dapat mengatur konektivitas ini menggunakan AWS Direct Connect, AWS Virtual Private Network, VPC peering, atau. AWS Transit Gateway
- Grup keamanan VPC default untuk VPC Amazon default Anda harus ditambahkan ke sistem file Anda menggunakan konsol Amazon. FSx Pastikan bahwa grup keamanan dan Jaringan VPC ACLs untuk subnet tempat Anda membuat sistem file memungkinkan lalu lintas di port dan ke arah yang ditunjukkan pada diagram berikut.



Tabel berikut mengidentifikasi protokol, port, dan perannya.

Protokol	Port	Peran
TCP/UDP	53	Sistem Nama Domain (DNS)
TCP/UDP	88	Autentikasi Kerberos
TCP/UDP	464	Ubah/atur kata sandi

Protokol	Port	Peran
TCP/UDP	389	Protokol Akses Direktori Ringan (LDAP)
UDP	123	Protokol Waktu Jaringan (NTP)
TCP	135	Komputasi TerdistribusiEnvironment/End Point Mapper (DCE/EPMAP)
TCP	445	Pembagian file SMB Layanan Direktori
TCP	636	Protokol Akses Direktori Ringan melalui TLS/SSL (LDAPS)
TCP	3268	Katalog Global Microsoft
TCP	3269	Katalog Global Microsoft melalui SSL
TCP	5985	WinRM 2.0 (Pengelolaan Jarak Jauh Microsoft Windows)
TCP	9389	Layanan Web Microsoft Active Directory DS, PowerShell **Important** Mengizinkan lalu lintas keluar pada port TCP 9389 diperlukan untuk penyebaran sistem file Single-AZ 2 dan Multi-AZ.
TCP	49152 - 65535	Port efemeral untuk RPC

Aturan lalu lintas ini juga perlu dicerminkan pada firewall yang berlaku untuk masing-masing pengontrol domain Active Directory, server DNS, klien, dan administrator. FSx FSx

> **Note**
>
> Jika Anda menggunakan jaringan VPC ACLs, Anda juga harus mengizinkan lalu lintas keluar pada port dinamis (49152-65535) dari sistem file Anda.

> **Important**
>
> Sementara grup keamanan Amazon VPC mengharuskan port dibuka hanya ke arah lalu lintas jaringan dimulai, sebagian besar firewall Windows dan ACLs jaringan VPC memerlukan port untuk dibuka di kedua arah.

Izin akun layanan

Anda harus memiliki akun layanan di Microsoft Active Directory yang dikelola sendiri dengan izin yang didelegasikan untuk menggabungkan objek komputer ke domain Active Directory yang dikelola sendiri. Akun layanan adalah akun pengguna di Direktori Aktif yang dikelola sendiri yang telah didelegasikan tugas-tugas tertentu.

Berikut ini adalah kumpulan izin minimum yang harus didelegasikan ke akun FSx layanan Amazon di OU tempat Anda bergabung dengan sistem file.

- Jika menggunakan Delegate Control di Active Directory User and Computers MMC:
  - Atur ulang kata sandi
  - Baca dan tulis Pembatasan Akun
  - Penulisan tervalidasi ke nama host DNS
  - Penulisan tervalidasi ke nama utama layanan
- Jika menggunakan Fitur Lanjutan di Pengguna Direktori Aktif dan Komputer MMC:
  - Ubah izin
  - Buat objek komputer
  - Hapus objek komputer

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.

Untuk informasi selengkapnya tentang menyetel izin yang diperlukan, lihatMendelegasikan izin ke akun atau grup FSx layanan Amazon.

Praktik terbaik saat menggunakan Active Directory yang dikelola sendiri

Kami menyarankan Anda mengikuti praktik terbaik ini saat bergabung dengan sistem file Amazon FSx untuk Windows File Server ke Microsoft Active Directory yang dikelola sendiri. Praktik terbaik ini akan membantu Anda dalam menjaga ketersediaan sistem file Anda yang berkelanjutan dan tidak terganggu.

Gunakan akun layanan terpisah untuk Amazon FSx

Gunakan akun layanan terpisah untuk mendelegasikan hak istimewa yang diperlukan FSx bagi Amazon agar sepenuhnya mengelola sistem file yang digabungkan ke Direktori Aktif yang dikelola sendiri. Kami tidak menyarankan menggunakan Admin Domain untuk tujuan ini.

Menggunakan grup Active Directory

Gunakan grup Active Directory untuk mengelola izin dan konfigurasi Direktori Aktif yang terkait dengan akun FSx layanan Amazon.

Memisahkan Unit Organisasi (OU)

Untuk mempermudah menemukan dan mengelola objek FSx komputer Amazon Anda, kami sarankan Anda memisahkan Unit Organisasi (OU) yang Anda gunakan untuk sistem file Windows File Server Anda FSx dari masalah pengontrol domain lainnya.

Pertahankan konfigurasi Active Directory up-to-date

Sangat penting bahwa Anda menyimpan konfigurasi Active Directory sistem file Anda up-to-date dengan perubahan apa pun. Misalnya, jika Active Directory yang dikelola sendiri menggunakan kebijakan pengaturan ulang kata sandi berbasis waktu, segera setelah kata sandi disetel ulang, pastikan untuk memperbarui kata sandi akun layanan pada sistem file Anda. Untuk informasi selengkapnya, lihat Memperbarui konfigurasi Direktori Aktif yang dikelola sendiri.

Mengubah akun FSx layanan Amazon

Jika Anda memperbarui sistem file Anda dengan akun layanan baru, itu harus memiliki izin dan hak istimewa yang diperlukan untuk bergabung dengan Direktori Aktif Anda dan memiliki izin kontrol penuh untuk objek komputer yang ada yang terkait dengan sistem file. Untuk informasi selengkapnya, lihat Mengubah akun FSx layanan Amazon.

Tetapkan subnet ke satu situs Microsoft Active Directory

Jika lingkungan Direktori Aktif Anda memiliki sejumlah besar pengontrol domain, gunakan Situs dan Layanan Direktori Aktif untuk menetapkan subnet yang digunakan oleh sistem FSx file Amazon Anda ke satu situs Direktori Aktif dengan ketersediaan dan keandalan tertinggi. Pastikan bahwa grup keamanan VPC, ACL jaringan VPC, aturan firewall Windows pada Anda DCs, dan kontrol perutean jaringan lainnya yang Anda miliki di infrastruktur Direktori Aktif memungkinkan komunikasi dari Amazon pada port yang diperlukan. FSx Ini memungkinkan Windows untuk kembali ke pengontrol domain lain jika tidak dapat menggunakan situs Direktori Aktif yang ditetapkan. Untuk informasi selengkapnya, lihat Kontrol akses sistem file dengan Amazon VPC.

Gunakan aturan grup keamanan untuk membatasi lalu lintas

Gunakan aturan grup keamanan untuk menerapkan prinsip hak istimewa paling sedikit di cloud pribadi virtual (VPC) Anda. Anda dapat membatasi jenis lalu lintas jaringan masuk dan keluar yang diizinkan untuk file Anda menggunakan aturan grup keamanan VPC. Misalnya, kami sarankan hanya mengizinkan lalu lintas keluar ke pengontrol domain Active Directory yang dikelola sendiri atau ke dalam subnet atau grup keamanan yang Anda gunakan. Untuk informasi selengkapnya, lihat Kontrol akses sistem file dengan Amazon VPC.

Jangan pindahkan objek komputer yang dibuat Amazon FSx

> **Important**
>
> Jangan pindahkan objek komputer yang FSx dibuat Amazon di OU setelah sistem file Anda dibuat. Dengan melakukannya, sistem file Anda akan mengalami kesalahan konfigurasi.

Validasi konfigurasi Direktori Aktif Anda

Sebelum mencoba bergabung dengan sistem file Windows File Server ke Active Directory Anda, kami sangat menyarankan Anda memvalidasi konfigurasi Active Directory menggunakan alat Validasi Direktori FSx Aktif Amazon. FSx

Akun FSx layanan Amazon

Sistem FSx file Amazon yang digabungkan ke Direktori Aktif yang dikelola sendiri memerlukan akun layanan yang valid sepanjang masa pakainya. Amazon FSx menggunakan akun layanan untuk mengelola sistem file Anda sepenuhnya dan melakukan tugas administratif yang memerlukan

pemutusan dan penggabungan kembali objek komputer ke domain Direktori Aktif Anda. Tugas-tugas ini termasuk mengganti server file yang gagal dan menambal perangkat lunak Microsoft Windows Server. FSx Agar Amazon dapat melakukan tugas-tugas ini, akun FSx layanan Amazon harus memiliki, setidaknya, serangkaian izin yang dijelaskan dalam Izin akun layanan didelegasikan kepadanya.

Meskipun anggota grup Admin Domain memiliki hak istimewa yang cukup untuk melakukan tugas ini, kami sangat menyarankan Anda menggunakan akun layanan terpisah untuk mendelegasikan hak istimewa yang diperlukan ke Amazon. FSx

Untuk informasi selengkapnya tentang cara mendelegasikan hak istimewa menggunakan fitur Kontrol Delegasi atau Fitur Lanjutan di snap-in Active Directory User and Computers MMC, lihat. Mendelegasikan izin ke akun atau grup FSx layanan Amazon

Jika Anda memperbarui sistem file Anda dengan akun layanan baru, akun layanan baru harus memiliki izin dan hak istimewa yang diperlukan untuk bergabung dengan Direktori Aktif Anda dan memiliki izin kontrol penuh untuk objek komputer yang ada yang terkait dengan sistem file. Untuk informasi selengkapnya, lihat Mengubah akun FSx layanan Amazon.

Mendelegasikan izin ke akun atau grup FSx layanan Amazon

Akun FSx layanan Amazon atau grup admin harus memiliki hak istimewa yang diperlukan FSx untuk bergabung dengan sistem file Windows File Server ke domain Active Directory yang dikelola sendiri. Untuk mendelegasikan izin ini, Anda dapat menggunakan Kontrol Delegasi atau Fitur Lanjutan di Active Directory User and Computers MMC snap-in, seperti yang dijelaskan dalam prosedur berikut.

Untuk menetapkan izin menggunakan Delegate Control

Untuk menetapkan izin ke akun layanan atau grup menggunakan Kontrol Delegasi

1. Masuk ke sistem Anda sebagai administrator domain untuk domain Active Directory Anda.
2. Buka MMC snap-in Pengguna Direktori Aktif dan Komputer.
3. Dalam panel tugas, perluas simpul domain.
4. Temukan dan buka menu konteks (klik kanan) untuk OU yang ingin Anda ubah, lalu pilih Delegasikan Kontrol.
5. Pada halaman Delegasi Control Wizard, pilih Selanjutnya.
6. Pilih Tambah untuk menambahkan nama akun atau grup FSx layanan Amazon Anda, lalu pilih Berikutnya.

7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer.
9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Berikutnya.
10. Untuk Izin, pilih:

    - Setel Ulang Kata Sandi
    - Baca dan tulis Pembatasan Akun
    - Menulis tervalidasi ke nama host DNS
    - Menulis tervalidasi ke nama utama layanan
11. Pilih Selanjutnya, dan kemudian pilih Selesai.
12. Tutup snap-in Active Directory User and Computers MMC.

Untuk menetapkan izin menggunakan Fitur Lanjutan

1. Masuk ke sistem Anda sebagai administrator domain untuk domain Active Directory Anda.
2. Buka MMC snap-in Pengguna Direktori Aktif dan Komputer.
3. Pilih Lihat dari bilah menu dan pastikan Fitur Lanjutan diaktifkan (tanda centang akan muncul di sebelahnya jika fitur diaktifkan).
4. Dalam panel tugas, perluas simpul domain.
5. Cari dan buka (klik kanan) menu konteks untuk OU yang ingin Anda ubah, lalu pilih Properties.
6. Di panel OU Properties, pilih tab Security.
7. Di tab Keamanan, pilih Advanced. Kemudian pilih Tambah.
8. Pada halaman Entri Izin, pilih Pilih prinsipal dan masukkan nama akun atau grup FSx layanan Amazon Anda. Untuk Berlaku untuk:, pilih Objek Ini dan semua Komputer Keturunan. Pastikan bahwa yang berikut ini dipilih:

    - Ubah izin
    - Buat Objek Komputer
    - Hapus Objek Komputer
9. Pilih Terapkan, lalu pilih OK.
10. Tutup snap-in Active Directory User and Computers MMC.

Memvalidasi konfigurasi Direktori Aktif Anda

Sebelum Anda membuat sistem file FSx untuk Windows File Server yang bergabung dengan Active Directory Anda, kami sarankan Anda memvalidasi konfigurasi Active Directory menggunakan alat Validasi Direktori FSx Aktif Amazon. Perhatikan bahwa konektivitas internet keluar diperlukan untuk berhasil memvalidasi konfigurasi Active Directory.

Untuk memvalidasi konfigurasi Direktori Aktif Anda

1. Luncurkan instans Amazon EC2 Windows di subnet yang sama dan dengan grup keamanan Amazon VPC yang sama yang Anda gunakan untuk sistem file Server File Windows FSx Anda. Pastikan EC2 instans Anda memiliki izin `AmazonEC2ReadOnlyAccess` IAM yang diperlukan. Anda dapat memvalidasi izin peran EC2 instance menggunakan simulator kebijakan IAM. Untuk informasi selengkapnya, lihat Menguji Kebijakan IAM dengan Simulator Kebijakan IAM di Panduan Pengguna IAM.
2. Bergabunglah dengan instance EC2 Windows Anda ke Active Directory Anda. Untuk informasi lebih lanjut, lihat Menggabungkan Instans Windows Secara Manual dalam Panduan Administrasi AWS Directory Service .
3. Connect ke EC2 instans Anda. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
4. Buka PowerShell jendela Windows (menggunakan Run as Administrator) pada EC2 instance.

   Untuk menguji apakah modul Active Directory yang diperlukan untuk Windows PowerShell diinstal, gunakan perintah pengujian berikut.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Jika hasil pengujian menunjukkan kesalahan, instasl menggunakan perintah berikut.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. Unduh alat validasi jaringan menggunakan perintah berikut.

   ```
   PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/WindowsGuide/
   samples/AmazonFSxADValidation.zip" -OutFile "AmazonFSxADValidation.zip"
   ```

6. Buka file zip dengan menggunakan perintah berikut.

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. Tambahkan `AmazonFSxADValidation` modul ke sesi saat ini.

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. Tetapkan parameter yang diperlukan dengan menggantikan perintah berikut:

   - Nama domain Direktori Aktif (*DOMAINNAME.COM*)
   - Siapkan `$Credential` objek untuk kata sandi akun layanan menggunakan salah satu opsi berikut.
     - Untuk membuat objek kredensial secara interaktif, gunakan perintah berikut.

       ```
       $Credential = Get-Credential
       ```

     - Untuk menghasilkan objek kredensi menggunakan AWS Secrets Manager sumber daya, gunakan perintah berikut.

       ```
       $Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
        $AdminSecret).SecretString
       $Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
        $Secret.Password -AsPlainText -Force)))
       ```

   - Alamat IP server DNS (*IP_ADDRESS_1*,*IP_ADDRESS_2*)
   - Subnet ID (s) untuk subnet di mana Anda berencana untuk membuat sistem FSx file Amazon Anda (*SUBNET_1SUBNET_2*, misalnya,`subnet-04431191671ac0d19`).

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')
```

```
    Credential = $Credential
}
```

9. (Opsional) Tetapkan Unit Organisasi, grup Administrator Delegasi DomainControllersMaxCount, dan aktifkan validasi izin akun layanan dengan mengikuti instruksi dalam `README.md` file yang disertakan sebelum menjalankan alat validasi.

> **Note**
>
> `Domain Admins`Grup ini memiliki nama yang berbeda jika sistem operasinya tidak dalam bahasa Inggris. Misalnya, grup ini dinamai `Administrateurs du domaine` dalam versi OS Prancis. Jika Anda tidak menentukan nilai, nama `Domain Admins` grup default digunakan dan pembuatan sistem file gagal.

10. Menjalankan alat validasi dengan menggunakan perintah ini.

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. Berikut ini adalah contoh hasil pengujian yang berhasil.

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

Berikut ini adalah contoh dari hasil pengujian dengan kesalahan.

```
Test 1 - Validate EC2 Subnets ...
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...
```

```
Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                          Value
----                          -----
SubnetsInSeparateAdSites      {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}



Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                          Value
----                          -----
SubnetsInSeparateAdSites      {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}


PS C:\AmazonFSxADValidation> $Result.Warnings.Count
```

```
0
```

Jika Anda menerima peringatan atau kesalahan ketika Anda menjalankan alat validasi, lihat panduan pemecahan masalah yang disertakan dalam paket alat validasi (`TROUBLESHOOTING.md`) dan Memecahkan Masalah Amazon FSx.

Bergabung dengan sistem FSx file Amazon ke domain Microsoft Active Directory yang dikelola sendiri

Saat Anda membuat sistem file Server File Windows baru FSx , Anda dapat mengonfigurasi integrasi Microsoft Active Directory sehingga bergabung dengan domain Microsoft Active Directory yang dikelola sendiri. Untuk melakukannya, berikan informasi berikut untuk Microsoft Active Directory Anda:

- Nama domain (FQDN) yang sepenuhnya memenuhi syarat dari direktori Microsoft Active Directory lokal Anda.

> **Note**
>
> Amazon FSx saat ini tidak mendukung domain Single Label Domain (SLD).

- Alamat IP dari server DNS untuk domain Anda.
- Kredensi untuk akun layanan di domain Microsoft Active Directory lokal Anda. Amazon FSx menggunakan kredensi ini untuk bergabung ke Active Directory yang dikelola sendiri.

Anda juga dapat menentukan pilihan berikut:

- Unit Organisasi (OU) tertentu dalam domain yang Anda inginkan untuk bergabung dengan sistem FSx file Amazon Anda.
- Nama grup domain yang anggotanya diberikan hak administratif untuk sistem FSx file Amazon. Nama grup domain yang Anda berikan harus unik di Direktori Aktif Anda.

Setelah Anda menentukan informasi ini, Amazon FSx menggabungkan sistem file baru Anda ke domain Active Directory yang dikelola sendiri menggunakan akun layanan yang Anda berikan.

> **Important**
>
> Amazon FSx hanya mendaftarkan catatan DNS untuk sistem file jika domain Active Directory tempat Anda bergabung menggunakan Microsoft DNS sebagai DNS default. Jika Anda menggunakan DNS pihak ketiga, Anda perlu mengatur entri DNS secara manual untuk sistem FSx file Amazon Anda setelah Anda membuat sistem file Anda. Untuk informasi lebih lanjut tentang memilih alamat IP yang benar untuk digunakan untuk sistem file, lihat Mendapatkan alamat IP sistem file yang benar untuk digunakan untuk entri DNS manual.

Sebelum Anda mulai

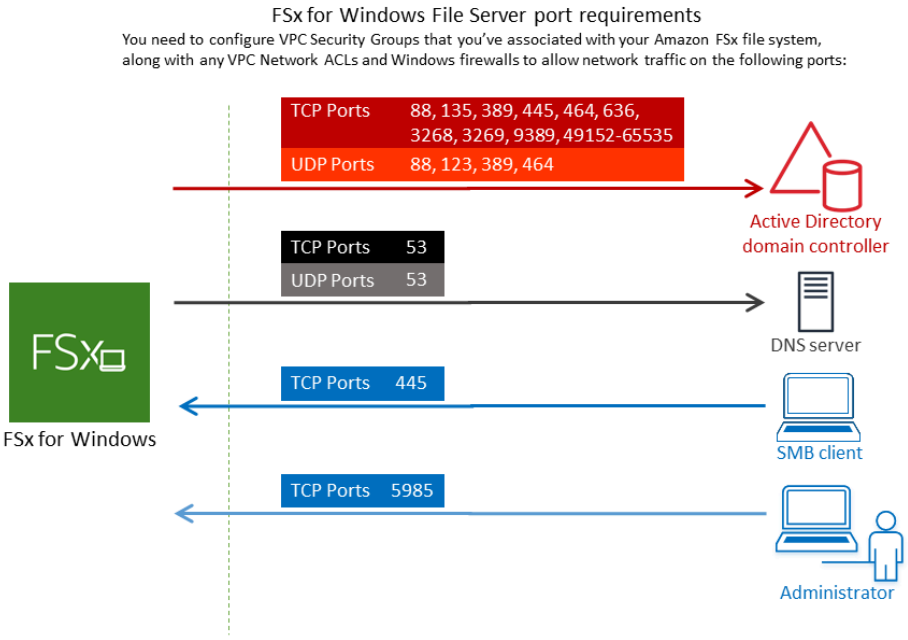
Pastikan bahwa Anda telah menyelesaikan Prasyarat yang dirinci di Menggunakan Microsoft Active Directory yang dikelola sendiri.

FSx Untuk membuat sistem file Windows File Server yang digabungkan ke Active Directory (Console) yang dikelola sendiri

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Pada dasbor, pilih Buat sistem file untuk memulai wizard pembuatan sistem file.
3. Pilih FSx untuk Windows File Server dan kemudian pilih Berikutnya. Halaman Buat sistem file muncul.
4. Berikan nama untuk sistem file Anda. Anda dapat menggunakan maksimum 256 huruf Unicode, spasi, dan angka, serta karakter khusus + - =. _ : /
5. Untuk Kapasitas penyimpanan, masukkan kapasitas penyimpanan sistem file Anda, dalam GiB. Jika Anda menggunakan penyimpanan SSD, masukkan bilangan bulat berapa pun dalam kisaran 32–65,536. Jika Anda menggunakan penyimpanan HDD, masukkan bilangan bulat berapa pun dalam kisaran 2,000–65,536. Anda dapat meningkatkan jumlah kapasitas penyimpanan sesuai kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan.
6. Pertahankan Kapasitas throughput pada pengaturan default-nya. Kapasitas throughput adalah kecepatan berkelanjutan di mana server file yang menyimpan sistem file Anda dapat melayani data. Pengaturan Kapasitas throughput yang disarankan didasarkan pada jumlah kapasitas penyimpanan yang Anda pilih. Jika Anda membutuhkan lebih dari kapasitas throughput yang disarankan, pilih Tentukan kapasitas throughput, dan kemudian pilih nilai. Untuk informasi selengkapnya, lihat FSx untuk kinerja Windows File Server.

Anda dapat mengubah kapasitas throughput sesuai kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

7. Pilih VPC yang ingin Anda kaitkan dengan sistem file Anda. Untuk tujuan latihan memulai ini, pilih VPC yang sama seperti untuk AWS Directory Service direktori dan instans Amazon EC2 Anda.
8. Pilih nilai untuk Availability Zone dan untuk Subnet.
9. Untuk Grup keamanan VPC, grup keamanan default untuk Amazon VPC Anda sudah ditambahkan ke sistem file Anda di konsol. Harap pastikan bahwa grup keamanan dan Jaringan VPC ACLs untuk subnet tempat Anda membuat sistem FSx file memungkinkan lalu lintas di port dan petunjuk yang ditunjukkan pada diagram berikut.



Tabel berikut mengidentifikasi peran masing-masing port.

Protokol	Port	Peran
TCP/UDP	53	Sisten Nama

Protokol	Port	Peran
		Doma (DNS)
TCP/UDP	88	Auten si Kerbe
TCP/UDP	464	Ubah/ Atur kata sandi
TCP/UDP	389	Protok Akses Direkt Ringa (LDAP
UDP	123	Protok Waktu Jaring (NTP)
TCP	135	Lingku n Komp Terdis busi/ Peme ta Titik Akhir (DCE/ EPMA P)

Protokol	Port	Peran
TCP	445	Pemb file SMB Layan Direkt
TCP	636	Protok Akses Direkt Ringa melalu TLS/ SSL (LDAP
TCP	3268	Katalo Globa Micros
TCP	3269	Katalo Globa Micros melalu SSL
TCP	5985	WinRI 2.0 (Peng aan Jarak Jauh Micros Windo

Protokol	Port	Peran
TCP	9389	Layan Web Micros Active Direct DS, Powe l
TCP	49152 - 65535	Port ephen untuk RPC

Important

Mengizinkan lalu lintas keluar pada TCP port 9389 diperlukan untuk single-AZ 2 dan semua deployment sistem file Multi-AZ.

Note

Jika Anda menggunakan jaringan VPC ACLs, Anda juga harus mengizinkan lalu lintas keluar pada port dinamis (49152-65535) dari sistem file Anda. FSx

- Aturan keluar untuk mengizinkan semua lalu lintas ke alamat IP yang terkait dengan server DNS dan pengontrol domain untuk domain Microsoft Active Directory yang dikelola sendiri. Untuk informasi selengkapnya, lihat Dokumentasi Microsoft tentang mengkonfigurasi firewall Anda untuk komunikasi Direktori Aktif.
- Pastikan bahwa aturan lalu lintas ini juga dicerminkan pada firewall yang berlaku untuk masing-masing pengontrol domain Active Directory, server DNS, klien, dan administrator. FSx FSx

> **Note**
>
> Jika Anda memiliki situs Direktori Aktif yang ditentukan, Anda harus memastikan bahwa subnet di VPC yang terkait dengan sistem file FSx Amazon Anda didefinisikan di situs Direktori Aktif, dan tidak ada konflik antara subnet di VPC Anda dan subnet di situs Anda yang lain. Anda dapat melihat dan mengubah pengaturan ini menggunakan Situs Direktori Aktif dan snap-in MMC Layanan.

> **Important**
>
> Sementara grup keamanan Amazon VPC mengharuskan port dibuka hanya ke arah lalu lintas jaringan dimulai, sebagian besar firewall Windows dan ACLs jaringan VPC memerlukan port untuk dibuka di kedua arah.

10. Untuk Autentikasi Windows, pilih Direktori Aktif Microsoft dikelola sendiri.
11. Masukkan nilai untuk nama domain yang sepenuhnya memenuhi syarat untuk direktori Microsoft Active Directory yang dikelola sendiri.

> **Note**
>
> Nama domain tidak boleh dalam format Single Label Domain (SLD). Amazon FSx saat ini tidak mendukung domain SLD.

> **Important**
>
> Untuk Single-AZ 2 dan semua sistem file Multi-AZ, nama domain Direktori Aktif tidak boleh melebihi 47 karakter.

12. Masukkan nilai untuk Unit Organisasi untuk direktori Microsoft Active Directory yang dikelola sendiri.

> **Note**
>
> Pastikan bahwa akun layanan yang Anda berikan memiliki izin yang didelegasikan ke OU yang Anda tentukan di sini atau ke default OU jika Anda tidak menentukannya.

13. Masukkan setidaknya satu, dan tidak lebih dari dua, nilai untuk Alamat IP Server DNS untuk direktori Microsoft Active Directory yang dikelola sendiri.
14. Masukkan nilai string untuk nama pengguna akun Layanan untuk akun di domain Direktori Aktif yang dikelola sendiri, seperti`ServiceAcct`. Amazon FSx menggunakan nama pengguna ini untuk bergabung ke domain Microsoft Active Directory Anda.

> **Important**
>
> JANGAN sertakan prefiks domain (`corp.com\ServiceAcct`) atau sufiks domain (`ServiceAcct@corp.com`) saat memasukkan Nama pengguna akun layanan. JANGAN menggunakan Nama yang Dibedakan (DN) saat memasukkan Nama pengguna akun layanan (`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

15. Masukkan nilai untuk kata sandi akun Layanan untuk akun di domain Direktori Aktif yang dikelola sendiri. Amazon FSx menggunakan kata sandi ini untuk bergabung ke domain Microsoft Active Directory Anda.
16. Masukkan kembali kata sandi untuk mengonfirmasinya dalam Konfirmasi kata sandi.
17. Untuk grup administrator sistem file yang didelegasikan, tentukan `Domain Admins` grup atau grup administrator sistem file yang didelegasikan khusus (jika Anda telah membuatnya). Grup yang Anda tentukan harus memiliki wewenang yang didelegasikan untuk melakukan tugas administratif pada sistem file Anda. Jika Anda tidak memberikan nilai, Amazon FSx menggunakan `Domain Admins` grup Builtin. Perhatikan bahwa Amazon FSx tidak mendukung memiliki `Delegated file system administrators group` (baik `Domain Admins` grup atau grup kustom yang Anda tentukan) yang terletak di wadah bawaan.

> **Important**
>
> Jika Anda tidak menyediakan grup administrator sistem file yang didelegasikan, Amazon secara default FSx mencoba menggunakan **`Domain Admins`** grup bawaan di domain Active Directory Anda. Jika nama grup Builtin ini telah diubah atau jika Anda

menggunakan grup yang berbeda untuk administrasi domain, Anda harus memberikan nama tersebut untuk grup di sini.

> **Important**
>
> JANGAN menyertakan awalan domain (corp.com\ FSx Admins) atau akhiran domain (FSxAdmins@corp.com) saat memberikan parameter nama grup.
> JANGAN menggunakan Nama yang Dibedakan (DN) untuk grup. Contoh nama yang dibedakan adalah CN = FSx Admin, OU = Contoh, DC = Corp, DC = COM.

FSx Untuk membuat sistem file Windows File Server bergabung dengan Active Directory ()AWS CLI yang dikelola sendiri

Contoh berikut membuat FSx untuk sistem file Windows File Server dengan `SelfManagedActiveDirectoryConfiguration` di `us-east-2` Availability Zone.

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> Jangan pindahkan objek komputer yang FSx dibuat Amazon di OU setelah sistem file Anda dibuat. Dengan melakukannya, sistem file Anda akan mengalami kesalahan konfigurasi.

Mendapatkan alamat IP sistem file yang benar untuk digunakan untuk entri DNS manual

Amazon FSx hanya mendaftarkan catatan DNS untuk sistem file jika Anda menggunakan Microsoft DNS sebagai layanan DNS default. Jika Anda menggunakan DNS pihak ketiga, Anda perlu mengatur entri DNS secara manual untuk sistem file Amazon FSx Anda. Bagian ini menjelaskan cara mendapatkan alamat IP sistem file yang benar untuk digunakan jika Anda harus secara manual menambahkan sistem file ke DNS Anda. Perhatikan bahwa setelah sistem file dibuat, alamat IP-nya tidak berubah sampai sistem file dihapus.

Cara mendapatkan alamat IP sistem file yang digunakan untuk entri DNS A

1. Di dalam https://console.aws.amazon.com/fsx/, pilih sistem file yang ingin Anda dapatkan alamat IP untuk menampilkan halaman detail sistem file.
2. Di tab Jaringan & keamanan lakukan salah satu hal berikut:

   - Untuk sistem file Single-AZ 1:
     - Di panel Subnet, pilih elastic network interface yang ditampilkan di bawah Network interface untuk membuka halaman Network Interfaces di konsol Amazon EC2 .
     - Alamat IP untuk sistem file Single-AZ 1 yang akan digunakan ditampilkan di kolom IPv4 IP pribadi Primer.
   - Untuk sistem file Single-AZ 2 atau Multi-AZ:
     - Di panel subnet Preferred, pilih elastic network interface yang ditampilkan di bawah Network interface untuk membuka halaman Network Interfaces di konsol Amazon EC2 .
     - Alamat IP untuk subnet pilihan untuk digunakan ditampilkan di kolom IPv4 IP pribadi Sekunder.
     - Di panel subnet Amazon FSx Standby, pilih elastic network interface yang ditampilkan di bawah Network interface untuk membuka halaman Network Interfaces di konsol Amazon. EC2
     - Alamat IP untuk subnet siaga yang akan digunakan ditampilkan di kolom IPv4 IP pribadi Sekunder.

> **Note**
>
> Jika Anda perlu mengatur entri DNS untuk Windows Remote PowerShell Endpoint untuk sistem file Single-AZ 2 atau Multi-AZ, Anda harus menggunakan IPv4 alamat pribadi Primer untuk antarmuka elastic network untuk subnet Preferred Anda. Untuk informasi selengkapnya, lihat Menggunakan Amazon FSx CLI untuk PowerShell.

Memperbarui konfigurasi Direktori Aktif yang dikelola sendiri

Untuk membantu memastikan ketersediaan sistem FSx file Amazon yang berkelanjutan dan tidak terganggu, Anda harus memperbarui konfigurasi Active Directory sistem file ketika salah satu properti Active Directory berikut berubah:

- Alamat IP server DNS
- Kredensi akun layanan dari Active Directory yang dikelola sendiri

Saat Anda memperbarui konfigurasi Direktori Aktif yang dikelola sendiri untuk sistem FSx file Amazon Anda, status sistem file Anda beralih dari Tersedia ke Pembaruan saat pembaruan diterapkan. Pastikan bahwa keadaan beralih kembali ke Tersedia setelah pembaruan diterapkan — perhatikan bahwa pembaruan dapat memakan waktu hingga beberapa menit untuk diselesaikan. Untuk informasi selengkapnya, lihat Pembaruan Direktori Aktif yang dikelola sendiri.

Jika ada masalah dengan konfigurasi Direktori Aktif yang dikelola sendiri yang diperbarui, status sistem file akan beralih ke Salah Konfigurasi. Status ini menampilkan pesan kesalahan dan tindakan korektif yang direkomendasikan di samping deskripsi sistem file di konsol, API, dan CLI. Setelah mengambil tindakan korektif yang disarankan, verifikasi bahwa status sistem file Anda akhirnya berubah menjadi Tersedia.

> **Important**
>
> Jika Anda memperbarui sistem file Anda dengan akun layanan baru, pastikan bahwa akun layanan baru memiliki izin kontrol penuh untuk objek komputer yang ada yang terkait dengan sistem file.

Untuk informasi tentang pemecahan masalah yang mungkin terkait dengan konfigurasi Direktori Aktif yang dikelola sendiri, lihat. Sistem file dalam keadaan salah konfigurasi

Anda dapat menggunakan AWS Management Console, Amazon FSx API, atau AWS CLI untuk memperbarui nama pengguna dan kata sandi akun layanan dan alamat IP server DNS dari konfigurasi Active Directory yang dikelola sendiri oleh sistem file. Anda dapat melacak kemajuan pembaruan konfigurasi Direktori Aktif yang dikelola sendiri kapan saja menggunakan, CLI AWS Management Console, dan API. Untuk informasi selengkapnya, lihat Pembaruan Direktori Aktif yang dikelola sendiri.

Untuk memperbarui konfigurasi Direktori Aktif yang dikelola sendiri (Konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Arahkan ke sistem File, dan pilih sistem file Windows yang ingin Anda perbarui konfigurasi Active Directory yang dikelola sendiri.
3. Di tab Jaringan & keamanan, lalu pilih Perbarui untuk Alamat IP server DNS, atau untuk nama pengguna akun layanan, tergantung pada properti Direktori Aktif yang Anda perbarui.
4. Masukkan alamat IP server DNS baru, atau kredensial akun layanan baru di kotak dialog yang muncul.
5. Pilih Perbarui untuk memulai pembaruan konfigurasi Direktori Aktif.

   Anda dapat memantau kemajuan pembaruan menggunakan AWS Management Console atau AWS CLI.

Untuk memperbarui konfigurasi Direktori Aktif yang dikelola sendiri (CLI)

- Untuk memperbarui konfigurasi Direktori Aktif yang dikelola sendiri dari sistem file Windows File Server FSx untuk Windows, gunakan AWS CLI perintah update-file-system. Atur parameter berikut:
  - `--file-system-id` ke ID dari sistem file yang Anda perbarui.
  - `UserName`nama pengguna baru untuk akun layanan Direktori Aktif yang dikelola sendiri.
  - `Password`kata sandi baru untuk akun layanan Direktori Aktif yang dikelola sendiri.
  - `DnsIps`alamat IP untuk server DNS Active Directory yang dikelola sendiri.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
    DnsIps=[192.0.2.0,192.0.2.24]}'
```

Jika tindakan pembaruan berhasil, layanan mengirimkan kembali respons HTTP 200. `AdminstrativeActions`Objek dalam respons menggambarkan permintaan dan statusnya.

Mengubah akun FSx layanan Amazon

Jika Anda memperbarui sistem file Anda dengan akun layanan baru, akun layanan baru harus memiliki izin dan hak istimewa yang diperlukan untuk bergabung dengan Direktori Aktif Anda dan memiliki izin kontrol penuh untuk objek komputer yang ada yang terkait dengan sistem file. Selain itu, pastikan bahwa akun layanan baru adalah bagian dari akun tepercaya dengan pengaturan Kebijakan Grup yang diaktifkan Pengontrol domain: Izinkan penggunaan kembali akun komputer selama bergabung dengan domain.

Kami sangat menyarankan menggunakan grup Active Directory untuk mengelola izin dan konfigurasi Active Directory yang terkait dengan akun layanan.

Saat mengubah akun layanan untuk Amazon FSx, pastikan bahwa akun layanan memiliki pengaturan berikut:

- Akun layanan baru (atau grup Direktori Aktif yang menjadi anggotanya) memiliki izin kontrol penuh untuk objek komputer yang ada yang terkait dengan sistem file.
- Akun layanan baru dan sebelumnya (atau grup Direktori Aktif yang menjadi anggotanya) adalah bagian dari akun tepercaya (atau grup Direktori Aktif tepercaya) dengan pengontrol Domain: Izinkan penggunaan kembali akun komputer selama pengaturan Kebijakan Grup bergabung dengan domain diaktifkan pada semua pengontrol domain di Direktori Aktif.

Jika akun layanan tidak memenuhi persyaratan ini, kondisi berikut dapat terjadi:

- Untuk sistem file Single-AZ, sistem file bisa menjadi MISCONFIGURED_UNAVAILABLE.
- Untuk sistem file multi-AZ, sistem file bisa menjadi MISCONFIGURATED dan nama RemotePowerShell endpoint mungkin berubah.

Mengkonfigurasi Kebijakan Grup pengontrol domain

Prosedur yang direkomendasikan Microsoft berikut menjelaskan cara menggunakan kebijakan grup pengontrol domain untuk mengonfigurasi kebijakan daftar izinkan.

Untuk mengonfigurasi kebijakan daftar izinkan pengontrol domain

1. Instal pembaruan Microsoft Windows 12 September 2023 atau yang lebih baru di semua komputer anggota dan pengontrol domain di Microsoft Active Directory yang dikelola sendiri.
2. Dalam kebijakan grup baru atau yang sudah ada yang berlaku untuk semua pengontrol domain di Direktori Aktif yang dikelola sendiri, konfigurasikan setelan berikut.

   a. Arahkan ke Konfigurasi Komputer>Kebijakan>Pengaturan Windows> Pengaturan Keamanan> Kebijakan Lokal>Opsi Keamanan.

   b. Klik dua kali Pengontrol domain: Izinkan penggunaan kembali akun komputer selama bergabung dengan domain.

   c. Pilih Tentukan setelan kebijakan ini dan<Edit Security ... >.

   d. Gunakan pemilih objek untuk menambahkan pengguna atau grup pembuat dan pemilik akun komputer tepercaya ke izin Izinkan. (Sebagai praktik terbaik, kami sangat menyarankan Anda menggunakan grup untuk izin.) Jangan menambahkan akun pengguna yang melakukan domain join.

   > **Warning**
   >
   > Batasi keanggotaan pada kebijakan untuk pengguna tepercaya dan akun layanan. Jangan menambahkan pengguna yang diautentikasi, semua orang, atau grup besar lainnya ke kebijakan ini. Sebagai gantinya, tambahkan pengguna tepercaya dan akun layanan tertentu ke grup dan tambahkan grup tersebut ke kebijakan.

3. Tunggu interval penyegaran Kebijakan Grup atau jalankan gpupdate /force di semua pengontrol domain.
4. Verifikasi bahwa kunci registri HKLM\ System\ CCS\ Control\ SAM — “ComputerAccountReuseAllowList” diisi dengan SDDL yang diinginkan. Jangan mengedit registri secara manual.
5. Cobalah untuk bergabung dengan komputer yang memiliki pembaruan 12 September 2023, atau yang lebih baru diinstal. Pastikan salah satu akun yang tercantum dalam polis memiliki akun komputer. Juga pastikan bahwa registri tidak memiliki NetJoinLegacyAccountReusekunci yang diaktifkan (diatur ke 1). Jika domain join gagal, periksa **`c:\windows\debug\netsetup.log`**.

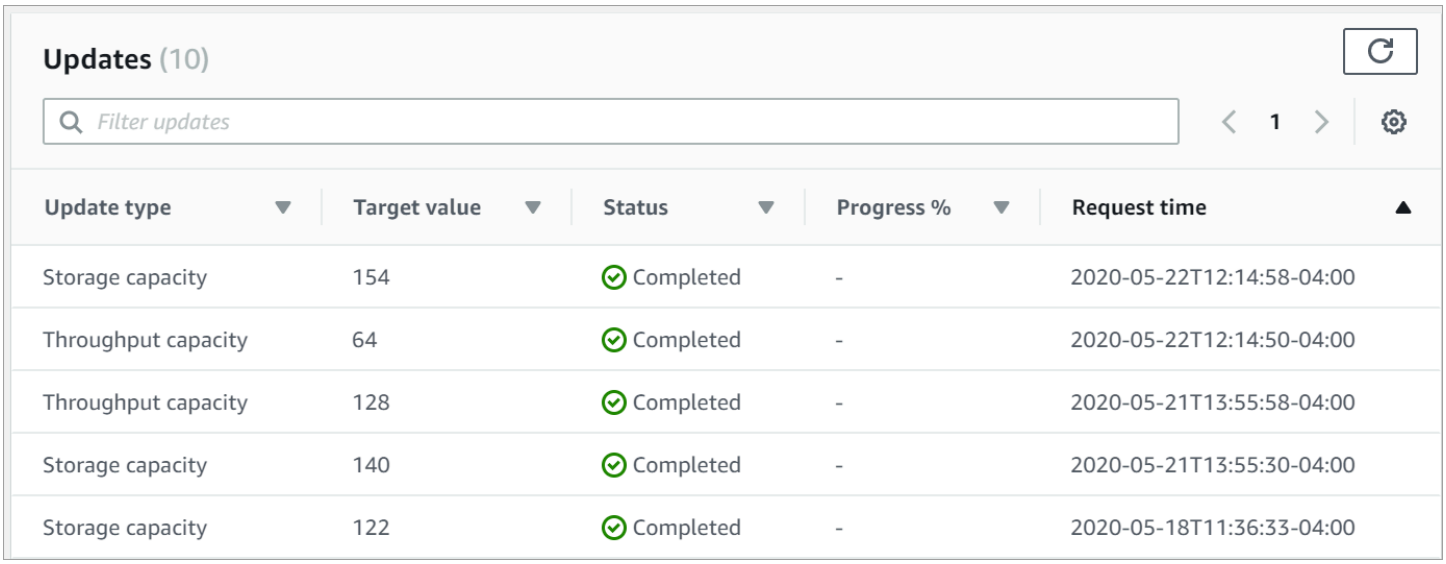
Pembaruan Direktori Aktif yang dikelola sendiri

Anda dapat memantau kemajuan pembaruan konfigurasi Direktori Aktif yang dikelola sendiri menggunakan API, atau AWS CLI, seperti yang dijelaskan dalam prosedur berikut. AWS Management Console

Saat Anda memperbarui konfigurasi Direktori Aktif yang dikelola sendiri oleh sistem file Anda, status sistem file beralih dari Tersedia ke Pembaruan saat pembaruan diterapkan. Setelah pembaruan selesai, status beralih kembali ke Tersedia. Pembaruan konfigurasi Active Directory dapat memakan waktu hingga beberapa menit untuk diselesaikan.

Memantau pembaruan di konsol

Di tab Pembaruan dalam jendela Detail sistem file, Anda dapat melihat 10 pembaruan terbaru untuk setiap jenis pembaruan.



Untuk pembaruan Direktori Aktif yang dikelola sendiri, Anda dapat melihat informasi berikut ini.

Jenis pembaruan

Jenis yang didukung adalah sebagai berikut:

- Alamat IP server DNS
- Kredensial akun layanan

Nilai target

Nilai yang diinginkan untuk memperbarui properti sistem file. Untuk pembaruan kredensial akun layanan, hanya nama pengguna yang ditampilkan, kata sandi akun layanan tidak pernah disertakan dalam bidang ini.

Status

Status terkini dari pembaruan. Untuk pembaruan Direktori Aktif yang dikelola sendiri, nilai yang mungkin adalah sebagai berikut:

- Tertunda - Amazon FSx telah menerima permintaan pembaruan, tetapi belum mulai memprosesnya.
- Sedang berlangsung - Amazon FSx sedang memproses permintaan pembaruan.
- Selesai – Pembaruan sistem file berhasil diselesaikan.
- Gagal – Pembaruan sistem file gagal. Pilih tanda tanya (?) untuk melihat detail tentang kegagalan.

Kemajuan%

Menampilkan kemajuan pembaruan sistem file dalam persentase dari selesai pembaruan.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Memantau pembaruan menggunakan AWS CLI dan API

Anda dapat melihat dan memantau permintaan pembaruan sistem file yang sedang berlangsung menggunakan describe-file-systems AWS CLI perintah dan tindakan DescribeFileSystemsAPI. Array `AdministrativeActions` mencantumkan 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif.

Contoh berikut menunjukkan kutipan respon dari perintah describe-file-systems CLI menunjukkan dua pembaruan sistem file Active Directory yang dikelola sendiri.

```
{
    "OwnerId": "111122223333",
    .
    .
    .
```

```
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694766.757,
                    "Status": "PENDING",
                    "TargetFileSystemValues": {
                        "WindowsConfiguration": {
                            "SelfManagedActiveDirectoryConfiguration": {
                                "UserName": "serviceUser",
                            }
                        }
                    }
                },
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1619032957.759,
                    "Status": "FAILED",
                    "TargetFileSystemValues": {
                        "WindowsConfiguration": {
                            "SelfManagedActiveDirectoryConfiguration": {
                            "DnsIps": [
                                    "10.0.138.161"
                                ]
                            }
                        }
                    },
                    "FailureDetails": {
                        "Message": "Failure details message."
                    }
                }
            ],
        .
        .
        .
```

FSx untuk kinerja Windows File Server

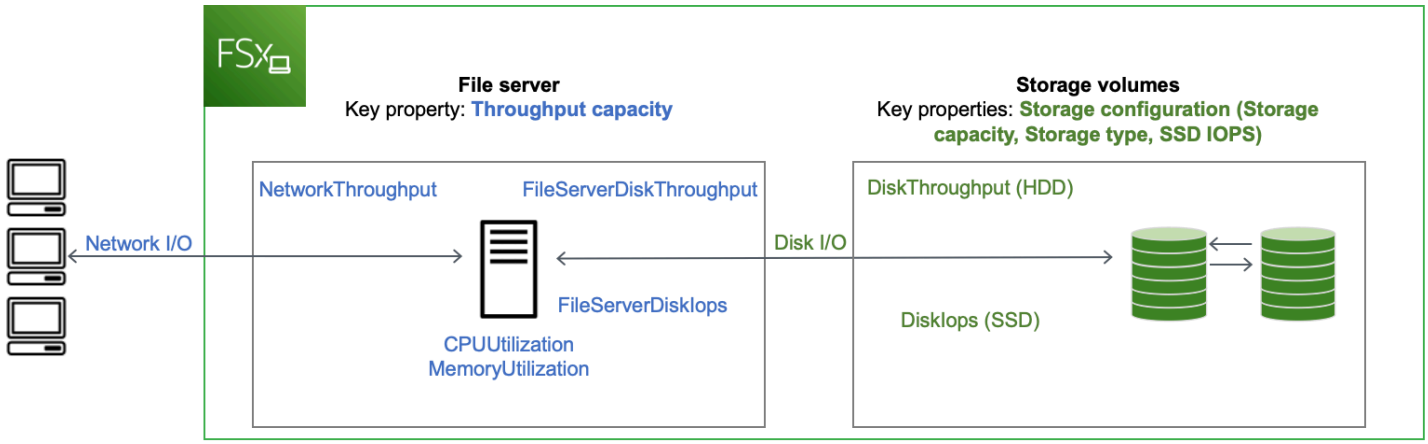
FSx untuk Windows File Server menawarkan opsi konfigurasi sistem file untuk memenuhi berbagai kebutuhan kinerja. Berikut ini adalah ikhtisar kinerja sistem FSx file Amazon, dengan diskusi tentang opsi konfigurasi kinerja yang tersedia dan tip kinerja yang berguna.

Topik

Kinerja sistem file

Masing-masing FSx untuk sistem file Windows File Server terdiri dari server file Windows yang berkomunikasi dengan klien dan satu set volume penyimpanan, atau disk, yang dilampirkan ke server file. Setiap server file menggunakan cache dalam memori untuk meningkatkan performa untuk data yang diakses paling sering.

Diagram berikut menggambarkan bagaimana data diakses dari sistem file Windows File Server FSx untuk Windows.



Ketika klien mengakses data yang disimpan dalam cache dalam memori, data disajikan langsung ke klien yang meminta sebagai jaringan I/O. Server file tidak perlu membacanya dari atau menuliskannya ke dalam disk. Kinerja akses data ini ditentukan oleh batas I/O jaringan dan ukuran cache dalam memori.

Ketika klien mengakses data yang tidak dalam cache, server file membacanya dari atau menulisnya ke dalam disk sebagai disk I/O. Data kemudian disajikan dari server file ke klien sebagai jaringan I/O. Kinerja akses data ini ditentukan oleh batas I/O jaringan serta batas I/O disk.

Kinerja I/O jaringan dan cache dalam memori server file ditentukan oleh kapasitas throughput sistem file. Kinerja I/O disk ditentukan oleh kombinasi kapasitas throughput dan konfigurasi penyimpanan. Kinerja I/O disk maksimum, yang terdiri dari throughput disk dan level IOPS disk, yang dapat dicapai oleh sistem file Anda adalah yang lebih rendah dari:

- Tingkat kinerja I/O disk yang disediakan oleh server file Anda, berdasarkan kapasitas throughput yang Anda pilih untuk sistem file Anda.
- Tingkat kinerja I/O disk yang disediakan oleh konfigurasi penyimpanan Anda (kapasitas penyimpanan, jenis penyimpanan, dan tingkat IOPS SSD yang Anda pilih untuk sistem file Anda).

Pertimbangan kinerja tambahan

Kinerja sistem file biasanya diukur dengan latensi, throughput, dan operasi I/O per detik (IOPS).

Latensi

FSx untuk server file Windows File Server menggunakan cache dalam memori yang cepat untuk mencapai latensi sub-milidetik yang konsisten untuk data yang diakses secara aktif. Untuk data yang

tidak ada dalam cache dalam memori, yaitu, untuk operasi file yang perlu dilayani dengan melakukan I/O pada volume penyimpanan yang mendasarinya, Amazon FSx menyediakan latensi operasi file sub-milidetik dengan penyimpanan solid state drive (SSD), dan latensi milidetik satu digit dengan penyimpanan hard disk drive (HDD).

Throughput dan IOPS

Sistem FSx file Amazon menyediakan hingga 2 GBps dan 80.000 IOPS di semua tempat Wilayah AWS Amazon FSx tersedia, dan 12 GBps throughput dan 400.000 IOPS di AS Timur (Virginia N.), AS Barat (Oregon), AS Timur (Ohio), Eropa (Irlandia), Asia Pasifik (Tokyo), dan Asia Pasifik (Singapura). Jumlah spesifik throughput dan IOPS yang dapat didorong oleh beban kerja Anda pada sistem file Anda tergantung pada kapasitas throughput, kapasitas penyimpanan, dan jenis penyimpanan sistem file Anda, bersama dengan sifat beban kerja Anda, termasuk ukuran set kerja aktif.

Performa klien tunggal

Dengan Amazon FSx, Anda bisa mendapatkan throughput penuh dan level IOPS untuk sistem file Anda dari satu klien yang mengaksesnya. Amazon FSx mendukung SMB Multichannel. Fitur ini memungkinkannya menyediakan hingga beberapa GBps throughput dan ratusan ribu IOPS untuk satu klien yang mengakses sistem file Anda. SMB Multichannel menggunakan beberapa koneksi jaringan antara klien dan server secara bersamaan untuk agregat bandwidth jaringan untuk pemanfaatan maksimal. Meskipun ada batasan teoritis untuk jumlah koneksi SMB yang didukung oleh Windows, batas ini adalah jutaan, dan praktis Anda dapat memiliki jumlah koneksi SMB yang tidak terbatas.

Performa burst

Beban kerja berbasis file biasanya runcing, ditandai dengan periode pendek dan intens I/O tinggi dengan banyak waktu idle antara semburan. Untuk mendukung beban kerja runcing, selain kecepatan dasar yang dapat dipertahankan oleh sistem file 24/7, Amazon FSx menyediakan kemampuan untuk meledak ke kecepatan yang lebih tinggi untuk periode waktu untuk operasi I/O jaringan dan I/O disk. Amazon FSx menggunakan mekanisme kredit I/O untuk mengalokasikan throughput dan IOPS berdasarkan pemanfaatan rata-rata - sistem file memperoleh kredit ketika throughput dan penggunaan IOPS mereka di bawah batas dasar mereka, dan dapat menggunakan kredit ini saat mereka melakukan operasi I/O.

Dampak kapasitas throughput terhadap performa

Kapasitas throughput menentukan kinerja sistem file dalam kategori berikut:

- Jaringan I/O — Kecepatan di mana server file dapat melayani data file ke klien yang mengaksesnya.
- CPU dan memori server file — Sumber daya yang tersedia untuk menyajikan data file dan melakukan aktivitas latar belakang seperti deduplikasi data dan salinan bayangan.
- Disk I/O — Kecepatan di mana file server dapat mendukung I/O antara file server dan volume penyimpanan.

Tabel berikut memberikan rincian tentang tingkat maksimum I/O jaringan (throughput dan IOPS) dan disk I/O (throughput dan IOPS) yang dapat Anda drive dengan setiap konfigurasi kapasitas throughput yang disediakan, dan jumlah memori yang tersedia untuk caching dan mendukung aktivitas latar belakang seperti deduplikasi data dan salinan bayangan. Meskipun Anda dapat memilih tingkat kapasitas throughput di bawah 32 megabyte per detik (MBps) saat Anda menggunakan Amazon API FSx atau CLI, perlu diingat bahwa level ini dimaksudkan untuk beban kerja pengujian dan pengembangan, bukan untuk beban kerja produksi.

> **Note**
>
> Perhatikan bahwa tingkat kapasitas throughput 4.608 MBps dan lebih tinggi hanya didukung di wilayah berikut: AS Timur (Virginia N.), AS Barat (Oregon), AS Timur (Ohio), Eropa (Irlandia), Asia Pasifik (Tokyo), dan Asia Pasifik (Singapura).

Jaringan I/O dan memori

FSx kapasitas throughput () MBps	Throughput jaringan () MBps		IOPS Jaringan	Memori (GB)
	Baseline	Burst (selama beberapa menit sehari)		
32	32	600	Ribuan	4

FSx kapasitas throughput () MBps	Throughput jaringan () MBps		IOPS Jaringan	Memori (GB)
64	64	600	Puluhan ribu	8
128	150	1.250		8
256	300	1.250	Ratusan ribu	16
512	600	1.250		32
1,024	1.500	–		72
2,048	3,125	–		144
4,608	9,375	–	Juta.	192
6,144	12.500	–		256
9,216	18,750	–		384
12,288	21.250	–		512

Disk I/O

FSx kapasitas throughput () MBps	Throughput disk () MBps		IOPS Disk	
	Baseline	Burst (selama 30 menit sehari)	Baseline	Burst (selama 30 menit sehari)
32	32	260	2K	12K
64	64	350	4K	16K
128	128	600	6K	20K
256	256	600	10K	20K

FSx kapasitas throughput () MBps	Throughput disk () MBps		IOPS Disk	
512	512	–	20K	–
1,024	1,024	–	40K	–
2,048	2,048	–	80K	–
4,608	4,608	–	150K	–
6,144	6,144	–	200K	–
9,216	9,216 [1]	–	300K [1]	–
12,288	12,288 [1]	–	400K [1]	–

> **Note**
>
> [1] Jika Anda memiliki sistem file Multi-AZ dengan kapasitas throughput 9.216 atau 12.288 MBps, kinerja akan dibatasi hingga 9.000 MBps dan 262.500 IOPS hanya untuk lalu lintas tulis. Jika tidak, untuk lalu lintas baca di semua sistem file Multi-AZ, baca dan tulis lalu lintas pada semua sistem file Single-AZ, dan semua tingkat kapasitas throughput lainnya, sistem file Anda akan mendukung batas kinerja yang ditunjukkan pada tabel.

Memilih tingkat kapasitas throughput yang tepat

Saat Anda membuat sistem file menggunakan Amazon Web Services Management Console, Amazon FSx secara otomatis memilih tingkat kapasitas throughput yang disarankan untuk sistem file Anda berdasarkan jumlah kapasitas penyimpanan yang Anda konfigurasikan. Meskipun kapasitas throughput yang disarankan harus cukup untuk sebagian besar beban kerja, Anda memiliki opsi untuk mengganti rekomendasi dan mengonfigurasi sejumlah kapasitas throughput tertentu untuk memenuhi kebutuhan beban kerja Anda. Misalnya, jika beban kerja Anda mengharuskan mengarahkan 1 GBps lalu lintas ke sistem file Anda, Anda harus memilih kapasitas throughput minimal 1.024. MBps Tabel berikut memberikan tingkat kapasitas throughput minimum yang direkomendasikan untuk sistem file berdasarkan jumlah kapasitas penyimpanan yang disediakan.

Kapasitas penyimpanan SSD (GiB)	Kapasitas penyimpanan HDD (GiB)	Kapasitas throughput minimum yang disarankan () MBps
Hingga 640	Hingga 3.200	32
641—1.280	3201—6.400	64
1281—2.560	6.401—12.800	128
2.561—5.120	12.801—25.600	256
5,121—10.240	25.601—51.200	512
10.241—20.480	>51.200	1,024
> 20.480	TA	2,048

Anda juga harus mempertimbangkan fitur yang Anda rencanakan untuk diaktifkan pada sistem file Anda dalam menentukan tingkat throughput yang akan dikonfigurasi. Misalnya, mengaktifkan Shadow Copies mungkin mengharuskan Anda untuk meningkatkan kapasitas throughput Anda ke tingkat hingga tiga kali beban kerja yang diharapkan untuk memastikan server file dapat mempertahankan salinan bayangan dengan kapasitas kinerja I/O yang tersedia. Jika Anda mengaktifkan Data Deduplication, Anda harus menentukan jumlah memori yang terkait dengan kapasitas throughput sistem file Anda dan memastikan jumlah memori ini cukup untuk ukuran data Anda.

Anda dapat menyesuaikan jumlah kapasitas throughput naik atau turun kapan saja setelah Anda membuatnya. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Anda dapat memantau pemanfaatan sumber daya kinerja server file oleh beban kerja Anda dan mendapatkan rekomendasi tentang kapasitas throughput mana yang harus dipilih dengan melihat tab Pemantauan & kinerja> Kinerja di konsol Amazon Anda. FSx Kami merekomendasikan pengujian di lingkungan pra-produksi untuk memastikan konfigurasi yang Anda pilih memenuhi persyaratan kinerja beban kerja Anda. Untuk sistem file multi-AZ, kami juga merekomendasikan pengujian dampak dari proses failover yang terjadi selama pemeliharaan sistem file, perubahan kapasitas throughput, dan gangguan layanan yang tidak direncanakan pada beban kerja Anda, serta memastikan bahwa Anda telah menyediakan kapasitas throughput yang cukup untuk mencegah

dampak kinerja selama peristiwa ini. Untuk informasi selengkapnya, lihat Mengakses metrik sistem file.

Dampak konfigurasi penyimpanan pada kinerja

Kapasitas penyimpanan sistem file Anda, jenis penyimpanan, dan tingkat IOPS SSD semuanya memengaruhi kinerja I/O disk sistem file Anda. Anda dapat mengonfigurasi sumber daya ini untuk memberikan tingkat kinerja yang diinginkan untuk beban kerja Anda.

Anda dapat meningkatkan kapasitas penyimpanan dan menskalakan SSD IOPS kapan saja. Untuk informasi selengkapnya, silakan lihat Mengelola kapasitas penyimpanan dan Mengelola SSD IOPS. Anda juga dapat memutakhirkan sistem file Anda dari jenis penyimpanan HDD ke jenis penyimpanan SSD. Untuk informasi selengkapnya, lihat Mengelola jenis penyimpanan sistem file Anda.

Sistem file Anda menyediakan tingkat default throughput disk dan IOPS berikut:

Jenis penyimpanan	Throughput disk (MBps per TiB penyimpanan)	Disk IOPS (per TiB penyimpanan)
SSD	750	3.000 [1]
HDD	12 baseline; 80 burst (hingga maksimal 1 GBps per sistem file)	12 baseline; 80 burst

> **Note**
>
> [1] Untuk sistem file dengan tipe penyimpanan SSD, Anda dapat menyediakan IOPS tambahan, hingga rasio maksimum 500 IOPS per GiB penyimpanan dan 400.000 IOPS per sistem file.

Kinerja HDD burst

Untuk volume penyimpanan HDD, Amazon FSx menggunakan model burst bucket untuk kinerja. Ukuran volume menentukan throughput tingkat dasar volume Anda, yang merupakan tingkat di mana volume mengakumulasi kredit throughput. Ukuran volume juga menentukan throughput lonjakan

volume Anda, yang merupakan tingkat di mana Anda dapat menghabiskan kredit saat tersedia. Volume yang lebih besar memiliki garis dasar dan throughput lonjakan yang lebih tinggi. Makin banyak kredit volume Anda, makin lama volume tersebut dapat mendorong I/O pada tingkat lonjakan.

Throughput yang tersedia dari volume penyimpanan HDD dinyatakan dengan rumus berikut:

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Untuk volume HDD 1-Tib, throughput burst dibatasi hingga 80 MiBps, bucket diisi dengan kredit pada 12 MiBps, dan dapat menampung hingga 1 kredit Tib-senilai.

Volume penyimpanan HDD dapat mengalami variasi kinerja yang signifikan tergantung pada beban kerja. Lonjakan mendadak dalam IOPS atau throughput dapat menyebabkan penurunan kinerja disk. `DiskThroughputBalance`Metrik ini memberikan informasi tentang saldo kredit burst untuk throughput disk dan pemanfaatan IOPS disk. Misalnya, jika beban kerja Anda melebihi batas HDD IOPS dasar (12 IOPS per TiB penyimpanan), pemanfaatan Disk IOPS (HDD) akan berada di atas 100% dan mengakibatkan menipisnya saldo kredit burst, yang dapat Anda lihat dalam metrik. `DiskThroughputBalance` Agar beban kerja Anda terus mendorong I/O tingkat tinggi, Anda mungkin perlu melakukan salah satu hal berikut:

- Kurangi permintaan I/O untuk beban kerja Anda sehingga saldo kredit burst diisi ulang.
- Tingkatkan kapasitas penyimpanan sistem file untuk memberikan tingkat baseline yang lebih tinggi dari IOPS disk.
- Tingkatkan sistem file untuk menggunakan penyimpanan SSD, yang menyediakan tingkat dasar IOPS disk yang lebih tinggi agar lebih sesuai dengan kebutuhan beban kerja Anda.

Contoh: kapasitas penyimpanan dan kapasitas throughput

Contoh berikut menggambarkan bagaimana kapasitas penyimpanan dan kapasitas throughput berdampak pada performa sistem file.

Sistem file yang dikonfigurasi dengan kapasitas penyimpanan HDD 2 TiB dan 32 kapasitas throughput memiliki MBps tingkat throughput berikut:

- Throughput jaringan — 32 MBps baseline dan 600 MBps burst (lihat tabel kapasitas throughput)
- Disk throughput — 24 MBps baseline dan 160 MBps burst, yang merupakan yang lebih rendah dari:

- tingkat throughput disk 32 MBps baseline dan 260 MBps burst yang didukung oleh server file, berdasarkan kapasitas throughput sistem file
- tingkat throughput disk 24 MBps baseline (12 MBps per TB* 2 TiB) dan 160 burst MBps (80 per TiB* 2 MBps TiB) didukung oleh volume penyimpanan, berdasarkan jenis dan kapasitas penyimpanan

Beban kerja Anda yang mengakses sistem file akan dapat mendorong hingga 32 MBps baseline dan 600 MBps burst throughput untuk operasi file yang dilakukan pada data yang diakses secara aktif yang di-cache di cache file server dalam memori, dan hingga 24 MBps baseline dan 160 MBps burst throughput untuk operasi file yang perlu pergi jauh-jauh ke disk, misalnya, karena cache terlewat.

Mengukur kinerja menggunakan CloudWatch metrik

Anda dapat menggunakan Amazon CloudWatch untuk mengukur dan memantau throughput dan IOPS sistem file Anda. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

Memecahkan masalah kinerja sistem file

Kinerja sistem file Windows File Server Anda FSx bergantung pada beberapa faktor, termasuk lalu lintas yang Anda arahkan ke sistem file Anda, bagaimana Anda menyediakan sistem file Anda, dan sumber daya yang dikonsumsi oleh fitur yang diaktifkan, seperti Deduplikasi Data atau Salinan Bayangan. Untuk informasi tentang memahami kinerja sistem file Anda, lihatFSx untuk kinerja Windows File Server.

Topik

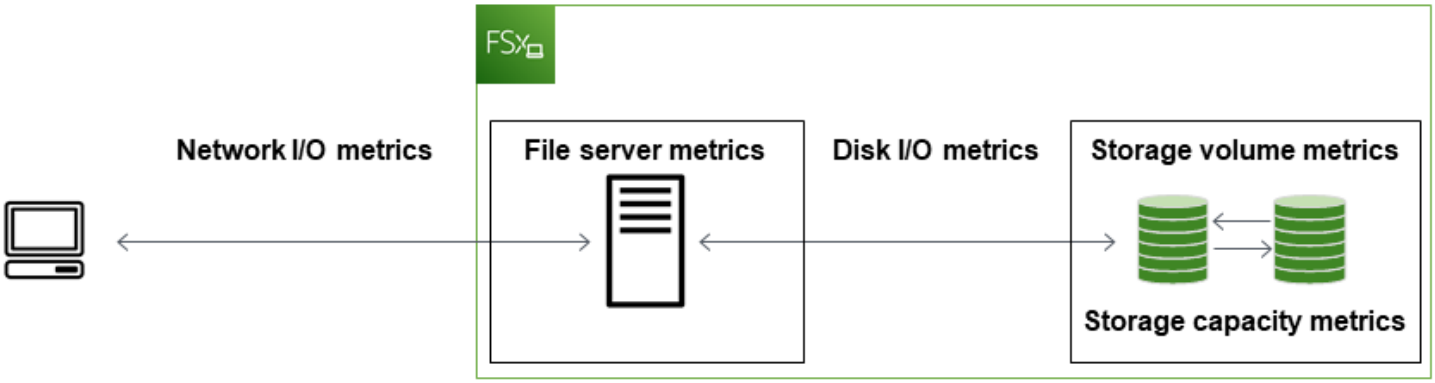
- Bagaimana cara menentukan batas throughput dan IOPS untuk sistem file saya?
- Apa perbedaan antara I/O jaringan dan disk I/O? Mengapa I/O jaringan saya berbeda dari I/O disk saya?
- Mengapa penggunaan CPU atau memori saya tinggi, bahkan ketika I/O jaringan saya rendah?
- Apa yang meledak? Berapa banyak ledakan yang digunakan sistem file saya? Apa yang terjadi ketika kredit burst habis?
- Saya melihat peringatan di halaman Pemantauan & kinerja — apakah saya perlu mengubah konfigurasi sistem file saya?
- Metrik saya sementara hilang, haruskah saya khawatir?

Bagaimana cara menentukan batas throughput dan IOPS untuk sistem file saya?

Untuk melihat throughput sistem file dan batas IOPS, lihat tabel yang menunjukkan tingkat kinerja berdasarkan jumlah kapasitas throughput penyediaan.

Apa perbedaan antara I/O jaringan dan disk I/O? Mengapa I/O jaringan saya berbeda dari I/O disk saya?

Sistem FSx file Amazon mencakup satu atau lebih server file yang melayani data melalui jaringan ke klien yang mengakses sistem file. Ini adalah jaringan I/O. Server file memiliki cache dalam memori yang cepat untuk meningkatkan kinerja untuk data yang paling sering diakses. Server file juga mengarahkan lalu lintas ke volume penyimpanan yang meng-host data sistem file Anda. Ini adalah disk I/O. Diagram berikut menggambarkan jaringan dan disk I/O untuk sistem file Amazon FSx .



Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

Mengapa penggunaan CPU atau memori saya tinggi, bahkan ketika I/O jaringan saya rendah?

Penggunaan CPU dan memori server file tidak hanya bergantung pada lalu lintas jaringan yang Anda kendarai, tetapi juga fitur yang telah Anda aktifkan pada sistem file Anda. Bagaimana Anda mengkonfigurasi dan menjadwalkan fitur-fitur ini dapat memengaruhi pemanfaatan CPU dan memori.

Pekerjaan Deduplikasi Data yang sedang berlangsung dapat menghabiskan memori. Anda dapat memodifikasi konfigurasi pekerjaan deduplikasi untuk mengurangi kebutuhan memori. Misalnya, Anda dapat membatasi pengoptimalan agar berjalan pada jenis file atau folder tertentu, atau menetapkan ukuran dan usia file minimum untuk pengoptimalan. Kami juga merekomendasikan

mengonfigurasi pekerjaan deduplikasi untuk dijalankan selama periode idle ketika ada beban minimal pada sistem file Anda. Untuk informasi selengkapnya, lihat Mengurangi biaya penyimpanan dengan Data Deduplication.

Jika Anda mengaktifkan enumerasi berbasis akses, Anda mungkin melihat pemanfaatan CPU yang tinggi saat pengguna akhir melihat atau mencantumkan file berbagi, atau selama fase Optimasi pekerjaan penskalaan penyimpanan. Untuk informasi selengkapnya, lihat Mengaktifkan enumerasi berbasis akses pada namespace di Dokumentasi Penyimpanan Microsoft.

Apa yang meledak? Berapa banyak ledakan yang digunakan sistem file saya? Apa yang terjadi ketika kredit burst habis?

Beban kerja berbasis file biasanya runcing, ditandai dengan periode I/O tinggi yang pendek dan intens dengan waktu idle di antara semburan. Untuk mendukung jenis beban kerja ini, selain kecepatan dasar yang dapat dipertahankan oleh sistem file, FSx Amazon menyediakan kemampuan untuk meledak ke kecepatan yang lebih tinggi untuk periode waktu untuk operasi I/O jaringan dan I/O disk.

Amazon FSx menggunakan mekanisme kredit I/O untuk mengalokasikan throughput dan IOPS berdasarkan pemanfaatan rata-rata — sistem file memperoleh kredit ketika throughput dan penggunaan IOPS mereka di bawah batas dasar mereka, dan dapat menggunakan kredit ini untuk meledak di atas batas dasar (hingga batas burst) bila diperlukan. Untuk informasi selengkapnya tentang batas dan durasi burst untuk sistem file Anda, lihatFSx untuk kinerja Windows File Server.

Saya melihat peringatan di halaman Pemantauan & kinerja — apakah saya perlu mengubah konfigurasi sistem file saya?

Halaman Pemantauan & kinerja mencakup peringatan yang menunjukkan kapan tuntutan beban kerja baru-baru ini telah mendekati atau melampaui batas sumber daya yang ditentukan oleh cara Anda mengonfigurasi sistem file Anda. Ini tidak berarti Anda perlu mengubah konfigurasi Anda, meskipun sistem file Anda mungkin kurang disediakan untuk beban kerja Anda jika Anda tidak mengambil tindakan yang disarankan.

Jika beban kerja yang menyebabkan peringatan itu tidak lazim dan Anda tidak mengharapkannya berlanjut, mungkin aman untuk tidak mengambil tindakan dan memantau penggunaan Anda ke depan. Namun, jika beban kerja yang menyebabkan peringatan itu khas dan Anda mengharapkannya berlanjut, atau bahkan meningkat, kami sarankan mengikuti tindakan yang disarankan untuk meningkatkan kinerja server file (dengan meningkatkan kapasitas throughput) atau meningkatkan

kinerja volume penyimpanan (dengan meningkatkan kapasitas penyimpanan, atau dengan beralih dari penyimpanan HDD ke SSD).

> **Note**
>
> Peristiwa sistem file tertentu dapat menggunakan sumber daya kinerja I/O disk dan berpotensi memicu peringatan kinerja. Sebagai contoh:
>
> - Fase optimasi penskalaan kapasitas penyimpanan dapat menghasilkan peningkatan throughput disk, seperti yang dijelaskan dalam Kapasitas penyimpanan meningkat dan performa sistem file
> - Untuk sistem file multi-AZ, peristiwa seperti penskalaan kapasitas throughput, penggantian perangkat keras, atau gangguan Availability Zone menghasilkan peristiwa failover dan failback otomatis. Setiap perubahan data yang terjadi selama waktu ini perlu disinkronkan antara server file primer dan sekunder, dan Windows Server menjalankan pekerjaan sinkronisasi data yang dapat menggunakan sumber daya I/O disk. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Metrik saya sementara hilang, haruskah saya khawatir?

Sistem file single-AZ akan mengalami ketidaktersediaan selama pemeliharaan sistem file, penggantian komponen infrastruktur, dan ketika Availability Zone tidak tersedia. Selama waktu ini, metrik tidak akan tersedia.

Dalam penyebaran Multi-AZ, Amazon FSx secara otomatis menyediakan dan memelihara server file siaga di Availability Zone yang berbeda. Jika ada pemeliharaan sistem file atau gangguan layanan yang tidak direncanakan, Amazon FSx secara otomatis gagal ke server file sekunder, memungkinkan Anda untuk terus mengakses data Anda tanpa intervensi manual. Selama periode singkat di mana sistem file Anda gagal dan gagal kembali, metrik mungkin tidak tersedia untuk sementara.

Mengelola FSx untuk sistem file Windows

Amazon FSx menyediakan berbagai kemampuan administratif yang membantu Anda mengelola dan mengembangkan sistem file Amazon FSx untuk Windows File Server dengan mudah untuk memenuhi perubahan beban kerja dan persyaratan pengguna, serta kebutuhan peraturan dan kepatuhan organisasi Anda. Berikut ini adalah daftar beberapa konfigurasi sistem file yang dapat Anda kelola menggunakan AWS Management Console, AWS CLI dan API, Amazon FSx CLI untuk manajemen jarak jauh, dan antarmuka PowerShell grafis Microsoft Windows Server asli.

- Kapasitas penyimpanan
- Jenis penyimpanan
- SSD IOPS
- Kapasitas throughput
- Alias DNS
- Deduplikasi data
- Salinan bayangan
- Kuota penyimpanan
- Mengaudit akses kunci
- Pembagian file

Bagian berikut memberikan informasi tentang fitur administrasi sistem file dan pengaturan yang tersedia untuk Anda. Kami telah menyertakan panduan untuk membantu Anda menentukan opsi mana yang terbaik untuk situasi Anda, dan praktik terbaik jika berlaku.

Topik

- Mengelola alias DNS
- Sesi pengguna dan file terbuka
- Mengelola penyimpanan FSx untuk Windows File Server
- Menggunakan Ruang Nama DFS
- Mengelola kapasitas throughput
- Menandai sumber daya Amazon FSx Anda
- Perbarui sistem file menggunakan AWS CLI

Status sistem FSx file Amazon

Anda dapat melihat status sistem FSx file Amazon dengan menggunakan FSx konsol Amazon, AWS CLI perintah describe-file-systems, atau operasi API DescribeFileSystems.

Status sistem file	Deskripsi
TERSEDIA	Sistem file dalam keadaan sehat, dan dapat dijangkau dan tersedia untuk digunakan.
CREATING	Amazon FSx sedang membuat sistem file baru.
DELETING	Amazon FSx menghapus sistem file yang ada.
MEMPERBARUI	Sistem file sedang mengalami pembaruan yang dikerjakan pelanggan.
SALAH KONFIGURASI	Sistem file dalam keadaan terganggu karena perubahan di lingkungan Direktori Aktif Anda. Sistem file Anda saat ini tidak tersedia atau berisiko kehilangan ketersediaan, dan cadangan mungkin tidak berhasil. Untuk informasi tentang memulihkan ketersediaan, lihatSistem file dalam keadaan salah konfigurasi.
SALAH KONFIGURASI_TIDAK TERSEDIA	Sistem file saat ini tidak tersedia karena perubahan di lingkungan Direktori Aktif Anda.

Status sistem file	Deskripsi
	Untuk informasi tentang memulihkan ketersedi aan, lihatSistem file dalam keadaan salah konfigurasi.
FAILED	• Saat membuat sistem file baru, Amazon FSx tidak dapat membuat sistem file baru. • Sistem file tidak tersedia. • Sistem file telah gagal dan Amazon tidak FSx dapat memulihkannya. • Amazon FSx tidak dapat membuat cadangan.

Menggunakan Amazon FSx CLI untuk PowerShell

Bab ini menjelaskan cara mengakses Amazon FSx CLI untuk manajemen jarak jauh PowerShell untuk melakukan tugas administrasi sistem file FSx untuk sistem file Windows. Anda juga dapat menggunakan Microsoft Windows-native graphical user interface (GUI) untuk melakukan beberapa tugas administratif.

Amazon FSx CLI untuk manajemen jarak jauh PowerShell memungkinkan administrasi sistem file untuk pengguna dalam grup administrator sistem file. Untuk memulai PowerShell sesi jarak jauh pada sistem file Windows File Server Anda, Anda harus terlebih dahulu memenuhi prasyarat berikut: FSx

- Dapat terhubung ke instance komputasi Windows yang memiliki konektivitas jaringan dengan sistem file Windows File Server Anda FSx .
- Masuk ke instans komputasi Windows sebagai anggota grup administrator sistem file. Jika Anda menggunakan AWS Managed Microsoft AD, itu adalah grup FSxAdministrator AWS Delegasi. Jika Anda menggunakan Microsoft Active Directory yang dikelola sendiri, itu adalah grup Admin Domain atau grup kustom yang Anda tentukan untuk administrasi saat Anda membuat sistem file. Untuk informasi selengkapnya, lihat Praktik terbaik saat menggunakan Active Directory yang dikelola sendiri.
- Aturan masuk grup keamanan VPC sistem file Anda memungkinkan lalu lintas di port 5985.

Amazon FSx CLI untuk manajemen jarak jauh PowerShell menggunakan fitur keamanan berikut:

- Kredensyal pengguna diautentikasi menggunakan otentikasi Kerberos.
- Komunikasi sesi manajemen antara klien yang terhubung dan sistem file dienkripsi menggunakan Kerberos.

Anda memiliki dua opsi untuk menjalankan perintah CLI manajemen jarak jauh pada sistem FSx file Amazon Anda:

- Anda dapat membuat PowerShell sesi Remote yang berjalan lama dan menjalankan perintah di dalam sesi.
- Anda dapat menggunakan `Invoke-Command` untuk menjalankan satu perintah atau satu blok perintah tanpa membuat PowerShell sesi Remote yang berjalan lama.

Jika Anda ingin mengatur dan meneruskan variabel sebagai parameter ke perintah manajemen jarak jauh, Anda harus menggunakannya`Invoke-Command`.

> **Note**
>
> Untuk sistem file Multi-AZ, Anda hanya dapat menggunakan Amazon FSx CLI untuk Manajemen Jarak Jauh saat sistem file menggunakan server file pilihannya. Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan: Sistem file Single-AZ dan Multi-AZ.

Anda perlu menggunakan Windows Remote PowerShell Endpoint sistem file untuk mengakses Remote PowerShell. Endpoint administrasi jarak jauh memiliki format`amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*, misalnya,`amznfsxctlyaa1k.corp.example.com`. Anda dapat menemukan nama endpoint dengan menggunakan AWS Management Console di halaman rincian sistem File pada tab Jaringan & keamanan. Gunakan AWS CLI `describe-file-systems`perintah untuk melihat `RemoteAdministrationEndpoint` properti yang dikembalikan dalam respons.

Anda dapat menggunakan `Get-Command` cmdlet untuk mengambil informasi tentang cmdlet, fungsi, dan alias yang tersedia di. PowerShell Untuk informasi selengkapnya, lihat dokumentasi Microsoft Get-Command.

Anda juga dapat menjalankan Amazon FSx CLI untuk CLI manajemen jarak jauh pada PowerShell perintah pada sistem file Anda menggunakan `Invoke-Command` cmdlet, menggunakan sintaks berikut:

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

Untuk petunjuk tentang cara memulai PowerShell sesi Remote berumur panjang pada sistem file Windows File Server Anda FSx , lihat Memulai PowerShell sesi FSx jarak jauh Amazon

Memulai PowerShell sesi FSx jarak jauh Amazon

Topik ini memberikan instruksi untuk memulai PowerShell sesi jarak jauh berumur panjang di server file Windows File Server Anda FSx .

Untuk memulai PowerShell sesi jarak jauh pada sistem file Anda

1. Connect ke instance komputasi yang memiliki konektivitas jaringan dengan sistem file Anda sebagai pengguna yang merupakan anggota Grup FSx Administrator yang didelegasikan yang Anda pilih saat membuat sistem file.
2. Buka PowerShell jendela Windows pada instance komputasi.
3. Di PowerShell, masukkan perintah berikut untuk membuka sesi jarak jauh berumur panjang di sistem FSx file Amazon Anda. Ganti *Remote-PowerShell-Endpoint* dengan PowerShell endpoint Windows Remote dari sistem file yang ingin Anda kelola. Gunakan `FsxRemoteAdmin` sebagai nama konfigurasi sesi.

   ```
   PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
    -ConfigurationName FsxRemoteAdmin
   [fs-0123456789abcdef0]: PS>
   ```

   Jika instans Anda bukan bagian dari domain Amazon FSx Active Directory, Anda akan diminta untuk memasukkan kredensyal pengguna dalam pop-up. Masukkan kredensyal pengguna yang merupakan anggota Grup FSx Administrator. Jika instans Anda bergabung dengan domain, Anda tidak akan diminta kredensialnya.

   > **Important**
   >
   > PowerShell Titik akhir Windows Remote mungkin berubah jika Anda menggunakan konfigurasi Direktori Aktif yang dikelola sendiri dan mengubah akun layanan tanpa

pengaturan Kebijakan Grup Direktori Aktif yang tepat. Untuk informasi lebih lanjut, lihat Mengubah akun FSx layanan Amazon untuk detail selengkapnya.

Tugas penyiapan sistem file satu kali menggunakan Amazon FSx CLI untuk manajemen jarak jauh PowerShell

Gunakan Amazon FSx CLI berikut untuk Manajemen Jarak Jauh pada PowerShell perintah untuk mengimplementasikan tugas administrasi sistem file dengan cepat mengikuti praktik terbaik kami.

Mengelola konsumsi penyimpanan

Gunakan perintah berikut untuk mengelola konsumsi penyimpanan sistem file Anda.

- Untuk mengaktifkan deduplikasi data dengan jadwal default, jalankan perintah berikut.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
```

  Secara opsional, gunakan perintah berikut untuk mendapatkan deduplikasi data yang beroperasi pada file Anda segera setelah file dibuat, tanpa memerlukan usia file minimum.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
```

  Untuk informasi selengkapnya, lihat Mengurangi biaya penyimpanan dengan Data Deduplication.

- Gunakan perintah berikut untuk menyalakam kuota penyimpanan pengguna dalam mode “Lacak”, yang hanya untuk tujuan pelaporan dan bukan untuk penegakan hukum.

```
$QuotaLimit = Quota limit in bytes
$QuotaWarningLimit = Quota warning threshold in bytes
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
 $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
```

  Untuk informasi selengkapnya, lihat Mengelola kuota penyimpanan.

Menyalakan salinan bayangan untuk mengaktifkan pengguna akhir untuk memulihkan file dan folder ke versi sebelumnya

Menyalakan salinan bayangan dengan jadwal default (hari kerja 7 Pagi dan 12 siang), sebagai berikut.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

Untuk informasi selengkapnya, lihat Mengkonfigurasi salinan bayangan untuk menggunakan penyimpanan dan jadwal default.

Memberlakukan enkripsi dalam transit

Perintah berikut memberlakukan enkripsi untuk klien yang telah connect ke sistem file Anda.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

Anda dapat menutup semua sesi terbuka dan memaksa klien yang saat ini telah connect untuk connect kembali menggunakan enkripsi.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

Untuk informasi selengkapnya, silakan lihat Mengelola enkripsi in transit dan Sesi pengguna dan file terbuka.

Memecahkan masalah akses ke Amazon CLI aktif FSx PowerShell

Ada sejumlah penyebab potensial untuk tidak dapat terhubung ke sistem file Anda menggunakan Remote PowerShell, masing-masing dengan resolusi mereka sendiri, sebagai berikut.

Untuk terlebih dahulu memastikan bahwa Anda dapat terhubung dengan sukses ke Windows Remote PowerShell Endpoint, Anda juga dapat menjalankan tes konektivitas dasar. Misalnya, Anda dapat menjalankan `test-netconnection endpoint -port 5985` perintah.

Grup keamanan sistem file tidak memiliki aturan masuk yang diperlukan untuk memungkinkan koneksi jarak jauh PowerShell

Grup keamanan sistem file harus memiliki aturan masuk yang memungkinkan lalu lintas di port 5985 untuk membuat sesi Remote PowerShell . Untuk informasi selengkapnya, lihat Grup keamanan Amazon VPC.

Anda memiliki kepercayaan eksternal yang dikonfigurasi antara Microsoft Active Directory yang AWS dikelola dan Active Directory lokal

Untuk menggunakan Amazon FSx Remote PowerShell dengan otentikasi Kerberos, Anda perlu mengonfigurasi kebijakan grup lokal pada klien untuk urutan pencarian hutan. Untuk informasi selengkapnya, lihat dokumentasi Microsoft Konfigurasi Urutan Pencarian Forest Kerberos (KFSO).

Terjadi kesalahan pelokalan bahasa saat mencoba memulai sesi jarak jauh PowerShell

Anda perlu menambahkan `-SessionOption` berikut ke perintah Anda: `-SessionOption (New-PSSessionOption -uiCulture "en-US")`

Berikut adalah dua contoh yang digunakan `-SessionOption` saat memulai PowerShell sesi jarak jauh pada sistem file Anda.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

Jendela pemeliharaan sistem file

Amazon FSx untuk Windows File Server melakukan patching perangkat lunak rutin untuk perangkat lunak Microsoft Windows Server yang dikelolanya. Jendela pemeliharaan menentukan hari dalam seminggu dan waktu hari ketika proses pemeliharaan ini dimulai. Anda dapat menentukan periode awal jendela pemeliharaan selama pembuatan sistem file. Jika Anda tidak menentukan satu, jendela awal pemeliharaan default 30 menit ditetapkan. Durasi jendela pemeliharaan tergantung pada beberapa faktor, termasuk ruang lingkup pemeliharaan, dan proses sinkronisasi aktivitas baca dan tulis file apa pun yang terjadi selama pemeliharaan antara server primer dan sekunder untuk sistem file multi-AZ. Untuk informasi selengkapnya, lihat Gagal dalam proses.

FSx untuk Windows File Server memungkinkan Anda menyesuaikan waktu mulai jendela pemeliharaan Anda untuk mengakomodasi beban kerja dan persyaratan operasional Anda. Anda dapat memindahkan waktu mulai jendela pemeliharaan Anda sesering yang diperlukan, asalkan waktu mulai jendela pemeliharaan dijadwalkan setidaknya sekali setiap 14 hari. Jika patch dirilis dan Anda belum menjadwalkan jendela pemeliharaan dalam 14 hari, FSx untuk Windows File Server dilanjutkan dengan pemeliharaan pada sistem file untuk memastikan keamanan dan keandalannya. Untuk informasi selengkapnya tentang cara menyesuaikan waktu mulai jendela pemeliharaan sistem file Anda, lihatMengubah jendela pemeliharaan mingguan.

Saat penambalan sedang berlangsung, perkirakan sistem file Single-AZ Anda tidak tersedia, biasanya kurang dari 20 menit. Sistem file multi-AZ tetap tersedia dan secara otomatis gagal dan gagal kembali antara server file pilihan dan siaga. Untuk informasi selengkapnya, lihat Gagal dalam proses. Karena menambal untuk sistem file Multi-AZ melibatkan kegagalan dan kegagalan kembali di antara server file, aktivitas baca dan tulis file apa pun yang terjadi selama waktu ini harus disinkronkan antara server file pilihan dan siaga. Untuk mengurangi waktu penambalan, kami sarankan untuk menjadwalkan jendela pemeliharaan Anda selama periode idle ketika ada beban minimal pada sistem file Anda.

> **Note**
>
> Untuk memastikan integritas data selama aktivitas pemeliharaan, Amazon FSx untuk Windows File Server menyelesaikan semua operasi penulisan yang tertunda ke volume penyimpanan yang mendasari yang menghosting sistem file Anda sebelum pemeliharaan dimulai.

Mengubah jendela pemeliharaan mingguan

FSx untuk Windows File Server memungkinkan Anda menyesuaikan kapan jendela pemeliharaan sistem file Anda mulai mengakomodasi beban kerja dan persyaratan operasional Anda. Anda dapat menggunakan FSx API AWS Management Console, AWS CLI, dan Amazon untuk mengubah saat jendela pemeliharaan mingguan dimulai, yang dijelaskan dalam prosedur berikut.

Untuk mengubah waktu mulai jendela pemeliharaan mingguan (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Pilih Sistem file di kolom navigasi sebelah kiri.
3. Pilih sistem file yang ingin Anda ubah jendela pemeliharaan mingguannya. Laman detail sistem file muncul.
4. Pilih Administrasi untuk menampilkan panel Pengaturan administrasi sistem file.
5. Pilih Perbarui untuk menampilkan jendela Ubah waktu pemeliharaan.
6. Masukkan hari dan waktu baru yang Anda ingin jendela pemeliharaan mingguannya dimulai.
7. Pilih Simpan untuk menyimpan perubahan Anda. Waktu mulai pemeliharaan baru ditampilkan di panel Pengaturan Administrasi.

Untuk mengubah waktu mulai jendela pemeliharaan mingguan menggunakan perintah update-file-systemCLI, lihat. Perbarui sistem file menggunakan AWS CLI

Mengelola alias DNS

Selain nama Domain Name System (DNS) default yang FSx disediakan Amazon, Anda juga dapat mengaitkan alias DNS yang Anda pilih dengan sistem file Anda. Dengan alias DNS, Anda dapat terus menggunakan nama DNS yang ada untuk mengakses data yang disimpan di Amazon FSx saat memigrasi penyimpanan sistem file dari lokal ke Amazon FSx, tanpa perlu memperbarui alat atau aplikasi apa pun.

Anda dapat mengaitkan alias DNS dengan yang baru dan yang sudah ada FSx untuk sistem file Windows File Server, dan ketika Anda mengembalikan cadangan ke sistem file baru, menggunakan file dan. AWS Management Console AWS CLI Anda dapat mengasosiasikan hingga 50 alias DNS dengan sistem file pada satu waktu.

> **Note**
>
> Support untuk alias DNS tersedia FSx untuk sistem file Windows File Server yang dibuat setelah pukul 12:00 ET pada 9 November 2020. Untuk menggunakan alias DNS pada sistem file yang dibuat sebelum pukul 12:00 ET pada tanggal 9 November 2020, lakukan hal berikut:
>
> 1. Ambil cadangan sistem file yang ada. Untuk informasi selengkapnya, lihat Bekerja dengan backup yang diinisiasi pengguna.
> 2. Pulihkan cadangan ke sistem file baru. Untuk informasi selengkapnya, lihat Memulihkan backup ke sistem file baru.
>
> Setelah sistem file baru tersedia, Anda akan dapat menggunakan alias DNS untuk mengaksesnya, menggunakan informasi yang diberikan di bagian ini.

> **Note**
>
> Informasi yang disajikan di sini mengasumsikan bahwa Anda bekerja sepenuhnya dalam Active Directory dan bahwa Anda tidak menggunakan penyedia DNS eksternal. Penyedia DNS pihak ketiga dapat mengakibatkan perilaku yang tidak terduga.
> Amazon FSx hanya mendaftarkan catatan DNS untuk sistem file jika domain Active Directory tempat Anda bergabung menggunakan Microsoft DNS sebagai DNS default. Jika Anda menggunakan DNS pihak ketiga, Anda perlu mengatur entri DNS secara manual untuk sistem FSx file Amazon Anda setelah Anda membuat sistem file Anda. Untuk informasi lebih lanjut tentang memilih alamat IP yang benar untuk digunakan untuk sistem file, lihat Mendapatkan alamat IP sistem file yang benar untuk digunakan untuk entri DNS manual.

Anda dapat mengaitkan alias DNS dengan sistem file Windows File Server yang ada FSx , saat Anda membuat sistem file baru, dan saat Anda membuat sistem file baru dari cadangan. Anda dapat mengasosiasikan hingga 50 alias DNS dengan sistem file pada satu waktu.

Selain mengaitkan alias DNS dengan sistem file Anda, agar klien terhubung ke sistem file menggunakan alias DNS, Anda juga harus melakukan hal berikut:

- Konfigurasikan nama utama layanan (SPNs) untuk otentikasi dan enkripsi Kerberos.

- Konfigurasikan catatan CNAME DNS untuk alias DNS yang menyelesaikan nama DNS default untuk sistem file Amazon Anda. FSx

Untuk informasi selengkapnya, lihat Mengakses data menggunakan alias DNS.

Nama alias DNS untuk sistem file Windows File Server Anda FSx harus memenuhi persyaratan berikut:

- Harus diformat sebagai nama domain yang sepenuhnya memenuhi syarat (FQDN).
- Harus berisi karakter alfanumerik atau tanda hubung saja (-).
- Tidak dapat meluncurkan atau mengakhiri dengan tanda hubung.
- Dapat memulai dengan angka.

Untuk nama alias DNS, Amazon FSx menyimpan karakter alfabet sebagai huruf kecil (a-z), terlepas dari bagaimana Anda menentukannya: sebagai huruf besar, huruf kecil, atau huruf yang sesuai dalam kode pelarian.

Jika Anda mencoba untuk mengaitkan alias yang sudah terkait dengan sistem file, itu tidak berpengaruh. Jika Anda mencoba memisahkan alias dari sistem file yang tidak terkait dengan sistem file, Amazon FSx merespons dengan kesalahan permintaan yang buruk.

> **Note**
>
> Ketika Amazon FSx menambahkan atau menghapus alias pada sistem file, klien yang terhubung sementara terputus dan secara otomatis akan terhubung kembali ke sistem file. Setiap file yang dibuka oleh klien yang memetakan bagian non-Continuously-Available (non-CA) pada saat pemutusan harus dibuka kembali oleh klien.

Topik

Status alias DNS

Alias DNS dapat memiliki salah satu nilai status berikut:

- Tersedia - Alias DNS dikaitkan dengan sistem FSx file Amazon.
- Membuat — Amazon FSx membuat alias DNS dan mengaitkannya dengan sistem file.
- Menghapus - Amazon FSx memisahkan alias DNS dari sistem file dan menghapusnya.
- Gagal membuat - Amazon FSx tidak dapat mengaitkan alias DNS dengan sistem file.
- Gagal menghapus - Amazon FSx tidak dapat memisahkan alias DNS dari sistem file.

Menggunakan alias DNS dengan autentikasi Kerberos

Kami menyarankan Anda menggunakan otentikasi dan enkripsi berbasis Kerberos dalam perjalanan dengan Amazon. FSx Kerberos menyediakan autentikasi paling aman untuk klien yang mengakses sistem file Anda. Untuk mengaktifkan otentikasi Kerberos untuk klien yang mengakses sistem FSx file Amazon Anda menggunakan alias DNS, Anda harus mengonfigurasi nama utama layanan (SPNs) yang sesuai dengan alias DNS pada objek komputer Active Directory sistem file Anda.

Jika Anda telah SPNs mengonfigurasi alias DNS yang telah ditetapkan ke sistem file lain pada objek komputer di Active Directory, Anda harus terlebih dahulu menghapusnya SPNs sebelum menambahkan SPNs ke objek komputer sistem file Anda. Untuk informasi selengkapnya, lihat Konfigurasikan nama utama layanan (SPNs) untuk Kerberos.

Melihat alias DNS untuk sistem file dan backup

Anda dapat melihat alias DNS yang saat ini terkait dengan sistem file Windows File Server Anda FSx dan backup menggunakan AWS Management Console, the, dan API AWS CLI, seperti yang dijelaskan dalam prosedur berikut.

Untuk melihat alias DNS yang terkait dengan sistem file

- Menggunakan konsol — Pilih sistem file untuk melihat laman detail Sistem file. Pilih tab Jaringan & keamanan untuk melihat Alias DNS.
- Menggunakan CLI atau API - Gunakan perintah `describe-file-system-aliases` CLI atau operasi API. DescribeFileSystemAliases

Untuk melihat alias DNS yang terkait dengan backup

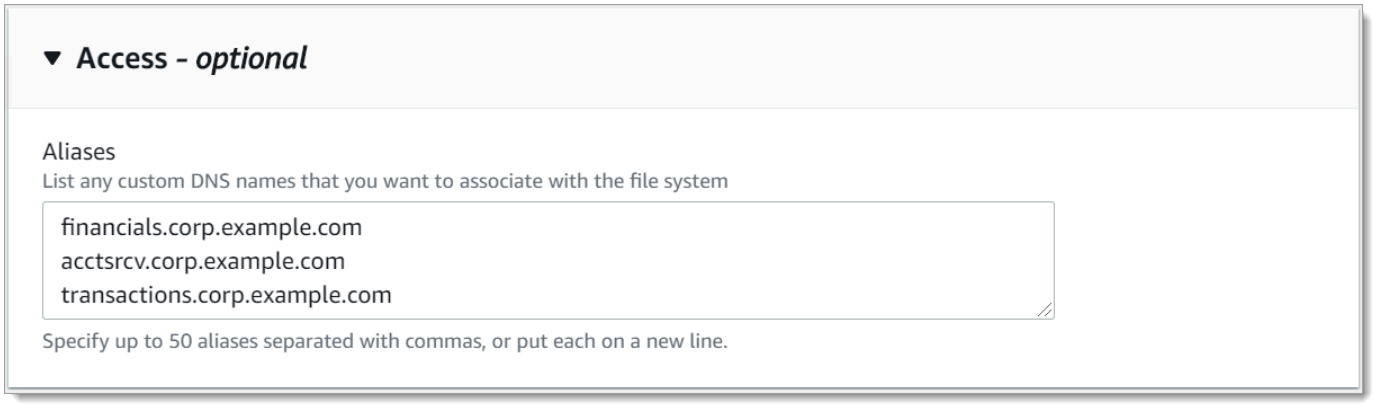
- Menggunakan konsol - Di panel navigasi, pilih Backup, kemudian pilih backup yang ingin Anda lihat. Di panel Ringkasan, lihat kolom Alias DNS.
- Menggunakan CLI atau API - Gunakan perintah `describe-backups` CLI atau operasi API. DescribeBackups

Mengaitkan alias DNS dengan sistem file

Anda dapat mengaitkan alias DNS saat membuat sistem file Windows File Server baru FSx dari awal, atau saat memulihkan cadangan ke sistem file baru, menggunakan,, dan API AWS CLI, menjelaskan prosedur berikut. AWS Management Console

Untuk mengaitkan alias DNS saat membuat sistem file baru (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat sistem file baru yang dijelaskan di Langkah 5. Buat sistem file Anda pada bagian Mulai.
3. Di bagian Akses - opsional dari wizard Buat sistem file, masukkan alias DNS yang ingin Anda kaitkan dengan sistem file Anda.



4. Ketika sistem file tersedia, Anda dapat mengaksesnya menggunakan alias DNS dengan mengkonfigurasi nama utama layanan (SPNs) dan memperbarui atau membuat catatan DNS CNAME untuk alias. Untuk informasi selengkapnya, lihat Mengakses data menggunakan alias DNS.

Untuk mengaitkan alias DNS saat membuat sistem FSx file Amazon (CLI) baru

1. Saat membuat sistem file baru, gunakan properti Alias dengan operasi CreateFileSystemAPI untuk mengaitkan alias DNS dengan sistem file baru.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. Ketika sistem file tersedia, Anda dapat mengaksesnya menggunakan alias DNS dengan mengkonfigurasi nama utama layanan (SPNs) dan memperbarui atau membuat catatan DNS CNAME untuk alias. Untuk informasi selengkapnya, lihat Mengakses data menggunakan alias DNS.

Untuk menambah atau menghapus alias DNS saat memulihkan cadangan (CLI)

1. Saat membuat sistem file baru dari cadangan sistem file yang ada, Anda dapat menggunakan properti Alias dengan operasi CreateFileSystemFromBackupAPI sebagai berikut:

   - Ssetiap alias yang terkait dengan backup dikaitkan dengan sistem file baru secara default.
   - Untuk membuat sistem file tanpa melestarikan alias dari backup, gunakan properti `Aliases` dengan satu set kosong.

     Untuk mengaitkan alias DNS tambahan, gunakan properti `Aliases` dan masukkan kedua alias asli yang terkait dengan backup dan alias baru yang ingin Anda kaitkan.

   Perintah CLI berikut mengaitkan dua alias dengan sistem file yang FSx dibuat Amazon dari cadangan.

```
aws fsx create-file-system-from-backup \
  --backup-id backup-0123456789abcdef0
  --storage-capacity 2000 \
  --storage-type HDD \
  --subnet-ids subnet-123456 \
```

```
  --windows-configuration Aliases=[transactions.corp.example.com,accts-
rcv.corp.example.com]
```

2. Ketika sistem file tersedia, Anda dapat mengaksesnya menggunakan alias DNS dengan mengkonfigurasi nama utama layanan (SPNs) dan memperbarui atau membuat catatan DNS CNAME untuk alias. Untuk informasi selengkapnya, lihat Mengakses data menggunakan alias DNS.

Mengelola alias DNS pada sistem file yang ada

Anda dapat menambahkan dan menghapus alias yang ada FSx untuk sistem file Windows File Server menggunakan AWS Management Console dan AWS CLI, seperti yang dijelaskan dalam prosedur berikut.

Untuk mengelola sistem file DNS alias (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Arahkan ke Sistem file, dan pilih sistem file Windows yang ingin Anda kelola alias DNS.
3. Pada tab Jaringan & keamanan, pilih Kelola untuk alias DNS untuk menampilkan jendela Kelola alias DNS.

   - Untuk mengaitkan alias DNS — Dalam kotak Mengaitkan alias, masukkan alias yang ingin Anda kaitkan. Pilih Kaitkan.
   - Untuk memisahkan alias DNS — dalam daftar Alias saat ini, pilih alias untuk memisahkan darinya. Pilih Pisahkan.

   Anda dapat memantau status alias yang telah Anda kelola di daftar Alias saat ini. Refresh daftar untuk memperbarui status. Dibutuhkan hingga 2,5 menit untuk mengaitkan atau memisahkan alias dengan sistem file.
4. Ketika alias tersedia, Anda dapat mengakses sistem file Anda menggunakan alias DNS dengan mengkonfigurasi nama utama layanan (SPNs) dan memperbarui atau membuat catatan DNS CNAME untuk alias. Untuk informasi selengkapnya, lihat Mengakses data menggunakan alias DNS.

Untuk mengaitkan alias DNS dengan sistem file yang ada (CLI)

1. Gunakan perintah `associate-file-system-aliases` CLI atau operasi AssociateFileSystemAliasesAPI untuk mengaitkan alias DNS dengan sistem file yang ada.

   Permintaan CLI berikut mengaitkan dua alias dengan sistem file yang ditentukan.

   ```
   aws fsx associate-file-system-aliases \
     --file-system-id fs-0123456789abcdef0 \
     --aliases financials.corp.example.com transfers.corp.example.com
   ```

   Respons menunjukkan status alias yang FSx diasosiasikan Amazon dengan sistem file.

   ```
   {
       "Aliases": [
           {
               "Name": "financials.corp.example.com",
               "Lifecycle": CREATING
           },
           {
               "Name": "transfers.corp.example.com",
               "Lifecycle": CREATING
           }
       ]
   }
   ```

2. Gunakan perintah `describe-file-system-aliases` CLI (DescribeFileSystemAliasesadalah operasi API yang setara) untuk memantau status alias yang Anda kaitkan.
3. Ketika `Lifecycle` memiliki nilai AVAILABLE (proses yang dapat memakan waktu hingga 2,5 menit), Anda dapat mengakses sistem file Anda menggunakan alias DNS dengan mengonfigurasi nama utama layanan (SPNs) dan memperbarui atau membuat catatan CNAME DNS untuk alias. Untuk informasi selengkapnya, lihat Mengakses data menggunakan alias DNS.

Untuk memisahkan alias DNS dari sistem file (CLI)

- Gunakan perintah `disassociate-file-system-aliases` CLI atau operasi DisassociateFileSystemAliasesAPI untuk memisahkan alias DNS dari sistem file yang ada.

  Perintah berikut memisahkan satu alias dari sistem file.

```
aws fsx disassociate-file-system-aliases \
  --file-system-id fs-0123456789abcdef0 \
  --aliases financials.corp.example.com
```

Respons menunjukkan status alias yang FSx diputuskan Amazon dari sistem file.

```
{
    "Aliases": [
        {
            "Name": "financials.corp.example.com",
            "Lifecycle": DELETING
        }
    ]
}
```

Gunakan perintah `describe-file-system-aliases` CLI (DescribeFileSystemAliasesadalah operasi API yang setara) untuk memantau status alias. Dibutuhkan hingga 2,5 menit agar alias terhapus.

Sesi pengguna dan file terbuka

Anda dapat memantau sesi pengguna yang terhubung dan membuka file pada sistem file Windows File Server Anda FSx menggunakan alat Folder Bersama. Alat Folder Bersama menyediakan lokasi pusat untuk memantau siapa yang terhubung ke sistem file, bersama dengan file apa yang terbuka dan oleh siapa. Anda dapat melakukan hal ini dengan cara berikut:

- Pulihkan akses ke file terkunci.
- Putuskan sesi pengguna, yang menutup semua file yang dibuka oleh pengguna tersebut.

Anda dapat menggunakan alat GUI Folder Bersama Windows-native dan FSx CLI Amazon untuk manajemen jarak jauh PowerShell untuk mengelola sesi pengguna dan membuka file pada sistem file Windows File Server Anda FSx .

Menggunakan GUI untuk mengelola pengguna dan sesi

Prosedur berikut merinci bagaimana Anda dapat mengelola sesi pengguna dan membuka file di sistem FSx file Amazon Anda menggunakan alat folder bersama Microsoft Windows.

Untuk meluncurkan alat folder bersama

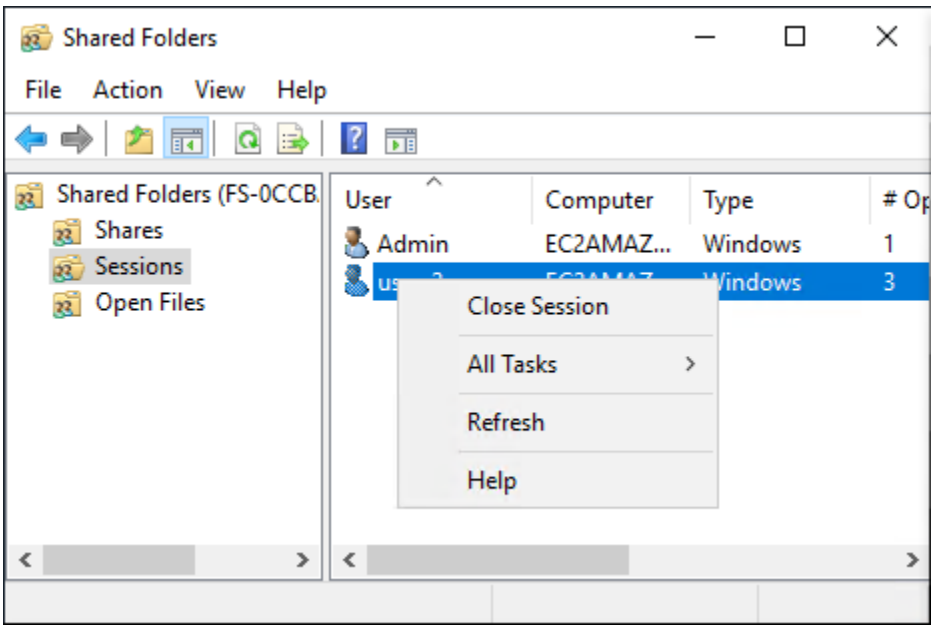
1. Luncurkan EC2 instans Amazon Anda dan sambungkan ke Microsoft Active Directory tempat sistem FSx file Amazon Anda bergabung. Untuk melakukannya, pilih salah satu berikut dari Panduan Administrasi AWS Directory Service :

   - Bergabunglah dengan instans Windows EC2 dengan mulus
   - Bergabung dengan instance Windows secara manual

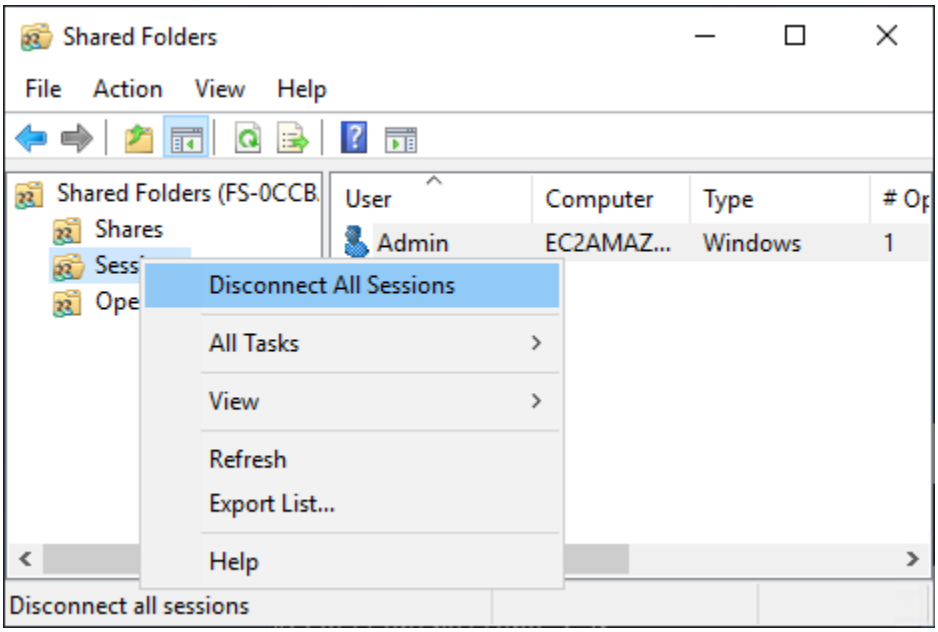
2. Connect ke instans Anda sebagai pengguna yang merupakan anggota dari grup administrator sistem file. Di Direktori Aktif Microsoft AWS Terkelola, grup ini disebut FSx Administrator AWS Delegasi. Di Direktori Aktif Microsoft yang dikelola sendiri, grup ini disebut Admin Domain atau nama kustom untuk grup administrator yang Anda berikan selama pembuatan. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
3. Buka menu start dan jalankan fsmgmt.msc menggunakan `Run As Administrator`. Tindakan ini akan membuka alat GUI Folder Bersama.
4. Untuk Tindakan, pilih Connect ke komputer lain.
5. Untuk Komputer lain, masukkan nama DNS sistem FSx file Amazon Anda, misalnya`fs-`*`012345678901234567`*`.`*`ad-domain`*`.com`.
6. Pilih OKE. Entri untuk sistem FSx file Amazon Anda kemudian muncul dalam daftar untuk alat Folder Bersama.

Untuk mengelola sesi pengguna (GUI)

Di alat Folder Bersama, pilih Sesi untuk melihat semua sesi pengguna yang terhubung ke sistem file Windows File Server Anda FSx . Jika pengguna atau aplikasi mengakses berbagi file di sistem FSx file Amazon Anda, snap-in ini menunjukkan sesi mereka. Anda dapat memutuskan sesi dengan membuka menu konteks (klik kanan) untuk sesi dan memilih Tutup Sesi.

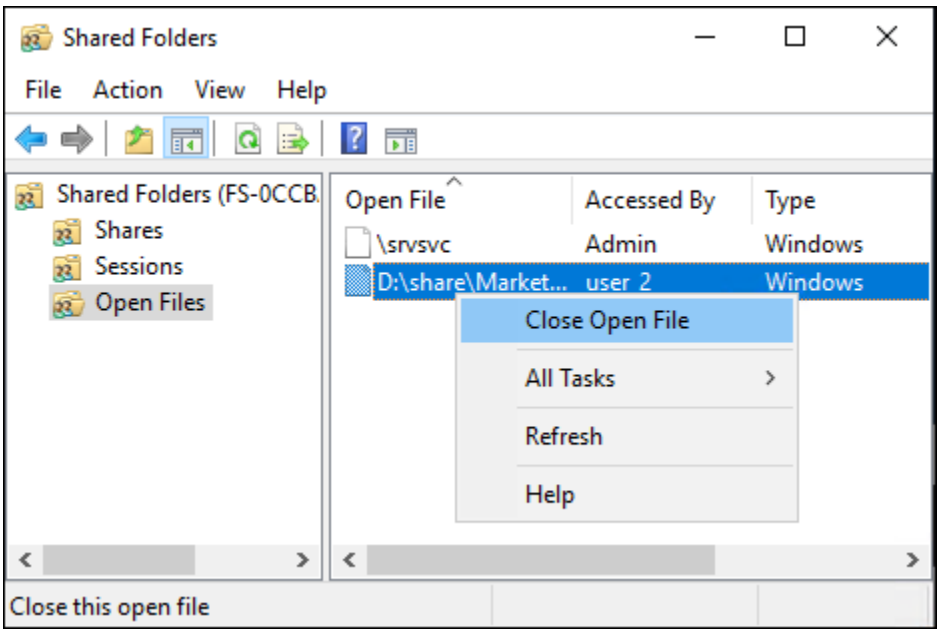


Untuk memutuskan semua sesi yang terbuka, buka menu konteks (klik kanan) untuk Sesi, pilih Putuskan Semua Sesi, dan konfirmasikan tindakan Anda.

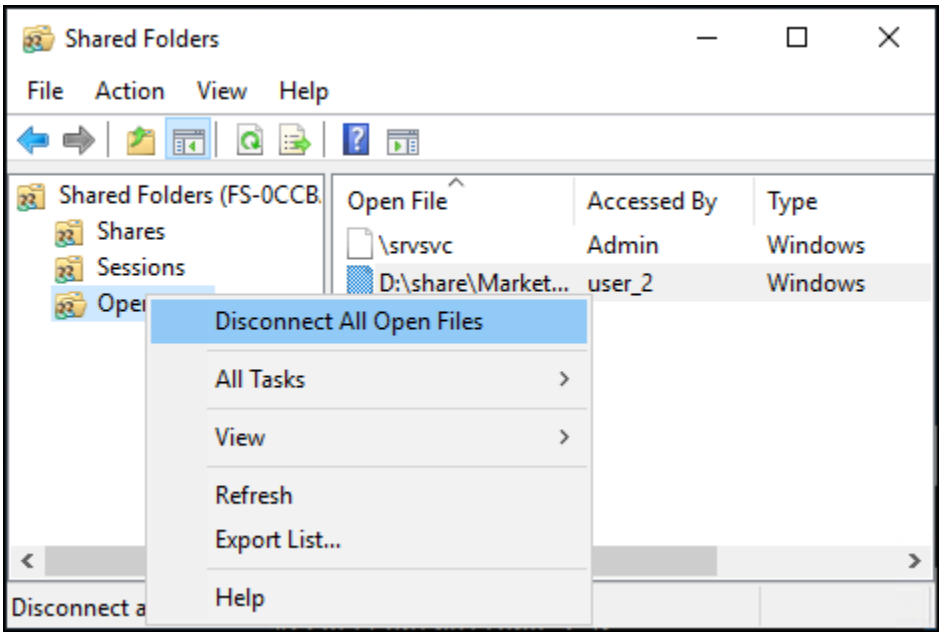


Untuk mengelola file terbuka (GUI)

Di alat Folder Bersama, pilih File Terbuka untuk melihat semua file pada sistem yang saat ini terbuka. Tampilan ini juga menunjukkan pengguna mana yang membuka file atau folder tersebut. Informasi ini dapat membantu dalam melacak mengapa pengguna lain tidak dapat membuka file tertentu. Anda dapat menutup file apa pun yang pengguna buka hanya dengan membuka menu konteks (klik kanan) untuk entri file dalam daftar dan memilih Tutup File yang Terbuka.



Untuk memutuskan semua file yang terbuka pada sistem file, menu konteks (klik kanan) untuk File Terbuka dan Pilih Putuskan Semua File Terbuka, dan konfirmasikan tindakan Anda.



Menggunakan PowerShell untuk mengelola sesi pengguna dan membuka file

Anda dapat mengelola sesi pengguna aktif dan membuka file di sistem file Anda menggunakan Amazon FSx CLI untuk manajemen jarak jauh. PowerShell Untuk mempelajari cara menggunakan CLI ini, lihat Menggunakan Amazon FSx CLI untuk PowerShell.

Berikut ini adalah perintah yang dapat Anda gunakan untuk manajemen sesi pengguna dan file terbuka.

Perintah	Deskripsi
Get-FSxSmbSession	Mengambil informasi tentang sesi Blok Pesan Server (SMB) yang saat ini dibuat antara sistem file dan klien terkait.
Close-FSxSmbSession	Mengakhiri sesi SMB.
Get-FSxSmbOpenFile	Mengambil informasi tentang file yang terbuka untuk klien yang terhubung ke sistem file.
Close-FSxSmbOpenFile	Menutup file yang terbuka untuk salah satu klien server SMB.

Bantuan online untuk setiap perintah memberikan referensi dari semua opsi perintah. Untuk mengakses bantuan ini, jalankan perintah dengan -?, misalnya Get-FSxSmbSession -?.

Mengelola penyimpanan FSx untuk Windows File Server

Konfigurasi penyimpanan sistem file Anda mencakup jumlah kapasitas penyimpanan yang disediakan, jenis penyimpanan, dan jika jenis penyimpanan adalah solid state drive (SSD), jumlah IOPS SSD. Anda dapat mengonfigurasi sumber daya ini, bersama dengan kapasitas throughput sistem file, saat membuat sistem file dan setelah dibuat, untuk mencapai kinerja yang diinginkan untuk beban kerja Anda. Pelajari cara mengelola penyimpanan sistem file dan kinerja terkait penyimpanan menggunakan AWS Management Console, AWS CLI, dan Amazon FSx CLI untuk pengelolaan jarak jauh PowerShell dengan menjelajahi topik-topik berikut.

Topik

- Meningkatkan kapasitas penyimpanan sistem file
- Memantau peningkatan kapasitas penyimpanan
- Meningkatkan kapasitas penyimpanan sistem file FSx Windows File Server secara dinamis
- Memperbarui jenis penyimpanan sistem file FSx untuk Windows
- Memantau pembaruan jenis penyimpanan
- Memperbarui IOPS SSD sistem file
- Memantau pembaruan IOPS SSD yang disediakan
- Mengelola deduplikasi data
- Menyelesaikan masalah deduplikasi data

Mengoptimalkan biaya penyimpanan

Anda dapat mengoptimalkan biaya penyimpanan menggunakan opsi konfigurasi penyimpanan yang tersedia FSx untuk Windows.

Opsi jenis penyimpanan - FSx untuk Windows File Server menyediakan dua jenis penyimpanan, hard disk drive (HDD) dan solid state drive (SSD) - untuk memungkinkan Anda mengoptimalkan biaya/kinerja untuk memenuhi kebutuhan beban kerja Anda. Penyimpanan HDD dirancang untuk spektrum beban kerja yang luas, termasuk direktori beranda, berbagi pengguna dan departemen, dan sistem pengelolaan konten. Penyimpanan SSD dirancang untuk beban kerja dengan performa tertinggi dan paling sensitif terhadap latensi, termasuk basis data, beban kerja pemrosesan media, dan aplikasi analitik data. Untuk informasi selengkapnya tentang jenis penyimpanan dan kinerja sistem file, lihatFSx untuk kinerja Windows File Server.

Deduplikasi data —Dataset besar sering memiliki data yang berlebihan, yang meningkatkan biaya penyimpanan data. Misalnya, pembagian file pengguna dapat menyimpan banyak salinan file yang sama, yang disimpan beberapa pengguna. Pembagian pembangunan perangkat lunak dapat berisi banyak biner yang tetap tidak berubah dari bangunan ke bangunan. Anda dapat mengurangi biaya penyimpanan data dengan menyalakan deduplikasi data untuk sistem file Anda. Saat dinyalakan, deduplikasi data secara otomatis mengurangi atau menghilangkan data berulang dengan menyimpan bagian duplikat dari set data hanya sekali. Untuk informasi selengkapnya tentang deduplikasi data, dan cara mengaktifkannya dengan mudah untuk sistem FSx file Amazon Anda, lihat. Mengurangi biaya penyimpanan dengan Data Deduplication

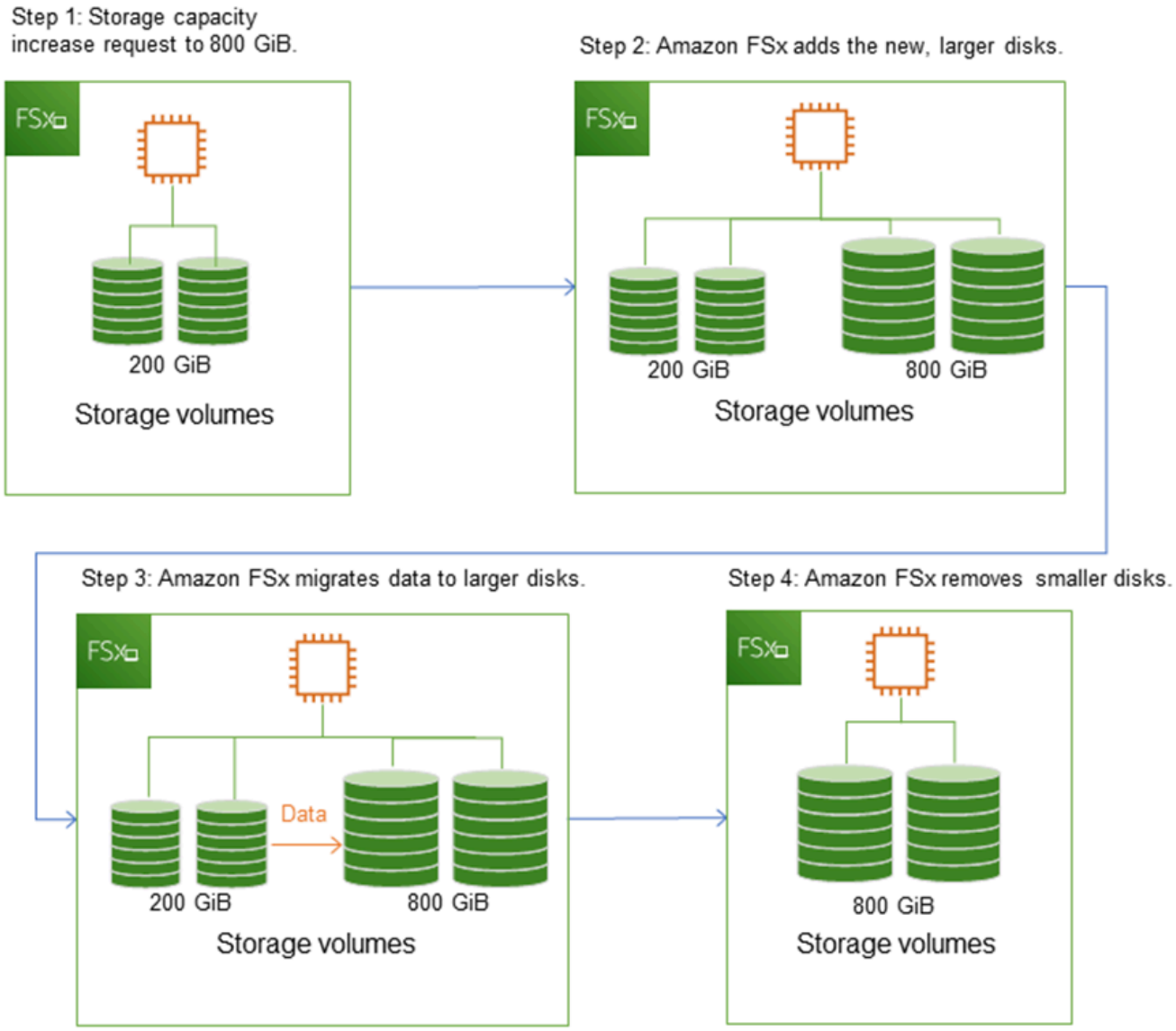
Mengelola kapasitas penyimpanan

Anda dapat meningkatkan kapasitas penyimpanan sistem file Windows Anda saat kebutuhan penyimpanan Anda berubah. FSx Anda dapat melakukannya menggunakan FSx konsol Amazon, Amazon FSx API, atau AWS Command Line Interface (AWS CLI). Faktor-faktor yang perlu dipertimbangkan saat merencanakan peningkatan kapasitas penyimpanan termasuk mengetahui kapan Anda perlu meningkatkan kapasitas penyimpanan, memahami bagaimana Amazon FSx memproses peningkatan kapasitas penyimpanan, dan melacak kemajuan permintaan peningkatan penyimpanan. Anda hanya dapat meningkatkan kapasitas penyimpanan sistem file; Anda tidak dapat mengurangi kapasitas penyimpanan.

> **Note**
>
> Anda tidak dapat meningkatkan kapasitas penyimpanan untuk sistem file yang dibuat sebelum 23 Juni 2019 atau sistem file dipulihkan dari cadangan milik sistem file yang dibuat sebelum 23 Juni 2019.

Saat Anda meningkatkan kapasitas penyimpanan sistem FSx file Amazon Anda, Amazon FSx menambahkan set disk baru yang lebih besar ke sistem file Anda di belakang layar. Amazon FSx kemudian menjalankan proses pengoptimalan penyimpanan di latar belakang untuk memigrasikan data secara transparan dari disk lama ke disk baru. Optimalisasi penyimpanan dapat memakan waktu antara beberapa jam dan beberapa hari, tergantung pada jenis penyimpanan dan faktor lainnya, dengan dampak nyata minimal pada kinerja beban kerja. Selama optimasi ini, penggunaan cadangan untuk sementara lebih tinggi, karena volume penyimpanan lama dan baru disertakan dalam cadangan tingkat sistem file. Kedua set volume penyimpanan disertakan untuk memastikan bahwa Amazon FSx dapat berhasil mengambil dan memulihkan dari cadangan bahkan selama aktivitas penskalaan penyimpanan. Penggunaan cadangan kembali ke tingkat dasar sebelumnya setelah volume penyimpanan lama tidak lagi disertakan dalam riwayat cadangan. Ketika kapasitas penyimpanan baru tersedia, Anda akan ditagih hanya untuk kapasitas penyimpanan yang baru.

Ilustrasi berikut menunjukkan empat langkah utama dari proses yang FSx digunakan Amazon saat meningkatkan kapasitas penyimpanan sistem file.



Anda dapat melacak kemajuan pengoptimalan penyimpanan, peningkatan kapasitas penyimpanan SSD, atau pembaruan IOPS SSD kapan saja menggunakan FSx konsol Amazon, CLI, atau API. Untuk informasi selengkapnya, lihat Memantau peningkatan kapasitas penyimpanan.

Apa yang perlu diketahui tentang meningkatkan kapasitas penyimpanan sistem file

Berikut adalah beberapa item penting yang perlu dipertimbangkan saat meningkatkan kapasitas penyimpanan:

- Hanya meningkatkan — Anda hanya dapat meningkatkan jumlah kapasitas penyimpanan untuk sistem file; Anda tidak dapat mengurangi kapasitas penyimpanan.
- Peningkatan minimum — Setiap peningkatan kapasitas penyimpanan harus sedikitnya 10 persen dari kapasitas penyimpanan sistem file saat ini, hingga maksimal nilai yang diizinkan adalah sebesar 65.536 GiB.
- Kapasitas throughput minimum — Untuk meningkatkan kapasitas penyimpanan, sistem file harus memiliki kapasitas throughput minimum 16. MBps Hal ini karena langkah optimasi penyimpanan adalah proses intensif throughput.
- Jeda waktu antar peningkatan — Anda tidak dapat meningkatkan kapasitas penyimpanan lebih lanjut pada sistem file hingga 6 jam setelah permintaan peningkatan terakhir, atau hingga proses optimasi penyimpanan selesai, mana saja yang lebih lama. Optimalisasi penyimpanan dapat memakan waktu dari beberapa jam hingga beberapa hari untuk menyelesaikannya. Untuk meminimalkan waktu yang diperlukan agar pengoptimalan penyimpanan selesai, kami sarankan untuk meningkatkan kapasitas throughput sistem file Anda sebelum meningkatkan kapasitas penyimpanan (kapasitas throughput dapat diperkecil kembali setelah penskalaan penyimpanan selesai), dan meningkatkan kapasitas penyimpanan ketika ada lalu lintas minimal pada sistem file.

> **Note**
>
> Peristiwa sistem file tertentu dapat menggunakan sumber daya kinerja I/O disk Misalnya: Fase optimasi penskalaan kapasitas penyimpanan dapat menghasilkan peningkatan throughput disk, dan berpotensi menyebabkan peringatan kinerja. Untuk informasi selengkapnya, lihat Peringatan dan rekomendasi kinerja.

Mengetahui kapan harus meningkatkan kapasitas penyimpanan

Tingkatkan kapasitas penyimpanan sistem file Anda saat kapasitas penyimpanan gratis tinggal sedikit. Gunakan `FreeStorageCapacity` CloudWatch metrik untuk memantau jumlah penyimpanan gratis yang tersedia di sistem file. Anda dapat membuat CloudWatch alarm Amazon pada metrik ini dan mendapatkan pemberitahuan saat turun di bawah ambang batas tertentu. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

Kami merekomendasikan untuk mempertahankan setidaknya 20% dari kapasitas penyimpanan gratis setiap saat di sistem file Anda. Menggunakan semua kapasitas penyimpanan Anda dapat berdampak negatif pada kinerja Anda dan mungkin menimbulkan ketidakkonsistenan data.

Anda dapat secara otomatis meningkatkan kapasitas penyimpanan sistem file Anda ketika jumlah kapasitas penyimpanan gratis turun di bawah ambang batas yang ditentukan yang Anda tentukan. Gunakan AWS CloudFormation template kustom yang AWS dikembangkan untuk menyebarkan semua komponen yang diperlukan untuk mengimplementasikan solusi otomatis. Untuk informasi selengkapnya, lihat Meningkatkan kapasitas penyimpanan secara dinamis.

Kapasitas penyimpanan meningkat dan performa sistem file

Sebagian besar beban kerja mengalami dampak kinerja minimal sementara Amazon FSx menjalankan proses pengoptimalan penyimpanan di latar belakang setelah kapasitas penyimpanan baru tersedia. Namun, sistem file dengan jenis penyimpanan HDD dan beban kerja yang melibatkan sejumlah besar pengguna akhir, I/O tingkat tinggi, atau kumpulan data yang memiliki sejumlah besar file kecil untuk sementara dapat mengalami penurunan kinerja. Untuk kasus ini, sebaiknya Anda terlebih dahulu meningkatkan kapasitas throughput sistem file Anda sebelum meningkatkan kapasitas penyimpanan. Untuk jenis beban kerja ini, kami juga merekomendasikan untuk mengubah kapasitas throughput selama periode idle ketika ada beban minimal pada sistem file Anda. Hal ini memungkinkan Anda untuk terus menyediakan throughput di tingkat yang sama untuk memenuhi kebutuhan performa aplikasi Anda. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Mengelola jenis penyimpanan sistem file Anda

Anda dapat mengubah jenis penyimpanan sistem file Anda dari HDD ke SSD menggunakan AWS Management Console dan AWS CLI. Saat Anda mengubah jenis penyimpanan menjadi SSD, ingatlah bahwa Anda tidak dapat memperbarui konfigurasi sistem file lagi hingga 6 jam setelah pembaruan terakhir diminta, atau hingga proses pengoptimalan penyimpanan selesai — waktu mana pun yang lebih lama. Optimalisasi penyimpanan dapat memakan waktu antara beberapa jam dan beberapa hari untuk menyelesaikannya. Untuk meminimalkan waktu ini, kami sarankan memperbarui jenis penyimpanan Anda ketika ada lalu lintas minimal pada sistem file Anda. Untuk informasi selengkapnya, lihat Memperbarui jenis penyimpanan sistem file FSx untuk Windows.

Anda tidak dapat mengubah jenis penyimpanan sistem file Anda dari SSD ke HDD. Jika Anda ingin mengubah jenis penyimpanan sistem file dari SSD ke HDD, Anda perlu mengembalikan cadangan sistem file ke sistem file baru yang Anda konfigurasikan untuk menggunakan penyimpanan HDD. Untuk informasi selengkapnya, lihat Memulihkan backup ke sistem file baru.

Tentang jenis penyimpanan

Anda dapat mengonfigurasi sistem file Windows File Server Anda FSx untuk menggunakan jenis penyimpanan solid state drive (SSD) atau hard disk drive magnetik (HDD).

Penyimpanan SSD sesuai untuk sebagian besar beban kerja produksi yang memiliki persyaratan kinerja tinggi dan sensitivitas latensi. Contoh beban kerja ini termasuk database, analisis data, pemrosesan media, dan aplikasi bisnis. Kami juga merekomendasikan SSD untuk kasus penggunaan yang melibatkan sejumlah besar pengguna akhir, I/O tingkat tinggi, atau kumpulan data yang memiliki sejumlah besar file kecil. Terakhir, kami sarankan menggunakan penyimpanan SSD jika Anda berencana untuk mengaktifkan salinan bayangan. Anda dapat mengonfigurasi dan menskalakan SSD IOPS untuk sistem file dengan penyimpanan SSD, tetapi bukan penyimpanan HDD.

Penyimpanan HDD dirancang untuk berbagai beban kerja — termasuk direktori rumah, berbagi file pengguna dan departemen, dan sistem manajemen konten. Penyimpanan HDD datang dengan biaya yang lebih rendah dibandingkan dengan penyimpanan SSD, tetapi dengan latensi yang lebih tinggi dan tingkat throughput disk dan IOPS disk yang lebih rendah per unit penyimpanan. Ini mungkin cocok untuk berbagi pengguna tujuan umum dan direktori rumah dengan persyaratan I/O rendah, sistem manajemen konten besar (CMS) di mana data jarang diambil, atau kumpulan data dengan sejumlah kecil file besar.

Untuk informasi selengkapnya, lihat Konfigurasi & kinerja penyimpanan.

Mengelola SSD IOPS

Untuk sistem file yang dikonfigurasi dengan penyimpanan SSD, jumlah IOPS SSD menentukan jumlah disk I/O yang tersedia ketika sistem file Anda harus membaca data dari dan menulis data ke disk, sebagai lawan dari data yang ada dalam cache. Anda dapat memilih dan menskalakan jumlah IOPS SSD secara independen dari kapasitas penyimpanan. IOPS SSD maksimum yang dapat Anda berikan tergantung pada jumlah kapasitas penyimpanan dan kapasitas throughput yang Anda pilih untuk sistem file Anda. Jika Anda mencoba meningkatkan IOPS SSD Anda di atas batas yang didukung oleh kapasitas throughput Anda, Anda mungkin perlu meningkatkan kapasitas throughput Anda untuk mendapatkan tingkat IOPS SSD tersebut. Untuk informasi selengkapnya, silakan lihat FSx untuk kinerja Windows File Server dan Mengelola kapasitas throughput.

Berikut adalah beberapa hal penting yang perlu diketahui tentang memperbarui IOPS SSD yang disediakan sistem file:

- Memilih mode IOPS — ada dua mode IOPS untuk dipilih:

  - Otomatis - pilih mode ini dan Amazon FSx akan secara otomatis menskalakan IOPS SSD Anda untuk mempertahankan 3 IOPS SSD per GiB kapasitas penyimpanan, hingga 400.000 IOPS SSD per sistem file.
  - User-provisioned — pilih mode ini sehingga Anda dapat menentukan jumlah IOPS SSD dalam kisaran 96-400.000. Tentukan angka antara 3—50 IOPS per GiB kapasitas penyimpanan untuk semua tempat Wilayah AWS Amazon FSx tersedia, atau antara 3—500 IOPS per GiB kapasitas penyimpanan di AS Timur (Virginia N.), AS Barat (Oregon), AS Timur (Ohio), Eropa (Irlandia), Asia Pasifik (Tokyo), dan Asia Pasifik (Singapura). Saat Anda memilih mode yang disediakan pengguna, dan jumlah IOPS SSD yang Anda tentukan tidak setidaknya 3 IOPS per GiB, permintaan gagal. Untuk tingkat IOPS SSD yang disediakan lebih tinggi, Anda membayar IOPS rata-rata di atas 3 IOPS per GiB per sistem file.
- Pembaruan kapasitas penyimpanan - Jika Anda meningkatkan kapasitas penyimpanan sistem file Anda, dan jumlahnya secara default memerlukan sejumlah IOPS SSD yang lebih besar dari tingkat IOPS SSD yang disediakan pengguna saat ini, Amazon FSx secara otomatis mengalihkan sistem file Anda ke mode Otomatis dan sistem file Anda akan memiliki minimal 3 SSD IOPS per GiB kapasitas penyimpanan.
- Pembaruan kapasitas throughput — Jika Anda meningkatkan kapasitas throughput, dan IOPS SSD maksimum yang didukung oleh kapasitas throughput baru Anda lebih tinggi daripada level IOPS SSD yang disediakan pengguna, FSx Amazon secara otomatis mengalihkan sistem file Anda ke mode Otomatis.
- Frekuensi IOPS SSD meningkat — Anda tidak dapat meningkatkan IOPS SSD lebih lanjut, peningkatan kapasitas throughput, atau pembaruan jenis penyimpanan pada sistem file hingga 6 jam setelah peningkatan terakhir diminta, atau hingga proses pengoptimalan penyimpanan selesai — waktu mana pun yang lebih lama. Optimalisasi penyimpanan dapat memakan waktu dari beberapa jam hingga beberapa hari untuk menyelesaikannya. Untuk meminimalkan waktu yang diperlukan agar pengoptimalan penyimpanan selesai, kami merekomendasikan penskalaan SSD IOPS ketika ada lalu lintas minimal pada sistem file.

> **Note**
>
> Perhatikan bahwa tingkat kapasitas throughput 4.608 MBps dan lebih tinggi hanya didukung sebagai berikut Wilayah AWS: AS Timur (Virginia N.), AS Barat (Oregon), AS Timur (Ohio), Eropa (Irlandia), Asia Pasifik (Tokyo), dan Asia Pasifik (Singapura).

Untuk informasi selengkapnya tentang cara memperbarui jumlah IOPS SSD yang disediakan untuk sistem file Windows File Server Anda FSx , lihat. Memperbarui IOPS SSD sistem file

Mengurangi biaya penyimpanan dengan Data Deduplication

Deduplikasi Data, sering disebut sebagai Dedup untuk jangka pendek, membantu administrator penyimpanan mengurangi biaya yang terkait dengan data duplikat. Dengan FSx Windows File Server, Anda dapat menggunakan Microsoft Data Deduplication untuk mengidentifikasi dan menghilangkan data yang berlebihan. Set data besar sering memiliki data berulang, yang meningkatkan biaya penyimpanan data. Sebagai contoh:

- Berbagi file pengguna mungkin memiliki banyak salinan dari file yang sama atau serupa.
- Saham pengembangan perangkat lunak dapat memiliki banyak binari yang tetap tidak berubah dari build ke build.

Anda dapat mengurangi biaya penyimpanan data dengan mengaktifkan deduplikasi data untuk sistem file Anda. Deduplikasi data mengurangi atau menghilangkan data berulang dengan menyimpan bagian duplikat dari set data hanya sekali. Saat Anda mengaktifkan Deduplikasi Data, kompresi data diaktifkan secara default, mengompresi data setelah deduplikasi untuk penghematan tambahan. Deduplikasi Data mengoptimalkan redundansi tanpa mengorbankan kesetiaan atau integritas data. Deduplikasi data berjalan sebagai proses latar belakang yang secara terus-menerus dan otomatis memindai dan mengoptimalkan sistem file Anda, dan transparan bagi pengguna Anda dan klien yang terhubung.

Penghematan penyimpanan yang dapat Anda capai dengan deduplikasi data tergantung pada sifat set data Anda, termasuk berapa banyak duplikasi yang ada di seluruh file. Penghematan umum rata-rata 50–60 persen untuk pembagian file tujuan umum. Dalam pembagian, penghematan berkisar antara 30–50 persen untuk dokumen pengguna hingga 70–80 persen untuk set data pengembangan perangkat lunak. Anda dapat mengukur potensi penghematan deduplikasi menggunakan PowerShell perintah `Measure-FSxDedupFileMetadata` jarak jauh yang dijelaskan di bawah ini.

Anda juga dapat menyesuaikan deduplikasi data untuk memenuhi kebutuhan penyimpanan spesifik Anda. Misalnya, Anda dapat mengonfigurasi deduplikasi untuk dijalankan hanya pada jenis file tertentu, atau Anda dapat membuat jadwal pekerjaan khusus. Karena pekerjaan deduplikasi dapat menggunakan sumber daya server file, kami sarankan untuk memantau status pekerjaan deduplikasi Anda menggunakan file. `Get-FSxDedupStatus`

Untuk informasi tentang mengonfigurasi deduplikasi data pada sistem file Anda, lihat. Mengelola deduplikasi data

Untuk informasi tentang penyelesaian masalah yang terkait dengan deduplikasi data, lihat.

Gunakan informasi berikut untuk membantu memecahkan masalah umum saat mengonfigurasi dan menggunakan deduplikasi data.

Topik

- Deduplikasi data tidak berfungsi
- Nilai deduplikasi secara tak terduga disetel ke 0
- Ruang tidak dibebaskan pada sistem file setelah menghapus file

Deduplikasi data tidak berfungsi

Untuk melihat status deduplikasi data saat ini, jalankan `Get-FSxDedupStatus` PowerShell perintah untuk melihat status penyelesaian untuk pekerjaan deduplikasi terbaru. Jika satu atau lebih pekerjaan gagal, Anda mungkin tidak melihat peningkatan kapasitas penyimpanan gratis pada sistem file Anda.

Alasan paling umum untuk pekerjaan deduplikasi gagal adalah memori yang tidak mencukupi.

- Microsoft merekomendasikan secara optimal memiliki 1 GB memori per 1 TB data logis (atau minimal 350 MB per 1 TB data logis). Gunakan tabel FSx kinerja Amazon untuk menentukan memori yang terkait dengan kapasitas throughput sistem file Anda dan memastikan sumber daya memori cukup untuk ukuran data Anda. Jika tidak, Anda perlu meningkatkan kapasitas throughput sistem file ke tingkat yang memenuhi persyaratan memori 1 GB per 1 TB data logis.
- Pekerjaan deduplikasi dikonfigurasi dengan default Windows yang direkomendasikan dari alokasi memori 25%, yang berarti bahwa untuk sistem file dengan memori 32 GB, 8 GB akan tersedia untuk deduplikasi. Alokasi memori dapat dikonfigurasi (menggunakan `Set-FSxDedupSchedule` perintah dengan parameter`-Memory`). Ketahuilah bahwa menggunakan alokasi memori yang lebih tinggi untuk dedup dapat memengaruhi kinerja sistem file.
- Anda dapat memodifikasi konfigurasi pekerjaan deduplikasi untuk mengurangi jumlah memori yang diperlukan. Misalnya, Anda dapat membatasi pengoptimalan agar berjalan pada jenis file atau folder tertentu, atau menetapkan ukuran dan usia file minimum untuk pengoptimalan. Kami juga merekomendasikan mengonfigurasi pekerjaan deduplikasi untuk dijalankan selama periode idle ketika ada beban minimal pada sistem file Anda.

Anda juga dapat melihat kesalahan jika pekerjaan deduplikasi tidak memiliki waktu yang cukup untuk diselesaikan. Anda mungkin perlu mengubah durasi maksimum pekerjaan, seperti yang dijelaskan dalamMengubah jadwal deduplikasi data.

Jika pekerjaan deduplikasi telah gagal untuk jangka waktu yang lama, dan telah ada perubahan pada data pada sistem file selama periode ini, pekerjaan deduplikasi berikutnya mungkin memerlukan lebih banyak sumber daya untuk menyelesaikan dengan sukses untuk pertama kalinya.

Nilai deduplikasi secara tak terduga disetel ke 0

Nilai untuk `SavedSpace` dan `OptimizedFilesSavingsRate` tiba-tiba 0 untuk sistem file di mana Anda telah mengkonfigurasi deduplikasi data.

Hal ini dapat terjadi selama proses optimasi penyimpanan ketika Anda meningkatkan kapasitas penyimpanan sistem file. Saat Anda meningkatkan kapasitas penyimpanan sistem file, Amazon FSx membatalkan pekerjaan deduplikasi data yang ada selama proses pengoptimalan penyimpanan, yang memigrasikan data dari disk lama ke disk baru yang lebih besar. Amazon FSx melanjutkan deduplikasi data pada sistem file setelah pekerjaan pengoptimalan penyimpanan selesai. Untuk informasi selengkapnya tentang peningkatan kapasitas penyimpanan dan optimasi penyimpanan, lihat Mengelola kapasitas penyimpanan.

Ruang tidak dibebaskan pada sistem file setelah menghapus file

Perilaku deduplikasi data yang diharapkan adalah jika data yang dihapus adalah sesuatu yang dedup telah menghemat ruang, maka ruang tersebut tidak benar-benar dibebaskan pada sistem file Anda sampai pekerjaan pengumpulan sampah berjalan.

Praktek yang mungkin membantu Anda adalah mengatur jadwal untuk menjalankan pekerjaan pengumpulan sampah tepat setelah Anda menghapus sejumlah besar file. Setelah pekerjaan pengumpulan sampah selesai, Anda dapat mengatur jadwal pengumpulan sampah kembali ke pengaturan semula. Hal ini memastikan Anda dapat dengan cepat melihat ruang dari penghapusan Anda.

Gunakan prosedur berikut untuk mengatur pekerjaan pengumpulan sampah untuk berjalan dalam 5 menit.

1. Untuk memastikan bahwa deduplikasi data diaktifkan, gunakan perintah `Get-FSxDedupStatus`. Untuk informasi lebih lanjut tentang perintah dan output yang diharapkan, lihat Menampilkan jumlah ruang yang dihemat.

2. Gunakan yang berikut ini untuk mengatur jadwal untuk menjalankan pekerjaan pengumpulan sampah 5 menit dari sekarang.

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. Setelah pekerjaan pengumpulan sampah telah berjalan dan ruang telah dibebaskan, atur jadwal kembali ke pengaturan aslinya.

Untuk informasi selengkapnya tentang deduplikasi data, lihat dokumentasi Microsoft Understanding Data Deduplication.

> **Warning**
>
> Tidak disarankan untuk menjalankan perintah Robocopy tertentu dengan deduplikasi data karena perintah ini dapat memengaruhi integritas data dari Chunk Store. Untuk informasi selengkapnya, lihat dokumentasi interoperabilitas Microsoft Data Deduplication.

Praktik terbaik saat menggunakan deduplikasi data

Berikut adalah beberapa praktik terbaik untuk menggunakan Data Deduplication:

- Jadwalkan pekerjaan Deduplikasi Data untuk dijalankan saat sistem file Anda menganggur: Jadwal default mencakup `GarbageCollection` pekerjaan mingguan di 2:45 UTC pada hari Sabtu. Diperlukan beberapa jam untuk menyelesaikannya jika Anda memiliki sejumlah besar churn data di sistem file Anda. Jika waktu ini tidak ideal untuk beban kerja Anda, jadwalkan pekerjaan ini untuk berjalan pada saat Anda mengharapkan lalu lintas rendah pada sistem file Anda.
- Konfigurasikan kapasitas throughput yang cukup untuk menyelesaikan Deduplikasi Data: Kapasitas throughput yang lebih tinggi memberikan tingkat memori yang lebih tinggi. Microsoft merekomendasikan memiliki 1 GB memori per 1 TB data logis untuk menjalankan Data Deduplication. Gunakan tabel FSx kinerja Amazon untuk menentukan memori yang terkait dengan

kapasitas throughput sistem file Anda dan memastikan bahwa sumber daya memori cukup untuk ukuran data Anda.

- Sesuaikan pengaturan Deduplikasi Data untuk memenuhi kebutuhan penyimpanan spesifik Anda dan mengurangi persyaratan kinerja: Anda dapat membatasi pengoptimalan untuk berjalan pada jenis file atau folder tertentu, atau menetapkan ukuran dan usia file minimum untuk pengoptimalan. Untuk mempelajari selengkapnya, lihat Mengurangi biaya penyimpanan dengan Data Deduplication.

Mengelola kuota penyimpanan

Anda dapat mengkonfigurasi kuota penyimpanan pengguna pada sistem file Anda untuk membatasi berapa banyak penyimpanan data yang dapat dipakai para pengguna. Setelah menetapkan kuota, Anda dapat melacak status kuota untuk memantau penggunaan dan melihat kapan para pengguna melampaui kuota mereka.

Anda juga dapat menerapkan kuota dengan menghentikan pengguna yang mencapai kuota mereka sehingga tidak dapat menulis ke ruang penyimpanan. Ketika Anda menegakkan kuota, pengguna yang melebihi kuota mereka menerima pesan galat "ruang disk tidak cukup".

Anda dapat mengatur ambang batas ini untuk pengaturan kuota:

- Peringatan — digunakan untuk melacak apakah pengguna atau grup mendekati batas kuota mereka, hanya relevan untuk pelacakan.
- Limit — batas kuota penyimpanan untuk pengguna atau grup.

Anda dapat mengkonfigurasi kuota default yang diterapkan untuk pengguna baru yang mengakses sistem file dan kuota yang berlaku untuk pengguna atau grup tertentu. Anda juga dapat melihat laporan berapa banyak penyimpanan yang dipakai setiap pengguna atau grup dan apakah mereka melampaui kuota.

Pemakaian penyimpanan pada tingkat pengguna dilacak berdasarkan kepemilikan file. Pemakaian penyimpanan dihitung dengan menggunakan ukuran file logis, bukan ruang penyimpanan fisik yang sebenarnya ditempati file. Kuota penyimpanan pengguna dilacak pada saat data ditulis ke file.

Memperbarui kuota untuk beberapa pengguna memerlukan menjalankan perintah pembaruan sekali untuk setiap pengguna, atau mengatur pengguna ke dalam grup dan memperbarui kuota untuk grup tersebut.

Anda dapat mengelola kuota penyimpanan pengguna pada sistem file Anda menggunakan Amazon FSx CLI untuk manajemen jarak jauh. PowerShell Untuk mempelajari cara menggunakan CLI ini, lihat Menggunakan Amazon FSx CLI untuk PowerShell.

Berikut ini adalah perintah yang dapat Anda gunakan untuk mengelola kuota penyimpanan pengguna.

Perintah kuota penyimpanan pengguna	Deskripsi
Enable-FSxUserQuotas	Mulai pelacakan dan pemberlakuan kuota penyimpanan pengguna, atau keduanya.
Disable-FSxUserQuotas	Hentikan pelacakan dan pemberlakuan kuota penyimpanan pengguna.
Get-FSxUserQuotaSettings	Mengambil pengaturan kuota penyimpanan pengguna saat ini untuk sistem file.
Get-FSxUserQuotaEntries	Mengambil entri kuota penyimpanan pengguna saat ini untuk pengguna individu dan kelompok pada sistem file.
Set-FSxUserQuotas	Mengatur kuota penyimpanan pengguna untuk pengguna individu atau grup. Nilai kuota ditentukan dalam byte.

Bantuan online untuk setiap perintah memberikan referensi dari semua opsi perintah. Untuk mengakses bantuan ini, jalankan perintah dengan -?, misalnya Enable-FSxUserQuotas -?.

Meningkatkan kapasitas penyimpanan sistem file

Anda dapat meningkatkan kapasitas penyimpanan sistem file Windows File Server Anda saat persyaratan penyimpanan Anda berubah. FSx Gunakan FSx konsol Amazon, FSx API Amazon AWS CLI, atau Amazon untuk meningkatkan kapasitas penyimpanan sistem file seperti yang dijelaskan dalam prosedur berikut. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan.

Untuk meningkatkan kapasitas penyimpanan untuk sistem file (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.

2. Arahkan ke Sistem file dan pilih sistem file Windows yang ingin Anda tingkatkan kapasitas penyimpanannya.
3. Untuk Tindakan, pilih perbarui penyimpanan. Atau, di panel Ringkasan, pilih Perbarui di sebelah Kapasitas penyimpanan sistem file.

   Jendela Perbarui kapasitas penyimpanan muncul.
4. Untuk Jenis input, pilih Persentase untuk memasukkan kapasitas penyimpanan baru sebagai perubahan persentase dari nilai saat ini, atau pilih absolut untuk memasukkan nilai baru dalam GiB.
5. Masukkan Kapasitas penyimpanan yang diinginkan.

   > **Note**
   >
   > Nilai kapasitas yang diinginkan minimal harus 10 persen lebih besar dari nilai saat ini, hingga nilai maksimum 65.536 GiB.
6. Pilih Perbarui untuk melakukan pembaruan kapasitas penyimpanan.
7. Anda dapat memantau kemajuan pembaruan di detail halaman Sistem file, di tab Pembaruan.

Untuk meningkatkan kapasitas penyimpanan untuk sistem file (CLI)

Untuk meningkatkan kapasitas penyimpanan FSx untuk sistem file Windows File Server untuk Windows, gunakan AWS CLI perintah update-file-system. Atur parameter berikut:

- `--file-system-id` ke ID dari sistem file yang Anda perbarui.
- `--storage-capacity` untuk nilai yang setidaknya 10 persen lebih besar dari nilai saat ini.

Anda dapat memantau kemajuan pembaruan dengan menggunakan AWS CLI perintah describe-file-systems. Cari `administrative-actions` di output.

Untuk informasi selengkapnya, lihat AdministrativeAction.

Memantau peningkatan kapasitas penyimpanan

Setelah meningkatkan kapasitas penyimpanan sistem file, Anda dapat memantau kemajuan peningkatan kapasitas penyimpanan menggunakan FSx konsol Amazon, API, atau AWS CLI seperti yang dijelaskan dalam prosedur berikut.

Memantau peningkatan dalam konsol

Di tab Pembaruan di jendela Detail sistem file, Anda dapat melihat 10 pembaruan terbaru untuk setiap jenis pembaruan.

Untuk pembaruan kapasitas penyimpanan, Anda dapat melihat informasi berikut.

Jenis pembaruan

Nilai yang mungkin adalah Kapasitas penyimpanan.

Nilai target

Nilai yang diinginkan untuk memperbarui kapasitas penyimpanan sistem file ke.

Status

Status terkini dari pembaruan. Untuk pembaruan kapasitas penyimpanan, nilai yang mungkin adalah sebagai berikut:

- Tertunda - Amazon FSx telah menerima permintaan pembaruan, tetapi belum mulai memprosesnya.
- Sedang berlangsung - Amazon FSx sedang memproses permintaan pembaruan.
- Pengoptimalan yang diperbarui - Amazon FSx telah meningkatkan kapasitas penyimpanan sistem file. Proses optimasi penyimpanan sekarang sedang memindahkan data sistem file ke disk baru yang lebih besar.
- Selesai — Peningkatan kapasitas penyimpanan berhasil diselesaikan.
- Gagal — Peningkatan kapasitas penyimpanan gagal. Pilih tanda tanya (?) untuk melihat detail mengapa pembaruan penyimpanan gagal.

Kemajuan%

Menampilkan kemajuan proses optimasi penyimpanan sebagai persen selesai.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Memantau peningkatan dengan AWS CLI dan API

Anda dapat melihat dan memantau permintaan peningkatan kapasitas penyimpanan sistem file menggunakan describe-file-systems AWS CLI perintah dan tindakan DescribeFileSystemsAPI.

Array `AdministrativeActions` mendaftar 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif. Saat Anda meningkatkan kapasitas penyimpanan sistem file, dua `AdministrativeActions` dihasilkan: tindakan `FILE_SYSTEM_UPDATE` dan `STORAGE_OPTIMIZATION`.

Contoh berikut menunjukkan kutipan dari respons perintah CLI describe-file-systems . Sistem file memiliki kapasitas penyimpanan 300 GB, dan ada tindakan administratif yang tertunda untuk meningkatkan kapasitas penyimpanan hingga 1000 GB.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
                }
            ]
```

Amazon FSx memproses `FILE_SYSTEM_UPDATE` tindakan terlebih dahulu, menambahkan disk penyimpanan baru yang lebih besar ke sistem file. Ketika penyimpanan baru tersedia untuk sistem file, status `FILE_SYSTEM_UPDATE` berubah menjadi `UPDATED_OPTIMIZING`. Kapasitas penyimpanan menunjukkan nilai baru yang lebih besar, dan Amazon FSx mulai memproses tindakan `STORAGE_OPTIMIZATION` administratif. Ini ditunjukkan dalam kutipan tanggana perintah CLI describe-file-systems berikut.

Properti `ProgressPercent` menampilkan kemajuan proses optimasi penyimpanan. Setelah proses optimasi penyimpanan berhasil diselesaikan, status tindakan `FILE_SYSTEM_UPDATE` berubah menjadi `COMPLETED`, dan tindakan `STORAGE_OPTIMIZATION` tidak lagi muncul.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

Jika peningkatan kapasitas penyimpanan gagal, status tindakan `FILE_SYSTEM_UPDATE` berubah menjadi `FAILED`. Properti `FailureDetails` menyediakan informasi tentang kegagalan, yang ditunjukkan dalam contoh berikut.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
```

```
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 1000
                }
            ]
```

Untuk informasi tentang pemecahan masalah tindakan yang gagal, lihat Pembaruan kapasitas penyimpanan atau throughput gagal dilakukan.

Meningkatkan kapasitas penyimpanan sistem file FSx Windows File Server secara dinamis

Sebagai alternatif untuk meningkatkan kapasitas penyimpanan sistem file Windows File Server Anda FSx secara manual seiring dengan meningkatnya jumlah data yang disimpan, Anda dapat menggunakan AWS CloudFormation template untuk meningkatkan penyimpanan secara otomatis. Solusi yang disajikan di bagian ini secara dinamis meningkatkan kapasitas penyimpanan sistem file ketika jumlah kapasitas penyimpanan gratis turun di bawah ambang batas yang ditentukan yang Anda tentukan.

AWS CloudFormation Template ini secara otomatis menyebarkan semua komponen yang diperlukan untuk menentukan ambang kapasitas penyimpanan gratis, CloudWatch alarm Amazon berdasarkan ambang batas ini, dan AWS Lambda fungsi yang meningkatkan kapasitas penyimpanan sistem file.

Solusinya mengambil parameter berikut:

- ID sistem file
- Ambang batas kapasitas penyimpanan yang gratis (nilai numerik)
- Unit pengukuran (persentase [default] atau GiB)
- Persentase yang digunakan untuk meningkatkan kapasitas penyimpanan (%)
- Alamat email untuk berlangganan SNS
- Sesuaikan alarm untuk ambang batas (Ya/Tidak)

Topik

Gambaran umum arsitektur

Menerapkan solusi ini akan membangun sumber daya berikut di Cloud. AWS

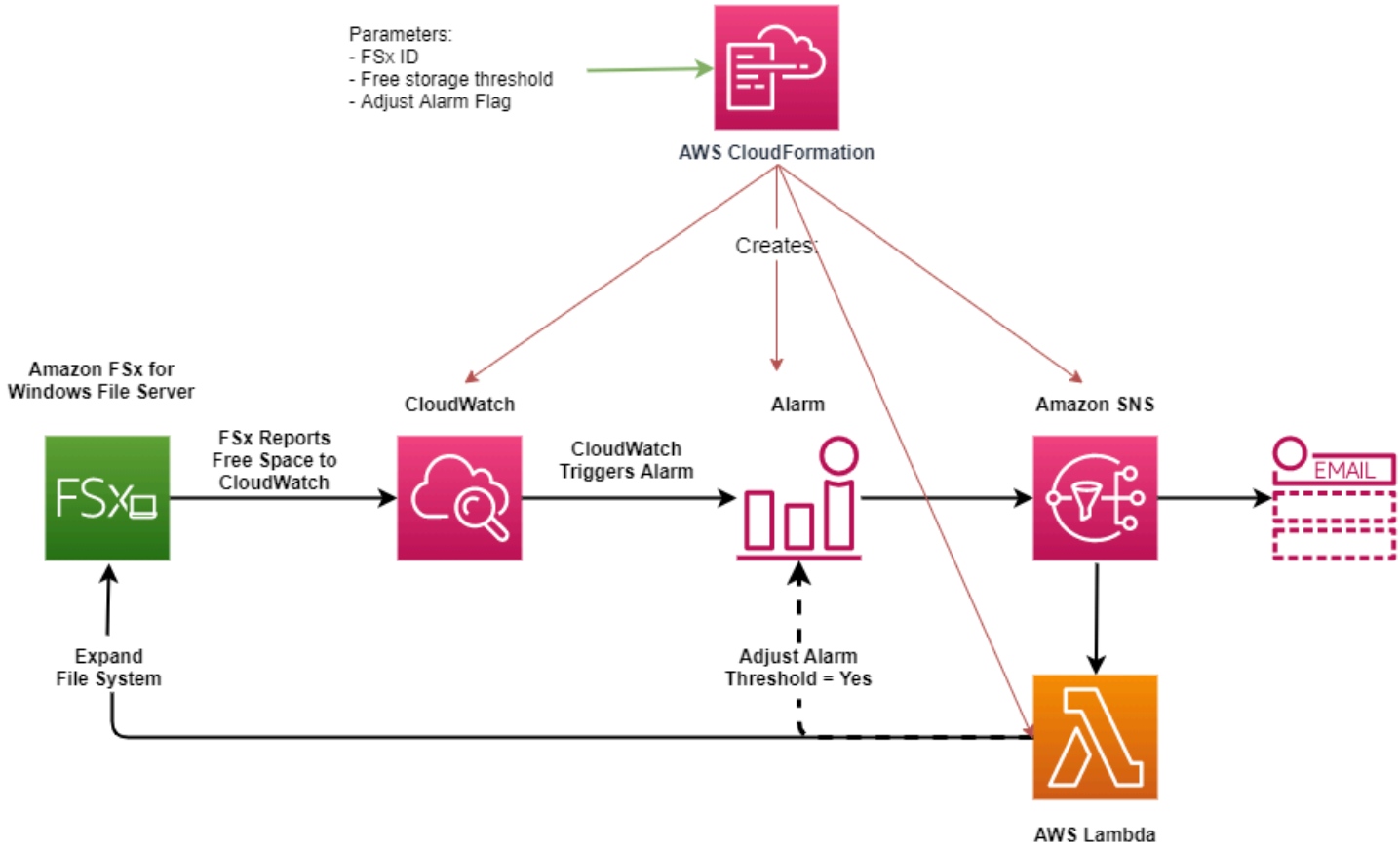


Diagram ini menggambarkan langkah-langkah berikut:

1. AWS CloudFormation Template menyebarkan CloudWatch alarm, AWS Lambda fungsi, antrean Amazon Simple Notification Service (Amazon SNS), dan semua peran yang diperlukan (IAM). AWS Identity and Access Management Peran IAM memberikan izin fungsi Lambda untuk menjalankan operasi FSx Amazon API.
2. CloudWatch memicu alarm ketika kapasitas penyimpanan gratis sistem file berada di bawah ambang batas yang ditentukan, dan mengirim pesan ke antrian Amazon SNS.
3. Solusi tersebut kemudian memicu fungsi Lambda yang terdaftar ke topik Amazon SNS ini.

4. Fungsi Lambda menghitung kapasitas penyimpanan sistem file yang baru berdasarkan nilai peningkatan persen yang ditentukan dan mengatur kapasitas penyimpanan sistem file yang baru.
5. Fungsi Lambda dapat secara opsional menyesuaikan ambang batas kapasitas penyimpanan gratis sehingga bisa menyamai persentase tertentu pada kapasitas penyimpanan baru milik sistem file.
6. Status CloudWatch alarm asli dan hasil operasi fungsi Lambda dikirim ke antrian Amazon SNS.

Untuk menerima pemberitahuan tentang tindakan yang dilakukan sebagai respons terhadap CloudWatch alarm, Anda harus mengonfirmasi langganan topik Amazon SNS dengan mengikuti tautan yang disediakan di email Konfirmasi Langganan.

AWS CloudFormation template

Solusi ini digunakan AWS CloudFormation untuk mengotomatiskan penyebaran komponen yang digunakan untuk secara otomatis meningkatkan kapasitas penyimpanan FSx untuk sistem file Windows File Server. Untuk menggunakan solusi ini, unduh AWS CloudFormation template Meningkatkan FSx Ukuran.

Template tersebut menggunakan Parameter yang dideskripsikan sebagai berikut. Tinjau parameter templat dan nilai-nilai default-nya, dan modifikasi templat-templat tersebut untuk kebutuhan sistem file Anda.

FileSystemId

Tidak ada nilai default. ID sistem file yang kapasitas penyimpanannya ingin Anda tingkatkan secara otomatis.

LowFreeDataStorageCapacityThreshold

Tidak ada nilai default. Tentukan ambang batas kapasitas penyimpanan bebas awal sebagai are yang memicu alarm berbunyi dan secara otomatis tingkatkan kapasitas penyimpanan sistem file, yang ditentukan dalam GiB atau sebagai persentase (%) dari kapasitas penyimpanan sistem file saat ini. Ketika dinyatakan sebagai persentase, CloudFormation template menghitung ulang ke GiB agar sesuai dengan pengaturan alarm. CloudWatch

LowFreeDataStorageCapacityThresholdUnit

Default adalah%. Tentukan unit-unit untuk `LowFreeDataStorageCapacityThreshold`, baik dalam GiB atau sebagai persentase dari kapasitas penyimpanan saat ini.

AlarmModificationNotification

Default-nya adalah Ya. Jika diatur ke Ya, `LowFreeDataStorageCapacityThreshold` semula, meningkat secara proporsional dengan nilai `PercentIncrease` untuk ambang batas alarm peringatan berikutnya.

Misalnya, ketika `PercentIncrease` diatur ke 20, dan AlarmModificationNotification disetel ke Ya, ambang batas ruang kosong yang tersedia (`LowFreeDataStorageCapacityThreshold`) yang ditentukan dalam GiB meningkat sebesar 20% untuk peristiwa peningkatan kapasitas penyimpanan berikutnya.

EmailAddress

Tidak ada nilai default. Menentukan alamat email yang akan digunakan untuk langganan SNS dan menerima peringatan ambang kapasitas penyimpanan.

PercentIncrease

Tidak ada nilai default. Tentukan jumlah yang digunakan untuk meningkatkan kapasitas penyimpanan, yang dinyatakan sebagai persentase dari kapasitas penyimpanan saat ini.

Deployment terotomasi dengan AWS CloudFormation

Prosedur berikut mengkonfigurasi dan menyebarkan AWS CloudFormation tumpukan untuk secara otomatis meningkatkan kapasitas penyimpanan FSx untuk sistem file Windows File Server. Dibutuhkan sekitar 5 menit untuk men-deploy.

> **Note**
>
> Menerapkan solusi ini menimbulkan penagihan untuk layanan terkait. AWS Untuk informasi lebih lanjut, lihat halaman detail harga untuk layanan tersebut.

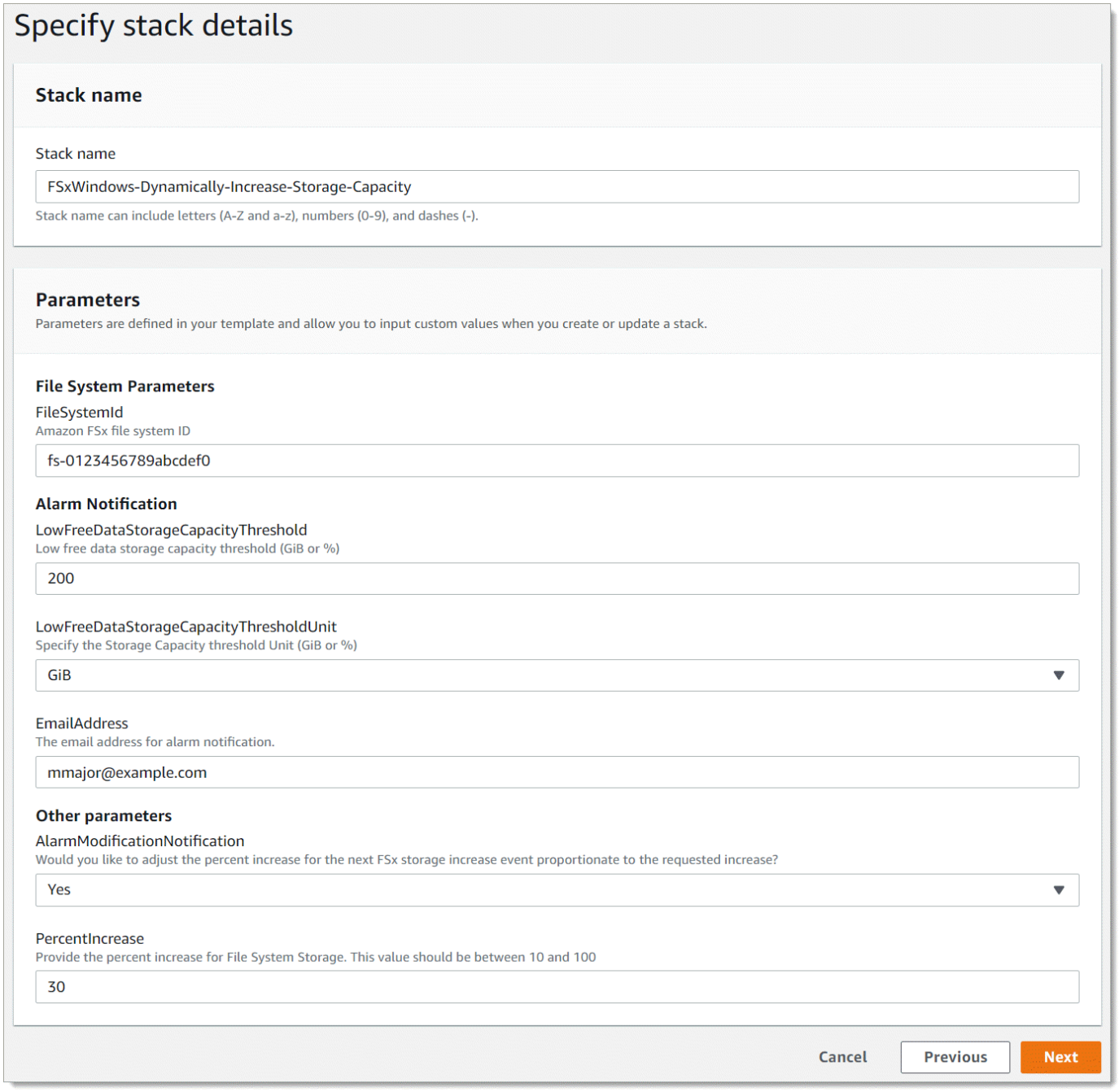
Sebelum memulai, Anda harus memiliki ID sistem FSx file Amazon yang berjalan di Amazon Virtual Private Cloud (Amazon VPC) di akun Anda AWS . Untuk informasi selengkapnya tentang membuat FSx sumber daya Amazon, lihatMemulai Amazon FSx untuk Windows File Server.

Untuk meluncurkan kapasitas penyimpanan otomatis yang meningkatkan tumpukan solusi

1. Unduh AWS CloudFormation template Tingkatkan FSx Ukuran. Untuk informasi selengkapnya tentang membuat CloudFormation tumpukan, lihat Membuat tumpukan di AWS CloudFormation konsol di Panduan AWS CloudFormation Pengguna.

   > **Note**
   >
   > Amazon saat FSx ini hanya tersedia di AWS Wilayah tertentu. Anda harus meluncurkan solusi ini di AWS Wilayah tempat Amazon FSx tersedia. Untuk informasi selengkapnya, lihat FSx titik akhir dan kuota Amazon di. Referensi Umum AWS

2. Dalam Spesifikasikan detail tumpukan, masukkan nilai untuk solusi peningkatan kapasitas penyimpanan otomatis Anda.



3. Masukkan Nama tumpukan.
4. Untuk Parameter, tinjau parameter untuk templat dan modifikasilah untuk kebutuhan sistem file Anda. Kemudian pilih Selanjutnya.
5. Masukkan pengaturan Opsi apa pun yang Anda inginkan untuk solusi kustom Anda, dan kemudian pilih Selanjutnya.
6. Untuk Meninjau, tinjau dan konfirmasikan pengaturan solusi. Pilih kotak centang untuk mengakui bahwa templat membuat sumber daya IAM.

7. Pilih Buat untuk men-deploy tumpukan.

Anda dapat melihat status tumpukan di AWS CloudFormation konsol di kolom Status. Anda akan melihat status CREATE_COMPLETE dalam waktu sekitar 5 menit.

Memperbarui tumpukan

Setelah tumpukan dibuat, Anda dapat memperbaruinya dengan menggunakan templat yang sama dan berikan nilai baru untuk parameternya. Untuk informasi selengkapnya, lihat Memperbarui tumpukan secara langsung di Panduan Pengguna AWS CloudFormation .

Memperbarui jenis penyimpanan sistem file FSx untuk Windows

Anda dapat mengubah jenis penyimpanan sistem file yang menggunakan penyimpanan HDD untuk menggunakan penyimpanan SSD. Anda dapat menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, atau Amazon untuk mengubah jenis penyimpanan sistem file, seperti yang ditunjukkan dalam prosedur berikut. Untuk informasi selengkapnya, lihat Mengelola jenis penyimpanan sistem file Anda.

Untuk memperbarui jenis penyimpanan sistem file (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Arahkan ke sistem File dan pilih sistem file Windows yang ingin Anda perbarui jenis penyimpanannya.
3. Di bawah Tindakan, pilih Perbarui jenis penyimpanan. Atau, di panel Ringkasan, pilih tombol Perbarui di sebelah HDD. Jendela Perbarui jenis penyimpanan muncul.
4. Untuk jenis penyimpanan yang diinginkan, pilih SSD. Pilih Perbarui untuk memulai pembaruan jenis penyimpanan.

   Anda dapat memantau kemajuan pembaruan jenis penyimpanan menggunakan konsol dan CLI.

Untuk memperbarui jenis penyimpanan sistem file (CLI)

Untuk memperbarui jenis penyimpanan FSx untuk sistem file Windows File Server untuk Windows, gunakan AWS CLI perintah update-file-system. Atur parameter berikut:

- `--file-system-id`ke ID sistem file yang ingin Anda perbarui.

- `--storage-type`ke SSD. Anda tidak dapat beralih dari jenis penyimpanan SSD ke jenis penyimpanan HDD.

Anda dapat memantau kemajuan pembaruan dengan menggunakan AWS CLI perintah describe-file-systems. Cari `administrative-actions` di output.

Untuk informasi selengkapnya, lihat AdministrativeAction.

Memantau pembaruan jenis penyimpanan

Setelah memperbarui jenis penyimpanan sistem file dari HDD ke penyimpanan SSD, Anda dapat memantau kemajuan pembaruan jenis penyimpanan menggunakan FSx konsol Amazon, atau API AWS CLI, seperti yang dijelaskan dalam prosedur berikut.

Memantau pembaruan sistem file di konsol

Pada tab Pembaruan di jendela Rincian sistem file, Anda dapat melihat 10 pembaruan terbaru untuk setiap jenis pembaruan.

Untuk pembaruan jenis penyimpanan, Anda dapat melihat informasi berikut.

Jenis pembaruan

Nilai yang mungkin adalah tipe Penyimpanan.

Nilai target

SSD

Status

Status terkini dari pembaruan. Untuk pembaruan jenis penyimpanan, nilai yang mungkin adalah sebagai berikut:

- Tertunda - Amazon FSx menerima permintaan pembaruan, tetapi belum mulai memprosesnya.
- Sedang berlangsung - Amazon FSx sedang memproses permintaan pembaruan.
- Pengoptimalan yang diperbarui - Kinerja penyimpanan SSD tersedia untuk operasi penulisan. Pembaruan memasuki status pengoptimalan yang diperbarui, yang biasanya berlangsung beberapa jam, di mana operasi baca akan memiliki tingkat kinerja antara HDD dan SSD. Setelah tindakan pembaruan Anda selesai, kinerja SSD baru Anda tersedia untuk dibaca dan ditulis.

- Selesai — Pembaruan jenis penyimpanan berhasil diselesaikan.
- Gagal - Pembaruan jenis penyimpanan gagal. Pilih tanda tanya (?) untuk melihat detailnya.

Kemajuan%

Menampilkan kemajuan proses optimasi penyimpanan dengan persentase yang lengkap.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Memantau pembaruan dengan AWS CLI dan API

Anda dapat melihat dan memantau permintaan pembaruan jenis penyimpanan sistem file menggunakan describe-file-systems AWS CLI perintah dan tindakan DescribeFileSystemsAPI. Array `AdministrativeActions` mencantumkan 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif. Saat Anda meningkatkan IOPS SSD sistem file, dua `AdministrativeActions` dihasilkan: a `FILE_SYSTEM_UPDATE` dan `STORAGE_TYPE_OPTIMIZATION` tindakan.

Memperbarui IOPS SSD sistem file

Untuk sistem file yang dikonfigurasi dengan penyimpanan SSD, tingkat IOPS SSD yang disediakan menentukan jumlah disk I/O yang tersedia ketika sistem file Anda harus membaca data dari dan menulis data ke disk, sebagai lawan dari membaca atau menulis data yang ada dalam cache. Anda dapat memperbarui SSD IOPS untuk sistem file menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, atau Amazon, seperti yang dijelaskan dalam prosedur berikut. Untuk informasi selengkapnya tentang mengelola IOPS SSD, lihatMengelola SSD IOPS.

Untuk memperbarui SSD IOPS untuk sistem file (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Arahkan ke sistem File dan pilih sistem file Windows yang ingin Anda perbarui SSD IOPS.
3. Di bawah Tindakan, pilih Perbarui IOPS SSD. Atau, di panel Ringkasan, pilih tombol Perbarui di sebelah IOPS SSD yang disediakan. Jendela penyediaan Perbarui IOPS terbuka.
4. Untuk Mode, pilih Automatic atau User-provisioned. Jika Anda memilih Otomatis, Amazon FSx secara otomatis menyediakan 3 IOPS SSD per GiB kapasitas penyimpanan untuk sistem file Anda. Jika Anda memilih User-provisioned, masukkan seluruh nomor dalam kisaran 96-400.000.
5. Pilih Perbarui untuk memulai pembaruan IOPS SSD yang disediakan.

6. Anda dapat memantau kemajuan pembaruan pada halaman detail sistem File, pada tab Pembaruan.

Untuk memperbarui SSD IOPS untuk sistem file (CLI)

Untuk memperbarui SSD IOPS untuk sistem file Windows File Server, gunakan `--windows-configuration DiskIopsConfiguration` properti. FSx Properti ini memiliki dua parameter, `Iops` dan`Mode`:

- Jika Anda ingin menentukan jumlah IOPS SSD, gunakan`Iops=`*`number_of_IOPS`*, hingga maksimum 400.000 di AWS Wilayah yang didukung dan. `Mode=USER_PROVISIONED`
- Jika Anda FSx ingin Amazon meningkatkan IOPS SSD Anda secara otomatis, gunakan `Mode=AUTOMATIC` dan jangan gunakan `Iops` parameternya. Amazon FSx secara otomatis mempertahankan 3 SSD IOPS per GiB kapasitas penyimpanan pada sistem file Anda, hingga maksimum 400.000 di Wilayah yang didukung. AWS

Anda dapat memantau kemajuan pembaruan dengan menggunakan AWS CLI perintah describe-file-systems. Cari `administrative-actions` di output.

Untuk informasi selengkapnya, lihat AdministrativeAction.

Memantau pembaruan IOPS SSD yang disediakan

Setelah memperbarui jumlah IOPS SSD yang disediakan untuk sistem file Anda, Anda dapat memantau kemajuan pembaruan IOPS SSD menggunakan FSx konsol Amazon, API, dan API AWS CLI, seperti yang dijelaskan dalam prosedur berikut.

Memantau pembaruan di konsol

Di tab Pembaruan dalam jendela Detail sistem file, Anda dapat melihat 10 pembaruan terbaru untuk setiap jenis pembaruan.

Untuk pembaruan IOPS SSD yang disediakan, Anda dapat melihat informasi berikut.

Jenis pembaruan

Nilai yang mungkin adalah Mode IOPS dan SSD IOPS.

Nilai target

Nilai yang diinginkan untuk memperbarui mode IOPS sistem file dan SSD IOPS ke.

Status

Status terkini dari pembaruan. Untuk pembaruan SSD IOPS, nilai yang mungkin adalah sebagai berikut:

- Tertunda - Amazon FSx telah menerima permintaan pembaruan, tetapi belum mulai memprosesnya.
- Sedang berlangsung - Amazon FSx sedang memproses permintaan pembaruan.
- Pengoptimalan yang diperbarui - Level IOPS baru tersedia untuk operasi penulisan beban kerja Anda. Pembaruan Anda memasuki status pengoptimalan yang diperbarui, yang biasanya berlangsung beberapa jam, selama operasi baca beban kerja Anda memiliki kinerja IOPS antara level sebelumnya dan level baru. Setelah tindakan pembaruan Anda selesai, level IOPS baru Anda tersedia untuk dibaca dan ditulis.
- Selesai - Pembaruan SSD IOPS berhasil diselesaikan.
- Gagal - Pembaruan SSD IOPS gagal. Pilih tanda tanya (?) untuk melihat detail mengapa pembaruan penyimpanan gagal.

Kemajuan%

Menampilkan kemajuan proses optimasi penyimpanan sebagai persen selesai.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Memantau pembaruan dengan AWS CLI dan API

Anda dapat melihat dan memantau permintaan pembaruan SSD IOPS sistem file menggunakan describe-file-systems AWS CLI perintah dan tindakan DescribeFileSystemsAPI. Array `AdministrativeActions` mencantumkan 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif. Saat Anda meningkatkan IOPS SSD sistem file, dua `AdministrativeActions` dihasilkan: a `FILE_SYSTEM_UPDATE` dan `IOPS_OPTIMIZATION` tindakan.

Mengelola deduplikasi data

Anda dapat mengelola pengaturan deduplikasi data sistem file Anda menggunakan Amazon FSx CLI untuk manajemen jarak jauh. PowerShell Untuk informasi selengkapnya tentang penggunaan

manajemen jarak jauh Amazon FSx CLI PowerShell, lihat. Menggunakan Amazon FSx CLI untuk PowerShell

Berikut ini adalah perintah yang dapat Anda gunakan untuk deduplikasi data.

Perintah deduplikasi data	Deskripsi
Enable-FSxDedup	Memungkinkan deduplikasi data pada pembagian file. Kompresi data setelah deduplikasi diaktifkan secara default saat Anda mengaktifkan deduplikasi data.
Disable-FSxDedup	Menonaktifkan deduplikasi data pada pembagian file.
Get-FSxDedupConfiguration	Mengambil informasi konfigurasi deduplikasi, termasuk ukuran dan usia file Minimum untuk optimasi, pengaturan kompresi, dan jenis file dan folder yang dikecualikan.
Set-FSxDedupConfiguration	Mengganti pengaturan konfigurasi deduplikasi, termasuk ukuran dan usia file minimum untuk optimasi, pengaturan kompresi, dan jenis file dan folder yang dikecualikan.
Get-FSxDedupStatus	Ambil status deduplikasi, dan sertakan properti hanya-baca yang menggambarkan penghematan dan status pengoptimalan pada sistem file, waktu, dan status penyelesaian untuk pekerjaan dedup terakhir pada sistem file.
Get-FSxDedupMetadata	Mengambil metadata optimasi deduplikasi.
Update-FSxDedupStatus	Menghitung dan mengambil informasi penghematan deduplikasi data yang diperbarui.
Measure-FSxDedupFileMetadata	Mengukur dan mengambil ruang penyimpanan potensial yang Anda dapat ambil kembali pada sistem file Anda jika Anda menghapus sekelompok folder. File sering memiliki potongan yang dibagikan di folder lain, dan mesin deduplikasi menghitung potongan yang unik dan akan dihapus.
Get-FSxDedupSchedule	Mengambil jadwal deduplikasi yang saat ini dijabarkan.

Perintah deduplikasi data	Deskripsi
New-FSxDedupSchedule	Buat dan sesuaikan jadwal deduplikasi data.
Set-FSxDedupSchedule	Ubah pengaturan konfigurasi untuk jadwal deduplikasi data yang ada.
Remove-FSxDedupSchedule	Hapus jadwal deduplikasi.
Get-FSxDedupJob	Dapatkan status dan informasi untuk semua pekerjaan deduplikasi yang sedang berjalan atau antrian.
Stop-FSxDedupJob	Membatalkan satu atau beberapa pekerjaan deduplikasi data yang ditetapkan.

Bantuan online untuk setiap perintah memberikan referensi dari semua opsi perintah. Untuk mengakses bantuan ini, jalankan perintah dengan -?, misalnya Enable-FSxDedup -?.

Mengaktifkan deduplikasi data

Anda mengaktifkan deduplikasi data pada Amazon FSx untuk Windows File Server berbagi file menggunakan `Enable-FSxDedup` perintah, sebagai berikut.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

Saat Anda mengaktifkan deduplikasi data, jadwal dan konfigurasi default dibuat. Anda dapat membuat, memodifikasi, dan menghapus jadwal dan konfigurasi menggunakan perintah di bawah ini.

Anda dapat menggunakan `Disable-FSxDedup` perintah untuk menonaktifkan deduplikasi data sepenuhnya pada sistem file Anda.

Membuat jadwal deduplikasi data

Meskipun jadwal default berfungsi dengan baik dalam banyak kasus, Anda dapat membuat jadwal deduplikasi baru dengan menggunakan `New-FsxDedupSchedule` perintah, ditampilkan sebagai berikut. Jadwal deduplikasi data menggunakan waktu UTC.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
```

```
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
}
```

Perintah ini membuat jadwal yang dinamai `CustomOptimization` yang berjalan pada hari Senin, Rabu, dan Sabtu, memulai pekerjaan pada pukul 8:00 pagi (UTC) setiap hari, dengan durasi maksimal 7 jam, setelah itu pekerjaan berhenti jika masih berjalan.

Perhatikan bahwa membuat jadwal pekerjaan deduplikasi kustom baru tidak akan menimpa atau menghapus jadwal default yang ada. Sebelum membuat pekerjaan deduplikasi khusus, Anda mungkin ingin menonaktifkan pekerjaan default jika Anda tidak membutuhkannya.

Anda dapat menonaktifkan jadwal deduplikasi default dengan menggunakan `Set-FsxDedupSchedule` perintah, ditampilkan sebagai berikut.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

Anda dapat menghapus jadwal deduplikasi dengan menggunakan perintah. `Remove-FSxDedupSchedule -Name "ScheduleName"` Perhatikan bahwa jadwal `BackgroundOptimization` deduplikasi default tidak dapat diubah atau dihapus dan harus dinonaktifkan sebagai gantinya.

Mengubah jadwal deduplikasi data

Anda dapat mengubah jadwal deduplikasi yang ada dengan menggunakan perintah `Set-FsxDedupSchedule`, sebagai berikut.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

Perintah ini mengubah jadwal `CustomOptimization` yang ada untuk berjalan pada hari Senin sampai Rabu dan Sabtu, memulai pekerjaan pada pukul 9:00 pagi (UTC) setiap hari, dengan durasi maksimal 9 jam, setelah itu pekerjaan berhenti jika masih berjalan.

Untuk mengubah usia file minimum sebelum mengoptimalkan pengaturan, gunakan perintah `Set-FSxDedupConfiguration`.

Menampilkan jumlah ruang yang dihemat

Untuk melihat jumlah ruang disk yang Anda hemat sehingga tidak menjalankan data deduplikasi, gunakan perintah `Get-FSxDedupStatus`, sebagai berikut.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

> **Note**
>
> Nilai yang ditunjukkan dalam respons perintah untuk parameter berikut tidak dapat diandalkan, dan Anda tidak boleh menggunakan nilai-nilai ini: Kapasitas, FreeSpace, UsedSpace, UnoptimizedSize, dan SavingsRate.

Menyelesaikan masalah deduplikasi data

Gunakan informasi berikut untuk membantu memecahkan masalah umum saat mengonfigurasi dan menggunakan deduplikasi data.

Topik

Deduplikasi data tidak berfungsi

Untuk melihat status deduplikasi data saat ini, jalankan `Get-FSxDedupStatus` PowerShell perintah untuk melihat status penyelesaian untuk pekerjaan deduplikasi terbaru. Jika satu atau lebih pekerjaan gagal, Anda mungkin tidak melihat peningkatan kapasitas penyimpanan gratis pada sistem file Anda.

Alasan paling umum untuk pekerjaan deduplikasi gagal adalah memori yang tidak mencukupi.

- Microsoft merekomendasikan secara optimal memiliki 1 GB memori per 1 TB data logis (atau minimal 350 MB per 1 TB data logis). Gunakan tabel FSx kinerja Amazon untuk menentukan memori yang terkait dengan kapasitas throughput sistem file Anda dan memastikan sumber daya memori cukup untuk ukuran data Anda. Jika tidak, Anda perlu meningkatkan kapasitas throughput sistem file ke tingkat yang memenuhi persyaratan memori 1 GB per 1 TB data logis.
- Pekerjaan deduplikasi dikonfigurasi dengan default Windows yang direkomendasikan dari alokasi memori 25%, yang berarti bahwa untuk sistem file dengan memori 32 GB, 8 GB akan tersedia untuk deduplikasi. Alokasi memori dapat dikonfigurasi (menggunakan `Set-FSxDedupSchedule` perintah dengan parameter`-Memory`). Ketahuilah bahwa menggunakan alokasi memori yang lebih tinggi untuk dedup dapat memengaruhi kinerja sistem file.
- Anda dapat memodifikasi konfigurasi pekerjaan deduplikasi untuk mengurangi jumlah memori yang diperlukan. Misalnya, Anda dapat membatasi pengoptimalan agar berjalan pada jenis file atau folder tertentu, atau menetapkan ukuran dan usia file minimum untuk pengoptimalan. Kami juga merekomendasikan mengonfigurasi pekerjaan deduplikasi untuk dijalankan selama periode idle ketika ada beban minimal pada sistem file Anda.

Anda juga dapat melihat kesalahan jika pekerjaan deduplikasi tidak memiliki waktu yang cukup untuk diselesaikan. Anda mungkin perlu mengubah durasi maksimum pekerjaan, seperti yang dijelaskan dalamMengubah jadwal deduplikasi data.

Jika pekerjaan deduplikasi telah gagal untuk jangka waktu yang lama, dan telah ada perubahan pada data pada sistem file selama periode ini, pekerjaan deduplikasi berikutnya mungkin memerlukan lebih banyak sumber daya untuk menyelesaikan dengan sukses untuk pertama kalinya.

Nilai deduplikasi secara tak terduga disetel ke 0

Nilai untuk `SavedSpace` dan `OptimizedFilesSavingsRate` tiba-tiba 0 untuk sistem file di mana Anda telah mengkonfigurasi deduplikasi data.

Hal ini dapat terjadi selama proses optimasi penyimpanan ketika Anda meningkatkan kapasitas penyimpanan sistem file. Saat Anda meningkatkan kapasitas penyimpanan sistem file, Amazon FSx membatalkan pekerjaan deduplikasi data yang ada selama proses pengoptimalan penyimpanan, yang memigrasikan data dari disk lama ke disk baru yang lebih besar. Amazon FSx melanjutkan deduplikasi data pada sistem file setelah pekerjaan pengoptimalan penyimpanan selesai. Untuk informasi selengkapnya tentang peningkatan kapasitas penyimpanan dan optimasi penyimpanan, lihat Mengelola kapasitas penyimpanan.

Ruang tidak dibebaskan pada sistem file setelah menghapus file

Perilaku deduplikasi data yang diharapkan adalah jika data yang dihapus adalah sesuatu yang dedup telah menghemat ruang, maka ruang tersebut tidak benar-benar dibebaskan pada sistem file Anda sampai pekerjaan pengumpulan sampah berjalan.

Praktek yang mungkin membantu Anda adalah mengatur jadwal untuk menjalankan pekerjaan pengumpulan sampah tepat setelah Anda menghapus sejumlah besar file. Setelah pekerjaan pengumpulan sampah selesai, Anda dapat mengatur jadwal pengumpulan sampah kembali ke pengaturan semula. Hal ini memastikan Anda dapat dengan cepat melihat ruang dari penghapusan Anda.

Gunakan prosedur berikut untuk mengatur pekerjaan pengumpulan sampah untuk berjalan dalam 5 menit.

1. Untuk memastikan bahwa deduplikasi data diaktifkan, gunakan perintah `Get-FSxDedupStatus`. Untuk informasi lebih lanjut tentang perintah dan output yang diharapkan, lihat Menampilkan jumlah ruang yang dihemat.
2. Gunakan yang berikut ini untuk mengatur jadwal untuk menjalankan pekerjaan pengumpulan sampah 5 menit dari sekarang.

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. Setelah pekerjaan pengumpulan sampah telah berjalan dan ruang telah dibebaskan, atur jadwal kembali ke pengaturan aslinya.

Menggunakan Ruang Nama DFS

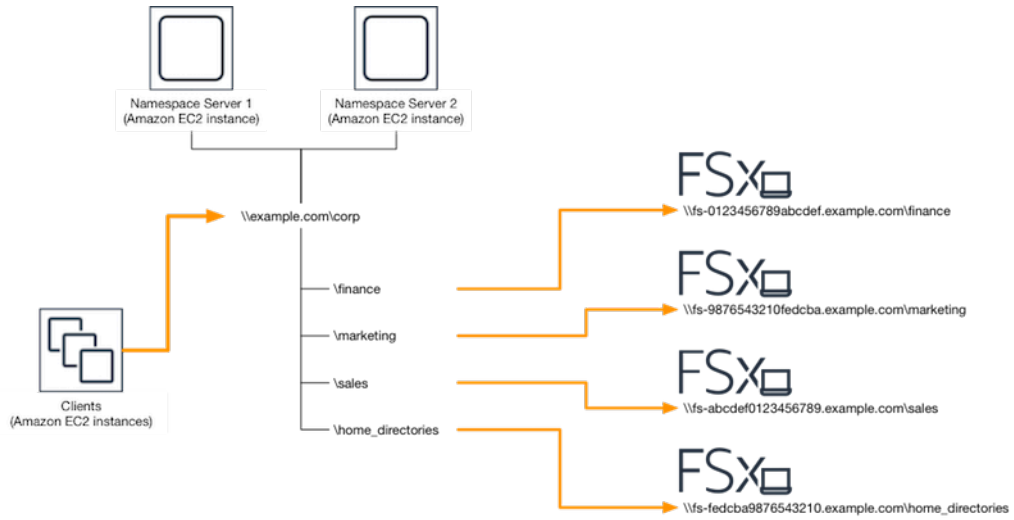
DFS Namespaces adalah layanan peran Windows Server yang Anda gunakan untuk mengelompokkan folder bersama yang terletak di server yang berbeda ke dalam satu atau lebih ruang nama yang terstruktur secara logis. Ini memungkinkan untuk memberi pengguna tampilan

virtual folder bersama, di mana satu jalur mengarah ke file yang terletak di beberapa sistem file, seperti yang ditunjukkan pada diagram berikut. Selain mengatur dan menyatukan akses ke berbagi file Anda di beberapa sistem file,

Kelompokkan beberapa FSx untuk sistem file Windows File Server dengan Ruang Nama DFS

Anda dapat menggunakan Ruang Nama Sistem File Terdistribusi (DFS) Microsoft untuk mengelompokkan berbagi file pada beberapa FSx untuk sistem file Windows File Server ke dalam satu struktur folder umum, atau namespace. Dengan menggunakan DFS Namespaces, Anda dapat menskalakan penyimpanan file di luar kapasitas penyimpanan maksimum sistem file tunggal (64 TiB) untuk kumpulan data file besar — hingga ratusan petabyte. Bagian ini menunjukkan cara mengatur ruang nama DFS pada beberapa FSx untuk sistem file Windows File Server.

DFS Namespaces adalah layanan peran Windows Server yang Anda gunakan untuk mengelompokkan folder bersama yang terletak di server yang berbeda ke dalam satu atau lebih ruang nama yang terstruktur secara logis. Ini memungkinkan untuk memberi pengguna tampilan virtual folder bersama, di mana satu jalur mengarah ke file yang terletak di beberapa sistem file, seperti yang ditunjukkan pada diagram berikut. Selain mengatur dan menyatukan akses ke berbagi file Anda di beberapa sistem file,



Untuk step-by-step prosedur pengelompokan FSx untuk sistem file Windows menggunakan DFS Namespaces, lihat. Kelompokkan beberapa sistem file di bawah satu namespace

Meningkatkan kinerja dengan pecahan

Amazon FSx untuk Windows File Server mendukung penggunaan Microsoft Distributed File System (DFS). Dengan menggunakan Ruang Nama DFS, Anda dapat meningkatkan kinerja (baik baca maupun tulis) untuk melayani beban kerja intensif I/O dengan menyebarkan data file Anda di beberapa sistem file Amazon. FSx Pada saat yang sama, Anda masih dapat menyajikan tampilan terpadu di bawah namespace umum untuk aplikasi Anda. Solusi ini melibatkan membagi data file Anda ke dataset yang lebih kecil atau serpihan dan menyimpannya di seluruh sistem file yang berbeda. Aplikasi yang mengakses data Anda dari beberapa instans dapat mencapai tingkat performa yang tinggi dengan membaca dan menulis ke serpihan ini secara paralel.

Anda dapat menggunakan solusi yang disediakan Sharding data menggunakan DFS Namespaces untuk performa scale-out untuk mendistribusikan akses baca/tulis ke data Anda secara seragam di beberapa data Anda FSx untuk sistem file Windows File Server.

Kelompokkan beberapa sistem file di bawah satu namespace

Dalam prosedur ini, Anda akan membuat namespace berbasis domain tunggal (`example.com\corp`) pada dua server namespace, untuk mengkonsolidasikan berbagi file yang disimpan di beberapa FSx untuk sistem file Windows (keuangan, pemasaran, penjualan, home_directories). Anda juga akan mengatur empat berbagi file di bawah namespace, masing-masing secara transparan mengarahkan pengguna untuk berbagi yang dihosting secara terpisah FSx untuk sistem file Windows. Ini memungkinkan pengguna Anda untuk mengakses berbagi file menggunakan namespace umum alih-alih harus menentukan nama DNS untuk masing-masing sistem file yang menghosting berbagi file.

> **Note**
>
> Amazon FSx tidak dapat ditambahkan ke root jalur berbagi DFS.

Untuk mengelompokkan beberapa sistem file ke dalam namespace DFS umum

1. Jika Anda belum menjalankan server Namespace DFS, Anda dapat meluncurkan sepasang server Namespace DFS yang sangat tersedia menggunakan template Setup-DFSN-Servers.Template. AWS CloudFormation Untuk informasi selengkapnya tentang membuat AWS CloudFormation tumpukan, lihat Membuat Tumpukan di AWS CloudFormation Konsol di Panduan AWS CloudFormation Pengguna.

2. Connect ke salah satu server Namespace DFS yang diluncurkan di langkah sebelumnya sebagai pengguna di grup Administrator yang didelegasikan AWS . Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
3. Akses konsol manajemen DFS dengan membuka. Buka menu Start dan jalankan fsmgmt.msc menggunakan. Ini membuka alat GUI Pengelolaan DFS.
4. Pilih Tindakan lalu Namespace Baru, ketik nama komputer server Namespace DFS pertama yang Anda luncurkan untuk Server dan pilih Selanjutnya.
5. Untuk Nama, ketik namespace yang Anda buat (misalnya, corp).
6. Pilih Edit pengaturan dan atur izin yang sesuai berdasarkan kebutuhan Anda. Pilih Selanjutnya.
7. Biarkan default opsi Namespace berbasis domain yang dipilih, biarkan opsi Mengaktifkan mode Windows Server 2008 yang dipilih, dan pilih Selanjutnya.

   > **Note**
   >
   > Mode Windows Server 2008 adalah opsi terbaru yang tersedia untuk Namespace.

8. Tinjau pengaturan namespace dan pilih Buat.
9. Dengan namespace yang baru dibuat yang dipilih di bawah Namespace di bilah navigasi, pilih Tindakan lalu Tambah Server Namespace.
10. Ketik nama komputer server Namespace DFS pertama yang Anda luncurkan untuk server Namespace.
11. Pilih Edit pengaturan, atur izin yang sesuai berdasarkan kebutuhan Anda, dan pilih OK.
12. Buka menu konteks (klik kanan) untuk namespace yang baru saja Anda buat, pilih Folder Baru, ketik nama folder (misalnya, `finance` untuk Nama, dan pilih OKE.
13. Ketik nama DNS berbagi file yang Anda ingin folder DFS Namespace menunjuk ke dalam format UNC (misalnya, `\\fs-0123456789abcdef0.example.com\finance`) untuk Jalur ke target folder dan pilih OK.
14. Jika pembagian file tidak ada:

    a. Pilih Ya untuk membuatnya.

    b. Dari dialog Buat Bagikan, pilih Browse.

    c. Pilih folder yang ada, atau buat folder baru di bawah D$, dan pilih OK.

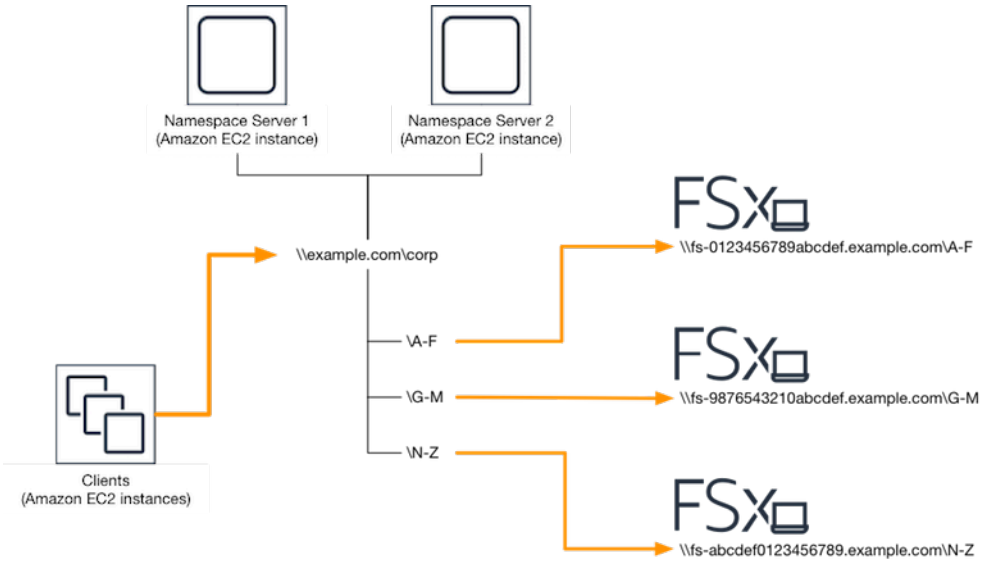
    d. Atur izin berbagi yang sesuai, dan pilih OK.

15. Dari dialog Folder baru, pilih OK. Folder baru akan dibuat di bawah namespace.

16. Ulangi empat langkah terakhir untuk folder lain yang ingin Anda bagikan di bawah namespace yang sama.

Sharding data menggunakan DFS Namespaces untuk performa scale-out

Prosedur berikut memandu Anda melalui pembuatan solusi DFS di Amazon FSx untuk kinerja scale-out. Dalam contoh ini, data yang disimpan di *corp* namespace dibagi menurut abjad. File data 'A-F', 'G-M' dan 'N-Z' semua disimpan pada berbagi file yang berbeda. Berdasarkan jenis data, ukuran I/O, dan pola akses I/O, Anda harus memutuskan cara terbaik membagi menjadi serpihan data Anda di beberapa berbagi file. Pilih konvensi serpihan yang mendistribusikan I/O secara merata di semua berbagi file yang Anda rencanakan untuk digunakan. Perlu diingat bahwa setiap namespace mensupport hingga 50.000 berbagi file dan ratusan petabyte kapasitas penyimpanan secara agregat.



Untuk mengatur Namespace DFS untuk performa menskalakan keluar

1. Jika Anda belum menjalankan server Namespace DFS, Anda dapat meluncurkan sepasang server Namespace DFS yang sangat tersedia menggunakan template Setup-DFSN-Servers.Template. AWS CloudFormation Untuk informasi selengkapnya tentang membuat AWS CloudFormation tumpukan, lihat Membuat Tumpukan di AWS CloudFormation Konsol di Panduan AWS CloudFormation Pengguna.
2. Connect ke salah satu server Namespace DFS yang diluncurkan di langkah sebelumnya sebagai pengguna di grup Administrator yang didelegasikan AWS . Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.

3. Mengakses konsol manajemen DFS. Buka menu Meluncurkan dan jalankan dfsmgmt.msc. Ini membuka alat GUI Pengelolaan DFS.
4. Pilih Tindakan lalu Namespace Baru, ketik nama komputer server Namespace DFS pertama yang Anda luncurkan untuk Server dan pilih Selanjutnya.
5. Untuk Nama, ketik namespace yang Anda buat (misalnya, corp).
6. Pilih Edit pengaturan dan atur izin yang sesuai berdasarkan kebutuhan Anda. Pilih Selanjutnya.
7. Biarkan default opsi Namespace berbasis domain yang dipilih, biarkan opsi Mengaktifkan mode Windows Server 2008 yang dipilih, dan pilih Selanjutnya.

   > **Note**
   >
   > Mode Windows Server 2008 adalah opsi terbaru yang tersedia untuk Namespace.

8. Tinjau pengaturan namespace dan pilih Buat.
9. Dengan namespace yang baru dibuat yang dipilih di bawah Namespace di bilah navigasi, pilih Tindakan lalu Tambah Server Namespace.
10. Ketik nama komputer server Namespace DFS pertama yang Anda luncurkan untuk server Namespace.
11. Pilih Edit pengaturan, atur izin yang sesuai berdasarkan kebutuhan Anda, dan pilih OK.
12. Buka menu konteks (klik kanan) untuk namespace yang baru saja Anda buat, pilih Folder Baru, masukkan nama folder untuk serpihan pertama (misalnya, `A-F` untuk Nama), dan pilih Tambah.
13. Ketik nama DNS berbagi file hosting serpihan ini dalam format UNC (misalnya, `\\fs-0123456789abcdef0.example.com\A-F`) untuk Path ke target folder dan pilih OK.
14. Jika pembagian file tidak ada:
    a. Pilih Ya untuk membuatnya.
    b. Dari dialog Buat Bagikan, pilih Browse.
    c. Pilih folder yang ada, atau buat folder baru di bawah D$, dan pilih OK.
    d. Atur izin berbagi yang sesuai, dan pilih OK.
15. Dengan target folder sekarang ditambahkan untuk serpihan, pilih OK.
16. Ulangi empat langkah terakhir untuk serpihan lain yang ingin Anda tambahkan ke namespace yang sama.

Mengelola kapasitas throughput

Anda dapat meningkatkan dan mengurangi kapasitas throughput sistem file Anda untuk membantu mengelola kinerjanya kapan saja. Kapasitas throughput adalah salah satu dimensi yang menentukan kecepatan di mana server file hosting Anda FSx untuk sistem file Windows File Server dapat melayani data. Tingkat kapasitas throughput yang lebih tinggi juga datang dengan tingkat operasi I/O per detik (IOPS) yang lebih tinggi dan jumlah memori cache yang lebih besar di server file. Untuk informasi selengkapnya, lihat FSx untuk kinerja Windows File Server.

Topik

Cara kerja penskalaan throughput

Saat Anda memodifikasi kapasitas throughput sistem file Anda, Amazon FSx mengalihkan server file sistem file ke server dengan throughput lebih atau lebih sedikit di belakang layar. Untuk sistem file multi-AZ, beralih ke server file baru memicu failover dan failback otomatis sementara FSx Amazon mengganti server file pilihan dan sekunder. Sistem file single-AZ tidak akan tersedia selama beberapa menit sementara server file diaktifkan selama penskalaan kapasitas throughput. Anda ditagih untuk jumlah kapasitas throughput baru setelah tersedia untuk sistem file Anda.

> **Note**
>
> Selama operasi pemeliharaan di bagian belakang, modifikasi sistem (termasuk modifikasi kapasitas throughput) mungkin tertunda. Operasi pemeliharaan dapat menyebabkan modifikasi sistem mengantri untuk diproses.

Untuk sistem file multi-AZ, penskalaan kapasitas throughput menghasilkan failover dan failback otomatis sementara Amazon FSx mengganti server file pilihan dan sekunder. Selama penggantian server file, yang terjadi selama penskalaan kapasitas throughput serta pemeliharaan sistem file dan gangguan layanan yang tidak direncanakan, lalu lintas yang sedang berlangsung ke sistem file akan dilayani oleh server file yang tersisa. Ketika server file yang diganti kembali online, FSx

untuk Windows akan menjalankan pekerjaan sinkronisasi ulang untuk memastikan bahwa data disinkronkan kembali ke server file yang baru diganti.

FSx untuk Windows dirancang untuk meminimalkan dampak aktivitas sinkronisasi ulang ini pada aplikasi dan pengguna. Namun, proses sinkronisasi ulang melibatkan sinkronisasi data dalam blok besar. Ini berarti bahwa blok data yang besar dapat memerlukan sinkronisasi meskipun hanya sebagian kecil yang diperbarui. Akibatnya, jumlah sinkronisasi ulang tidak hanya bergantung pada jumlah churn data, tetapi juga sifat churn data pada sistem file. Jika beban kerja Anda berat dan berat IOPS, proses sinkronisasi data mungkin memakan waktu lebih lama dan memerlukan sumber daya kinerja tambahan.

Sistem file Anda akan terus tersedia selama waktu ini, tetapi untuk mengurangi durasi sinkronisasi data, kami sarankan untuk memodifikasi kapasitas throughput selama periode idle ketika ada beban minimal pada sistem file Anda. Kami juga menyarankan untuk memastikan bahwa sistem file Anda memiliki kapasitas throughput yang cukup untuk menjalankan pekerjaan sinkronisasi selain beban kerja Anda, untuk mengurangi durasi sinkronisasi data. Terakhir, kami sarankan untuk menguji dampak failover sementara sistem file Anda memiliki beban yang lebih ringan.

Mengetahui kapan harus memodifikasi kapasitas throughput

Amazon FSx terintegrasi dengan Amazon CloudWatch, memungkinkan Anda memantau tingkat penggunaan throughput sistem file yang sedang berlangsung. Kinerja (throughput dan IOPS) yang dapat Anda drive melalui sistem file Anda tergantung pada karakteristik beban kerja spesifik Anda, bersama dengan kapasitas throughput sistem file Anda, kapasitas penyimpanan, dan jenis penyimpanan. Anda dapat menggunakan CloudWatch metrik untuk menentukan dimensi mana yang akan diubah untuk meningkatkan kinerja. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

FSx untuk Windows File Server menyediakan peringatan kinerja berdasarkan nilai CloudWatch metrik untuk sistem file Anda di dasbor Pemantauan & kinerja di halaman detail sistem File di konsol Amazon FSx . Ini termasuk kapasitas throughput, dan metrik sistem file lainnya yang dapat memanfaatkan peningkatan kapasitas throughput. Untuk informasi selengkapnya, lihat Peringatan dan rekomendasi kinerja.

Konfigurasikan sistem file Anda dengan kapasitas throughput yang cukup untuk memenuhi tidak hanya lalu lintas yang diharapkan dari beban kerja Anda, tetapi juga sumber daya kinerja tambahan yang diperlukan untuk mendukung fitur yang Anda aktifkan pada sistem file Anda. Misalnya, jika Anda menjalankan deduplikasi data, kapasitas throughput yang Anda pilih harus menyediakan memori

yang cukup untuk menjalankan deduplikasi berdasarkan penyimpanan yang Anda miliki. Jika Anda menggunakan salinan bayangan, tingkatkan kapasitas throughput ke nilai yang setidaknya tiga kali lipat dari nilai yang diharapkan didorong oleh beban kerja Anda untuk menghindari Windows Server menghapus salinan bayangan Anda. Untuk informasi selengkapnya, lihat Dampak kapasitas throughput terhadap performa.

Memodifikasi kapasitas throughput

Anda dapat menambah atau mengurangi kapasitas throughput sistem file menggunakan FSx konsol Amazon, AWS Command Line Interface (AWS CLI), atau Amazon FSx API, seperti yang dijelaskan dalam prosedur berikut.

Untuk mengubah kapasitas throughput sistem file (CLI)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Arahkan ke Sistem file, dan pilih sistem file Windows yang ingin Anda tingkatkan kapasitas throughput-nya.
3. Untuk Tindakan, pilih Perbarui throughput.

   Atau, pada panel Ringkasan, pilih Perbarui di samping Kapasitas throughput pada sistem file.

   Jendela Perbarui kapasitas throughput akan muncul.
4. Pilih nilai baru untuk Kapasitas throughput dari daftar.
5. Pilih Perbarui untuk memulai pembaruan kapasitas throughput.

   > **Note**
   >
   > Sistem file Multi-AZ melakukan fail over dan fail back ketika memperbarui penghitungan skala throughput, dan siap sepenuhnya. Sistem file single-AZ untuk sementara tidak dapat digunakan saat pembaruan.
6. Anda dapat memantau perkembangan pembaruan pada laman rincian Sistem file pada tab Pembaruan.

   Anda dapat memantau kemajuan pembaruan dengan menggunakan FSx konsol Amazon, the AWS CLI, dan API. Untuk informasi selengkapnya, lihat Memantau pembaruan kapasitas throughput.

Untuk mengubah kapasitas throughput sistem file (CLI)

Untuk menambah atau mengurangi kapasitas throughput sistem file, gunakan AWS CLI perintah update-file-system. Atur parameter berikut:

- `--file-system-id` untuk ID dari sistem file yang Anda perbarui.
- `ThroughputCapacity`ke nilai yang diinginkan; nilai yang valid adalah 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4608, 6144, 9216, 12288. MBps

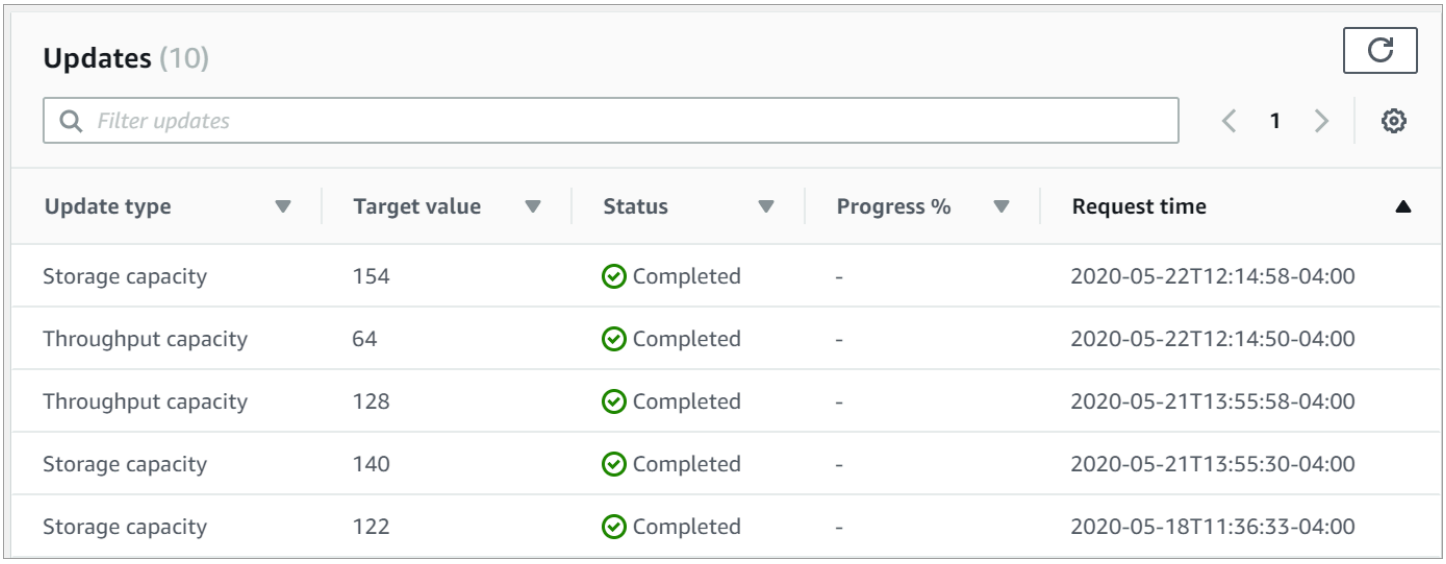
Anda dapat memantau kemajuan pembaruan dengan menggunakan FSx konsol Amazon, the AWS CLI, dan API. Untuk informasi selengkapnya, lihat Memantau pembaruan kapasitas throughput.

Memantau pembaruan kapasitas throughput

Anda dapat memantau kemajuan modifikasi kapasitas throughput menggunakan FSx konsol Amazon, API, dan. AWS CLI

Memantau perubahan kapasitas throughput pada konsol

Pada tab Pembaruan pada jendela Rincian sistem file, Anda dapat melihat 10 tindakan pembaruan terkini untuk masing-masing jenis tindakan pembaruan.



Untuk melakukan tindakan pembaruan kapasitas throughput, Anda dapat melihat informasi berikut.

Jenis pembaruan

Nilai yang mungkin adalah kapasitas Throughput.

Nilai target

Nilai yang diinginkan untuk mengubah kapasitas throughput pada sistem file.

Status

Status terkini dari pembaruan tersebut. Untuk pembaruan kapasitas throughput, nilai yang mungkin didapat adalah sebagai berikut:

- Tertunda - Amazon FSx telah menerima permintaan pembaruan, tetapi belum mulai memprosesnya.
- Sedang berlangsung - Amazon FSx sedang memproses permintaan pembaruan.
- Pengoptimalan yang diperbarui - Amazon FSx telah memperbarui jaringan I/O, CPU, dan sumber daya memori sistem file. Tingkat kinerja I/O disk baru tersedia untuk operasi tulis. Operasi baca Anda akan melihat kinerja I/O disk antara level sebelumnya dan level baru hingga sistem file Anda tidak lagi dalam keadaan ini.
- Selesai – Pembaruan kapasitas throughput berhasil diselesaikan.
- Gagal – Pembaruan kapasitas throughput gagal. Pilih tanda tanya (?) untuk melihat secara terperinci mengapa pembaruan throughput gagal.

Waktu permintaan

Waktu Amazon FSx menerima permintaan pembaruan.

Memantau perubahan dengan API AWS CLI dan

Anda dapat melihat dan memantau permintaan modifikasi kapasitas throughput sistem file menggunakan perintah describe-file-systemsCLI dan tindakan API DescribeFileSystems. Daftar `AdministrativeActions` berisi 10 tindakan pembaruan terkini untuk setiap jenis tindakan administratif. Jika Anda mengubah kapasitas throughput sistem file, muncul sebuah tindakan administratif `FILE_SYSTEM_UPDATE`.

Contoh berikut menunjukkan kutipan tanggapan atas perintah CLI `describe-file-systems`. Sistem file memiliki kapasitas throughput 8 MBps, dan kapasitas throughput target 256. MBps

```
.
.
.
    "ThroughputCapacity": 8,
```

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Saat Amazon FSx berhasil memproses tindakan, statusnya berubah menjadi`COMPLETED`. Kapasitas throughput yang baru kemudian tersedia untuk sistem file tersebut, dan tampak dalam properti `ThroughputCapacity`. Ini ditunjukkan dalam kutipan tanggapan atas perintah CLI describe-file-systems berikut.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Jika perubahan kapasitas throughput gagal, statusnya berubah menjadi `FAILED`, dan properti `FailureDetails` memberikan informasi tentang kegagalan tersebut. Untuk informasi lebih lanjut tentang pemecahan masalah atas tindakan gagal, lihat Pembaruan kapasitas penyimpanan atau throughput gagal dilakukan.

Menandai sumber daya Amazon FSx Anda

Untuk membantu Anda mengelola sistem file Anda dan sumber daya Windows File Server lainnya FSx , Anda dapat menetapkan metadata Anda sendiri ke setiap sumber daya dalam bentuk tag. Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Hal ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang telah Anda tetapkan. Topik ini menjelaskan tag dan menunjukkan cara membuatnya.

Topik

Dasar-dasar tag

Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri dari kunci dan nilai opsional, yang keduanya Anda tentukan.

Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menentukan satu set tag untuk akun Anda untuk sistem file Windows File Server yang membantu Anda melacak setiap pemilik instans dan tingkat tumpukan. FSx

Sebaiknya rancang serangkaian kunci tag yang memenuhi kebutuhan setiap jenis sumber daya. Penggunaan set kunci tag yang konsisten akan memudahkan manajemen sumber daya Anda. Anda dapat mencari dan memfilter sumber daya berdasarkan tag yang Anda tambahkan. Untuk informasi selengkapnya tentang cara menerapkan strategi penandaan sumber daya yang efektif, lihat AWS whitepaper Tagging Best Practices.

Tag tidak memiliki arti semantik ke Amazon FSx dan ditafsirkan secara ketat sebagai serangkaian karakter. Selain itu, tag tidak secara otomatis ditetapkan ke sumber daya Anda. Anda dapat mengedit kunci dan nilai tanda, dan dapat menghapus tanda dari sumber daya kapan saja. Anda dapat mengatur nilai tanda ke string kosong, tetapi tidak dapat mengatur nilai tanda ke null. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang telah ada pada sumber

daya tersebut, nilai yang baru akan menimpa nilai yang lama. Jika sumber daya dihapus, semua tanda untuk sumber daya tersebut juga akan dihapus.

Jika Anda menggunakan API FSx untuk Windows File Server, AWS CLI, atau AWS SDK, Anda dapat menggunakan tindakan `TagResource` API untuk menerapkan tag ke sumber daya yang ada. Selain itu, beberapa tindakan pembuatan sumber daya memungkinkan Anda menentukan tag untuk sumber daya saat sumber daya tersebut dibuat. Jika tag tidak dapat diterapkan selama pembuatan sumber daya, kami akan mengembalikan proses pembuatan sumber daya. Hal ini untuk memastikan bahwa sumber daya dibuat dengan tag atau tidak akan dibuat sama sekali, dan tidak akan ada sumber daya yang dibiarkan tidak bertanda. Dengan menandai sumber daya saat pembuatan, Anda dapat menghilangkan kebutuhan untuk menjalankan skrip penandaan kustom setelah pembuatan sumber daya. Untuk informasi selengkapnya tentang memungkinkan pengguna menandai sumber daya saat pembuatan, lihat Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat.

Pemberian tag pada sumber daya Anda

Anda dapat menandai FSx sumber daya Windows File Server yang ada di akun Anda. Jika menggunakan FSx konsol Amazon, Anda dapat menerapkan tag ke sumber daya menggunakan tab Tag di layar sumber daya yang relevan. Saat Anda membuat sumber daya, Anda dapat menerapkan kunci Nama dengan nilai, dan Anda dapat menerapkan tag pilihan Anda saat membuat sistem file baru. Konsol dapat mengatur sumber daya sesuai dengan tag Nama, tetapi tag ini tidak memiliki arti semantik apa pun FSx untuk layanan Server File Windows.

Anda dapat menerapkan izin tingkat sumber daya berbasis tag dalam kebijakan IAM Anda ke tindakan API Server File Windows FSx untuk Windows yang mendukung penandaan pada pembuatan untuk menerapkan kontrol terperinci atas pengguna dan grup yang dapat menandai sumber daya saat pembuatan. Sumber daya Anda diamankan secara tepat sejak pembuatan—tanda segera diterapkan pada sumber daya Anda, oleh karena itu, izin tingkat sumber daya berbasis tanda yang mengontrol penggunaan sumber daya langsung berlaku. Sumber daya Anda dapat dilacak dan dilaporkan dengan lebih akurat. Anda dapat menerapkan penggunaan pemberian tag pada sumber daya baru serta mengontrol kunci dan nilai tag mana yang ditetapkan pada sumber daya Anda.

Anda juga dapat menerapkan izin tingkat sumber daya ke `TagResource` dan `UntagResource` FSx untuk tindakan API Server File Windows dalam kebijakan IAM Anda untuk mengontrol kunci dan nilai tag mana yang ditetapkan pada sumber daya yang ada.

Untuk informasi selengkapnya tentang penandaan sumber daya untuk penagihan, lihat Menggunakan tanda alokasi biaya dalam Buku Panduan AWS Billing .

Pembatasan tanda

Batasan dasar berikut berlaku untuk tag:

- Jumlah maksimum tag per sumber daya – 50
- Untuk setiap sumber daya, setiap kunci tanda harus unik, dan setiap kunci tanda hanya dapat memuat satu nilai.
- Panjang kunci maksimum – 128 karakter Unicode dalam UTF-8
- Panjang nilai maksimum – 256 karakter Unicode dalam UTF-8
- Karakter yang diizinkan FSx untuk tag Windows File Server adalah: huruf, angka, dan spasi yang dapat direpresentasikan dalam UTF-8, dan karakter berikut: + - =. _:/@.
- Kunci dan nilai tag peka huruf besar dan kecil.
- `aws:`Awalan dicadangkan untuk AWS digunakan. Jika tag memiliki kunci tag dengan awalan ini, Anda tidak dapat mengedit atau menghapus kunci atau nilai tag tersebut. Tag dengan awalan `aws:` tidak dihitung terhadap tag per batas sumber daya.

Anda tidak dapat menghapus sumber daya hanya berdasarkan tagnya; Anda harus menentukan pengenal sumber daya. Misalnya, untuk menghapus sistem file yang Anda tag dengan kunci tag yang disebut`DeleteMe`, Anda harus menggunakan `DeleteFileSystem` tindakan dengan pengenal sumber daya sistem file, seperti fs-1234567890abcdef0.

Saat Anda menandai sumber daya publik atau bersama, tag yang Anda tetapkan hanya tersedia untuk Anda Akun AWS; tidak ada orang lain yang Akun AWS akan memiliki akses ke tag tersebut. Untuk kontrol akses berbasis tag ke sumber daya bersama, masing-masing Akun AWS harus menetapkan set tag sendiri untuk mengontrol akses ke sumber daya.

Izin diperlukan untuk menandai sumber daya

Untuk informasi selengkapnya tentang izin yang diperlukan untuk menandai FSx sumber daya Amazon saat pembuatan, lihatMemberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat. Untuk informasi selengkapnya tentang penggunaan tag untuk membatasi akses ke FSx sumber daya Amazon dalam kebijakan IAM, lihat. Menggunakan tag untuk mengontrol akses ke FSx sumber daya Amazon Anda

Perbarui sistem file menggunakan AWS CLI

Ada tiga elemen yang dapat Anda perbarui menggunakan prosedur dalam panduan ini. Semua elemen lain dari sistem file Anda yang dapat Anda perbarui, Anda dapat melakukannya dari konsol. Prosedur ini mengasumsikan Anda telah AWS CLI diinstal dan dikonfigurasi di komputer lokal Anda. Untuk informasi lebih lanjut, lihat Instal dan Konfigurasikan di Panduan Pengguna AWS Command Line Interface .

- AutomaticBackupRetentionDays— jumlah hari yang Anda ingin menyimpan backup otomatis untuk sistem file Anda.
- DailyAutomaticBackupStartTime— waktu hari di Coordinated Universal Time (UTC) yang Anda inginkan untuk memulai jendela pencadangan otomatis harian. Window adalah 30 menit mulai dari waktu yang ditentukan ini. Window tidak dapat menindih Window cadangan pemeliharaan mingguan.
- WeeklyMaintenanceStartTime— waktu dalam seminggu Anda ingin jendela pemeliharaan dimulai. Hari 1 adalah Senin, 2 adalah Selasa, dan seterusnya. Window adalah 30 menit mulai dari waktu yang ditentukan ini. Window ini tidak dapat menindih window cadangan otomatis harian.

Prosedur berikut menguraikan cara memperbarui sistem file Anda dengan AWS CLI.

Untuk memperbarui berapa lama cadangan otomatis dipertahankan untuk sistem file Anda

1. Buka prompt perintah atau terminal di komputer Anda.
2. Jalankan perintah berikut, dengan mengganti ID sistem file dengan ID untuk sistem file Anda, dan jumlah hari di mana Anda ingin mempertahankan cadangan otomatis Anda.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

Untuk memperbarui window cadangan harian sistem file Anda

1. Buka prompt perintah atau terminal di komputer Anda.
2. Jalankan perintah berikut, ganti ID sistem file dengan ID untuk sistem file Anda, serta waktu kapan Anda ingin memulai window.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

Untuk memperbarui window pemeliharaan mingguan sistem file Anda

1. Buka prompt perintah atau terminal di komputer Anda.
2. Jalankan perintah berikut, ganti ID sistem file dengan ID untuk sistem file Anda, serta tanggal dan waktu dengan kapan Anda ingin memulai window.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

Melindungi data Anda dengan backup, shadow copy, dan replikasi terjadwal

Selain secara otomatis mereplikasi data sistem file Anda untuk memastikan daya tahan tinggi, Amazon FSx memberi Anda opsi berikut untuk lebih melindungi data yang disimpan di sistem file Anda:

- FSx Pencadangan Amazon asli mendukung retensi cadangan dan kebutuhan kepatuhan Anda di Amazon. FSx
- AWS Backup Pencadangan sistem FSx file Amazon Anda adalah bagian dari solusi pencadangan terpusat dan otomatis di seluruh AWS layanan di cloud dan di tempat.
- Shadow copy Windows memungkinkan pengguna Anda untuk dengan mudah membatalkan perubahan file dan membandingkan versi file dengan memulihkan file ke versi sebelumnya.
- AWS DataSync replikasi terjadwal sistem FSx file Amazon Anda ke sistem file kedua memberikan perlindungan dan pemulihan data.

Topik

Melindungi data Anda dengan backup

Anda dapat melindungi data pada sistem file Windows File Server Anda FSx dengan mengambil cadangan sistem file biasa. Amazon FSx memberi Anda beberapa opsi untuk membuat cadangan sistem file Anda. Anda dapat menggunakan backup harian otomatis untuk mengambil cadangan setiap hari. Anda dapat mengambil cadangan yang diprakarsai pengguna dari sistem file Anda kapan saja. Anda juga dapat menggunakan AWS Backup sebagai bagian dari solusi cadangan terpusat untuk AWS sumber daya Anda. Solusi pencadangan ini dapat membantu Anda memenuhi kebutuhan penyimpanan data, bisnis, dan kepatuhan Anda.

Sebaiknya gunakan pencadangan harian otomatis yang diaktifkan secara default untuk sistem file Anda, dan gunakan AWS Backup untuk solusi pencadangan terpusat di seluruh. Layanan AWS AWS

Backup memungkinkan Anda mengonfigurasi paket cadangan tambahan dengan frekuensi yang berbeda (misalnya, beberapa kali sehari, harian, atau mingguan) dan periode retensi.

Dengan Amazon FSx, backup, sangat tahan lama file-system-consistent, dan inkremental. Setiap cadangan berisi semua informasi yang diperlukan untuk membuat sistem file baru, secara efektif memulihkan point-in-time snapshot dari sistem file. Untuk memastikan konsistensi sistem file, Amazon FSx menggunakan Volume Shadow Copy Service (VSS) di Microsoft Windows. Untuk memastikan daya tahan tinggi, Amazon FSx menyimpan cadangan di Amazon Simple Storage Service (Amazon S3).

FSx Pencadangan Amazon bersifat inkremental, baik yang dihasilkan menggunakan pencadangan harian otomatis atau fitur pencadangan yang diprakarsai pengguna. Hal ini berarti hanya data pada sistem file yang telah berubah setelah backup terbaru Anda saja yang disimpan. Hal ini meminimalisir waktu yang diperlukan untuk membuat backup dan menghemat biaya penyimpanan dengan tidak menduplikasi data.

Pada titik tertentu selama proses pencadangan, penyimpanan I/O dapat ditangguhkan sebentar, biasanya selama beberapa detik. Karena layanan VSS perlu menyiram setiap penulisan yang di-cache ke disk sebelum melanjutkan I/O, durasi jeda mungkin lebih lama jika beban kerja Anda memiliki sejumlah besar operasi tulis per detik (). `DataWriteOperations` Sebagian besar pengguna akhir dan aplikasi akan mengalami suspensi I/O ini sebagai jeda I/O singkat. Aplikasi Anda mungkin memiliki sensitivitas yang berbeda terhadap pengaturan batas waktu tergantung pada bagaimana mereka dikonfigurasi.

Membuat cadangan reguler untuk sistem file Anda adalah praktik terbaik yang melengkapi replikasi yang dilakukan FSx Amazon untuk Windows File Server untuk sistem file Anda. FSx Pencadangan Amazon membantu mendukung retensi cadangan dan kebutuhan kepatuhan Anda. Bekerja dengan FSx cadangan Amazon itu mudah, apakah itu membuat cadangan, menyalin cadangan, memulihkan sistem file dari cadangan, atau menghapus cadangan. Perhatikan bahwa untuk melihat penggunaan untuk cadangan sistem file tunggal, Anda harus mengaktifkan tag untuk cadangan tertentu dan mengaktifkan pelaporan penagihan berbasis tag.

Topik

- Bekerja dengan backup harian otomatis
- Bekerja dengan backup yang diinisiasi pengguna
- Menggunakan AWS Backup dengan Amazon FSx
- Menyalin cadangan

- Memulihkan backup ke sistem file baru
- Membuat backup yang diinisiasi pengguna
- Menghapus cadangan
- Ukuran backup
- Menyalin cadangan dalam akun yang sama
- Memulihkan cadangan ke sistem file baru

Bekerja dengan backup harian otomatis

Secara default, Amazon FSx mengambil cadangan harian otomatis dari sistem file Anda. Backup harian otomatis ini terjadi selama jendela backup harian didirikan ketika Anda membuat sistem file. Ketika Anda memilih jendela cadangan harian Anda, kami sarankan Anda memilih waktu yang nyaman dalam sehari yang berada di luar jam operasi normal untuk aplikasi yang menggunakan sistem file. Kami juga merekomendasikan memilih jendela cadangan di luar jendela pemeliharaan karena pencadangan otomatis mungkin tidak terjadi jika ada pemeliharaan sistem file yang sedang berlangsung.

Backup harian otomatis disimpan untuk jangka waktu tertentu, yang dikenal sebagai periode penyimpanan. Saat Anda membuat sistem file di FSx konsol Amazon, periode retensi cadangan harian otomatis default adalah 30 hari. Periode retensi default berbeda di Amazon FSx API dan CLI. Anda dapat mengatur periode penyimpanan backup menjadi antara 0–90 hari. Pengaturan periode penyimpanan ke 0 (nol) hari akan mematikan backup harian otomatis. Backup harian otomatis dihapus saat sistem file dihapus.

> **Note**
>
> Pengaturan periode penyimpanan ke 0 hari berarti sistem file Anda tidak pernah dicadangkan secara otomatis. Kami sangat menyarankan Anda menggunakan backup harian otomatis untuk sistem file yang memiliki fungsionalitas dengan tingkat kepentingan apa saja yang ter-associate dengan sistem file.

Anda dapat menggunakan AWS CLI atau salah satu AWS SDKs untuk mengubah jendela cadangan dan periode retensi cadangan untuk sistem file Anda. Gunakan Operasi API `UpdateFileSystem` atau Perintah CLI `update-file-system`. Untuk informasi selengkapnya, lihat Perbarui sistem file menggunakan AWS CLI.

> **Important**
>
> Menurunkan periode retensi untuk pencadangan harian otomatis akan mengakibatkan penghapusan cadangan permanen di luar jendela retensi baru. Pastikan Anda tidak lagi membutuhkan cadangan lama ini sebelum melanjutkan.

Bekerja dengan backup yang diinisiasi pengguna

Dengan Amazon FSx, Anda dapat secara manual mengambil cadangan sistem file Anda kapan saja. Anda dapat melakukannya menggunakan FSx konsol Amazon, API, atau AWS Command Line Interface (AWS CLI). Pencadangan sistem file FSx Amazon yang diprakarsai pengguna Anda tidak pernah kedaluwarsa, dan tersedia selama Anda ingin menyimpannya. Backup yang diinisiasi pengguna dipertahankan bahkan setelah Anda menghapus sistem file yang di-backup. Anda dapat menghapus cadangan yang diprakarsai pengguna hanya dengan menggunakan FSx konsol Amazon, API, atau CLI. Mereka tidak pernah dihapus secara otomatis oleh Amazon FSx. Untuk informasi selengkapnya, lihat Menghapus cadangan.

Jika pencadangan dimulai saat sistem file sedang dimodifikasi (seperti selama pembaruan kapasitas throughput, atau selama pemeliharaan sistem file), permintaan cadangan akan diantrian dan akan dilanjutkan ketika aktivitas selesai.

Untuk mempelajari cara mengambil backup yang diprakarsai pengguna dari sistem file Anda, lihat. Membuat backup yang diinisiasi pengguna

Menggunakan AWS Backup dengan Amazon FSx

AWS Backup adalah cara sederhana dan hemat biaya untuk melindungi data Anda dengan mencadangkan sistem file Amazon FSx Anda. AWS Backup adalah layanan cadangan terpadu yang dirancang untuk menyederhanakan pembuatan, penyalinan, pemulihan, dan penghapusan cadangan, sambil memberikan pelaporan dan audit yang lebih baik. AWS Backup membuatnya lebih mudah untuk mengembangkan strategi cadangan terpusat untuk kepatuhan hukum, peraturan, dan profesional. AWS Backup juga membuat melindungi volume AWS penyimpanan, database, dan sistem file Anda lebih sederhana dengan menyediakan tempat sentral di mana Anda dapat melakukan hal berikut:

- Konfigurasikan dan audit AWS sumber daya yang ingin Anda cadangkan.
- Otomatiskan penjadwalan cadangan.

- Tetapkan kebijakan penyimpanan.
- Salin cadangan di seluruh AWS Wilayah dan di seluruh AWS akun.
- Pantau semua aktivitas backup, penyalinan, dan pemulihan terbaru.

AWS Backup menggunakan fungsionalitas cadangan bawaan Amazon FSx. Cadangan yang diambil dari AWS Backup konsol memiliki tingkat konsistensi dan kinerja sistem file yang sama, dan opsi pemulihan yang sama dengan cadangan yang diambil melalui konsol Amazon. FSx Pencadangan yang diambil AWS Backup bersifat inkremental relatif terhadap FSx cadangan Amazon lainnya yang Anda ambil, baik yang dimulai pengguna atau otomatis.

Jika Anda menggunakannya AWS Backup untuk mengelola cadangan ini, Anda mendapatkan fungsionalitas tambahan, seperti opsi retensi tak terbatas dan kemampuan untuk membuat cadangan terjadwal sesering setiap jam. Selain itu, AWS Backup pertahankan cadangan Anda yang tidak dapat diubah bahkan setelah sistem file sumber dihapus. Hal ini melindungi dari penghapusan yang tidak disengaja atau berbahaya.

Pencadangan yang diambil oleh dianggap sebagai cadangan AWS Backup yang diprakarsai pengguna, dan mereka dihitung terhadap kuota cadangan yang diprakarsai pengguna untuk Amazon. FSx Anda dapat melihat dan memulihkan cadangan yang diambil AWS Backup di FSx konsol Amazon, CLI, dan API. Namun, Anda tidak dapat menghapus cadangan yang diambil AWS Backup di FSx konsol Amazon, CLI, atau API. Untuk informasi selengkapnya tentang cara menggunakan AWS Backup untuk mencadangkan sistem FSx file Amazon, lihat Bekerja dengan Sistem FSx File Amazon di Panduan AWS Backup Pengembang.

Menyalin cadangan

Anda dapat menggunakan Amazon FSx untuk menyalin cadangan secara manual dalam AWS akun yang sama ke AWS Wilayah lain (Salinan lintas wilayah) atau dalam Wilayah yang sama (Salinan dalam AWS wilayah). Anda dapat membuat salinan lintas wilayah hanya dalam AWS partisi yang sama. Anda dapat membuat salinan cadangan yang dimulai pengguna menggunakan FSx konsol Amazon, AWS CLI, atau API. Saat Anda membuat salinan backup yang diinisiasi pengguna, salinan tersebut memiliki jenis `USER_INITIATED`.

Anda juga dapat menggunakan AWS Backup untuk menyalin cadangan di seluruh AWS Wilayah dan di seluruh akun. AWS AWS Backup adalah layanan manajemen cadangan yang dikelola sepenuhnya yang menyediakan antarmuka pusat untuk rencana pencadangan berbasis kebijakan. Dengan pengelolaan lintas akun, Anda dapat secara otomatis menggunakan kebijakan backup untuk menerapkan rencana pencadangan di seluruh akun dalam organisasi Anda.

Salinan backup lintas wilayah Sangat berharga untuk pemulihan bencana lintas-Wilayah. Anda mengambil cadangan dan menyalinnya ke AWS Wilayah lain sehingga jika terjadi bencana di AWS Wilayah utama, Anda dapat memulihkan dari cadangan dan memulihkan ketersediaan dengan cepat di Wilayah lain AWS . Anda juga dapat menggunakan salinan cadangan untuk mengkloning kumpulan data file Anda ke AWS Wilayah lain atau dalam Wilayah yang sama AWS . Anda membuat salinan cadangan dalam AWS akun yang sama (Lintas wilayah atau Dalam wilayah) dengan menggunakan FSx konsol Amazon, AWS CLI, atau Amazon FSx API. Anda juga dapat menggunakan AWS Backup untuk melakukan salinan backup, baik sesuai permintaan atau berbasis kebijakan.

Salinan cadangan lintas akun berharga untuk memenuhi persyaratan kepatuhan peraturan untuk menyalin cadangan ke akun yang terisolasi. Mereka juga menyediakan lapisan perlindungan data tambahan untuk membantu mencegah penghapusan cadangan yang tidak disengaja atau berbahaya, kehilangan kredensil, atau kompromi kunci. AWS KMS Support backup lintas akun fan-in (penyalinan backup dari beberapa akun utama ke satu akun salinan backup yang terisolasi) dan fan-out (penyalinan backup dari satu akun utama ke beberapa akun salinan backup yang terisolasi).

Anda dapat membuat salinan cadangan lintas akun AWS Backup dengan menggunakan AWS Organizations dukungan. Batasan akun untuk salinan lintas akun ditentukan oleh AWS Organizations kebijakan. Untuk informasi selengkapnya tentang penggunaan AWS Backup untuk membuat salinan cadangan lintas akun, lihat Membuat salinan cadangan Akun AWS di Panduan AWS Backup Pengembang.

Batasan salinan Backup

Berikut ini adalah beberapa batasan saat Anda menyalin cadangan:

- Salinan cadangan Lintas Wilayah hanya didukung antara dua AWS Wilayah komersial, antara Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia), dan antara Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat), tetapi tidak di seluruh wilayah tersebut.
- Salinan backup Lintas-Wilayah tidak di-support di WIlayah-wilayah opt-in.
- Anda dapat membuat salinan cadangan In-Region dalam AWS Wilayah mana pun.
- Backup sumber harus memiliki status `AVAILABLE` sebelum Anda dapat menyalinnya.
- Anda tidak dapat menghapus backup sumber jika sedang disalin. Mungkin ada jeda singkat antara saat backup tujuan menjadi tersedia dan ketika Anda diizinkan untuk menghapus backup sumber. Anda harus mengingat bahwa terdapat jeda jika Anda mencoba lagi menghapus backup sumber.
- Anda dapat memiliki hingga lima permintaan salinan cadangan yang sedang berlangsung ke satu AWS Wilayah tujuan per akun.

Izin untuk penyalinan backup lintas Wilayah

Anda menggunakan pernyataan kebijakan IAM untuk memberikan izin untuk melakukan operasi penyalinan backup. Untuk berkomunikasi dengan AWS Wilayah sumber untuk meminta salinan cadangan Lintas wilayah, pemohon (peran IAM atau pengguna IAM) harus memiliki akses ke cadangan sumber dan Wilayah sumber. AWS

Anda menggunakan kebijakan untuk memberikan izin melakukan tindakan `CopyBackup` untuk operasi penyalinan backup. Tentukan tindakan dalam bidang `Action` kebijakan, dan tentukan nilai sumber daya dalam bidang `Resource` kebijakan, sebagaimana contoh berikut ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

Untuk informasi selengkapnya tentang kebijakan IAM, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.

Salinan penuh dan bersifat tambahan

Saat Anda menyalin cadangan ke AWS Wilayah tujuan atau AWS akun tujuan yang berbeda dari cadangan sumber, salinan pertama adalah salinan cadangan lengkap, bahkan jika Anda menggunakan kunci KMS yang sama untuk mengenkripsi salinan sumber dan tujuan cadangan.

Setelah salinan cadangan pertama, semua salinan cadangan berikutnya ke Wilayah tujuan yang sama dalam AWS akun yang sama bersifat inkremental, asalkan Anda belum menghapus semua cadangan yang disalin sebelumnya di Wilayah tersebut dan telah menggunakan kunci yang sama. AWS KMS Jika salah satu kondisi tidak terpenuhi, operasi penyalinan menghasilkan salinan cadangan penuh (bukan tambahan).

Untuk mempelajari cara menyalin cadangan sistem file Anda, lihat. Menyalin cadangan dalam akun yang sama

Memulihkan backup ke sistem file baru

Anda dapat menggunakan cadangan yang tersedia untuk membuat sistem file baru, secara efektif memulihkan point-in-time snapshot dari sistem file lain. Anda dapat memulihkan cadangan menggunakan konsol, AWS CLI, atau salah satu AWS SDKs. Memulihkan backup ke sistem file yang baru menghabiskan waktu yang sama dengan membuat sistem file baru. Data yang dipulihkan dari backup di-lazy-load ke sistem file, pada waktu lazy-load Anda akan mengalami latensi yang sedikit lebih tinggi.

Untuk memastikan bahwa pengguna dapat terus mengakses sistem file yang dipulihkan, pastikan bahwa domain Active Directory yang terkait dengan sistem file yang dipulihkan sama dengan sistem file asli, atau dipercaya oleh domain Active Directory dari sistem file asli. Untuk informasi selengkapnya tentang Active Directory, lihatBekerja dengan Microsoft Active Directory.

Untuk mempelajari cara mengembalikan cadangan ke sistem file baru FSx untuk Windows, lihatMemulihkan cadangan ke sistem file baru.

> **Note**
>
> Anda hanya dapat mengembalikan cadangan sistem file ke sistem file baru dengan jenis penyebaran dan kapasitas penyimpanan yang sama seperti aslinya. Anda dapat meningkatkan kapasitas penyimpanan sistem file baru setelah tersedia. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan.

Anda dapat mengubah salah satu pengaturan sistem file berikut saat memulihkan cadangan ke sistem file baru:

- Jenis penyimpanan
- Kapasitas throughput
- VPC
- Zona Ketersediaan
- Subnet
- Grup keamanan VPC
- Konfigurasi Direktori Aktif
- AWS KMS kunci enkripsi
- Waktu mulai pencadangan otomatis harian

- Window pemeliharaan mingguan

Membuat backup yang diinisiasi pengguna

Selain backup sistem file harian otomatis, Anda dapat membuat cadangan sistem file yang dimulai pengguna kapan saja, menggunakan FSx konsol Amazon seperti yang dijelaskan dalam prosedur berikut.

Untuk membuat backup sistem file yang diinisiasi pengguna

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Dari dasbor konsol, pilih nama sistem file yang ingin Anda backup.
3. Dari Tindakan, pilih Buat backup.
4. Di kotak dialog Buat backup yang terbuka, berikan nama untuk backup Anda. Nama Backup dapat terdiri dari maksimal 256 karakter Unicode, termasuk huruf, spasi, angka, dan karakter khusus . + - = _ : /
5. Pilih Buat cadangan.

Anda sekarang telah membuat backup sistem file Anda. Anda dapat menemukan tabel semua cadangan Anda di FSx konsol Amazon dengan memilih Cadangan di navigasi sisi kiri. Cadangan baru yang diprakarsai pengguna Anda memiliki tipe`USER_INITIATED`, dan statusnya `CREATING` sampai menjadi. `AVAILABLE` Untuk informasi selengkapnya, lihat Bekerja dengan backup yang diinisiasi pengguna.

Menghapus cadangan

Anda dapat menghapus pencadangan harian yang dimulai pengguna dan otomatis dari sistem file Anda menggunakan konsol Amazon FSx , CLI, atau API, yang dijelaskan dalam prosedur berikut. Untuk menghapus cadangan yang diambil oleh AWS Backup, yang memiliki jenis AWS Backup, Anda harus menggunakan konsol, CLI AWS Backup , atau API. Menghapus cadangan adalah tindakan permanen dan tidak dapat dipulihkan. Data apapun di backup yang terhapus juga ikut dihapus. Jangan hapus cadangan kecuali Anda yakin tidak memerlukan cadangan tersebut lagi di masa mendatang.

Untuk menghapus cadangan (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.

2. Dari dasbor konsol, pilih Backup dari navigasi sebelah kiri.
3. Pilih backup yang ingin Anda hapus dari tabel backup, dan kemudian pilih Hapus backup.
4. Di kotak dialog Hapus cadangan yang terbuka, konfirmasikan bahwa ID cadangan tersebut mengidentifikasi cadangan yang ingin Anda hapus.
5. Konfirmasikan bahwa kotak centang dicentang untuk cadangan yang ingin Anda hapus.
6. Pilih Hapus backup.

Cadangan Anda dan semua data yang termasuk kini dihapus secara permanen dan tidak dapat dipulihkan.

Ukuran backup

Ukuran cadangan ditentukan menggunakan penyimpanan yang digunakan dalam sistem file, bukan total kapasitas penyimpanan yang disediakan. Ukuran backup Anda akan tergantung pada kapasitas penyimpanan yang digunakan serta jumlah churn data pada sistem file Anda. Bergantung pada bagaimana data Anda didistribusikan di seluruh volume penyimpanan sistem file dan seberapa sering itu berubah, total penggunaan cadangan Anda mungkin lebih besar atau kurang dari kapasitas penyimpanan yang Anda gunakan. Saat Anda menghapus sebuah cadangan, hanya data yang unik dari cadangan tersebut yang dihapus.

Untuk menyediakan cadangan yang tahan lama file-system-consistent, dan inkremental, Amazon FSx mencadangkan data di tingkat blok. Data pada volume penyimpanan sistem file dapat disimpan di beberapa blok tergantung pada pola yang ditulis atau ditulis ulang. Akibatnya, ukuran total penggunaan cadangan mungkin tidak sesuai dengan ukuran file dan direktori yang tepat pada sistem file. Penggunaan dan biaya cadangan Anda secara keseluruhan dapat ditemukan di AWS Billing Dasbor atau AWS Cost Management Console.

Gunakan tag untuk mengatur AWS tagihan Anda untuk mencerminkan struktur biaya Anda sendiri. Untuk melakukan ini, daftar untuk mendapatkan Akun AWS tagihan Anda dengan nilai kunci tag disertakan. Kemudian, untuk melihat biaya sumber daya gabungan, atur informasi penagihan Anda sesuai dengan sumber daya Anda dengan nilai kunci tag yang sama. Misalnya, Anda dapat memberi tag pada beberapa sumber daya dengan nama aplikasi tertentu, kemudian mengatur informasi penagihan Anda untuk melihat biaya total aplikasi tersebut di beberapa layanan. Untuk informasi selengkapnya, lihat Menggunakan Tag Alokasi Biaya dalam Panduan Pengguna AWS Billing .

> **Note**
>
> Saat Anda meningkatkan kapasitas penyimpanan, proses migrasi data dari kumpulan disk penyimpanan lama ke set disk penyimpanan baru yang lebih besar dapat mengakibatkan peningkatan sementara dalam penggunaan cadangan hingga cadangan yang terkait dengan kumpulan disk penyimpanan lama dihapus. Jika penyimpanan sistem file Anda hanya digunakan sebagian sebelum Anda meningkatkan kapasitas penyimpanan, ukuran data yang perlu dimigrasikan ke disk baru mungkin lebih besar dari ukuran data yang ada pada disk penyimpanan asli. Hal ini dapat menyebabkan peningkatan penggunaan cadangan hingga tingkat kapasitas penyimpanan baru. Anda harus mempertimbangkan dampak peningkatan kapasitas penyimpanan pada perencanaan cadangan Anda.

Menyalin cadangan dalam akun yang sama

Anda dapat menggunakan AWS Management Console dan AWS CLI untuk menyalin cadangan secara manual dalam AWS akun yang sama ke akun lain Wilayah AWS (Salinan lintas wilayah) atau dalam salinan yang sama Wilayah AWS (In-region copy) menggunakan prosedur berikut.

Untuk menyalin sebuah backup dalam akun yang sama (Lintas-WIlayah atau Dalam-Wilayah) menggunakan konsol

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Pada panel navigasi, pilih Backup.
3. Di tabel Backup, pilih backup yang ingin Anda salin, dan kemudian pilih Salin backup.
4. Di bagian Pengaturan, lakukan hal berikut:
   - Dalam daftar Wilayah Tujuan, pilih AWS Wilayah tujuan untuk menyalin cadangan. Tujuan dapat berada di AWS Wilayah lain (salinan Lintas wilayah) atau dalam Wilayah yang sama AWS (Salinan dalam wilayah).
   - (Opsional) Pilih Salin Tag untuk menyalin tag dari backup sumber untuk backup tujuan. Jika Anda memilih Salin Tag dan juga menambahkan tag pada langkah 6, semua tag digabung.
5. Untuk Enkripsi, pilih kunci AWS KMS enkripsi untuk mengenkripsi cadangan yang disalin.
6. Untuk Tag - opsional, masukkan kunci dan nilai untuk menambahkan tag untuk backup yang disalin. Jika Anda menambahkan tag di sini dan juga Salin tag terpilih pada langkah 4, semua tag tergabung.

7. Pilih Salin cadangan.

Cadangan Anda disalin dalam AWS akun yang sama ke AWS Wilayah yang dipilih.

Untuk menyalin backup dalam akun yang sama (lintas-Wilayah atau dalam-Wilayah) menggunakan CLI

- Gunakan perintah `copy-backup` CLI atau operasi CopyBackupAPI untuk menyalin cadangan dalam AWS akun yang sama, baik di seluruh AWS Wilayah atau di dalam Wilayah. AWS

  Perintah berikut menyalin backup dengan sebuah ID `backup-0abc123456789cba7` dari Wilayah `us-east-1`.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  Respoons menunjukkan deskripsi backup yang disalin.

  Anda dapat melihat cadangan Anda di FSx konsol Amazon atau secara terprogram menggunakan perintah `describe-backups` CLI atau operasi API. DescribeBackups

Memulihkan cadangan ke sistem file baru

Anda dapat mengembalikan cadangan sistem file untuk membuat sistem file baru menggunakan AWS Management Console, CLI, dan API, seperti yang dijelaskan dalam prosedur berikut.

Untuk memulihkan sistem file dari sebuah backup

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Dari dasbor konsol, pilih Backup dari navigasi sebelah kiri.
3. Pilih backup yang ingin Anda pulihkan dari tabel Backup, dan kemudian pilih Pulihkan backup.

   Dengan melakukannya maka akan membuka wizard pembuatan sistem file. Wizard ini identik dengan wizard pembuatan sistem file standar, kecuali Jenis Deployment dan Kapasitas penyimpanan yang telah ditetapkan dan tidak dapat diubah. Namun, Anda dapat mengubah kapasitas throughput, VPC ter-associate, dan pengaturan lainnya, dan jenis penyimpanan. Jenis

penyimpanan diatur ke SSD secara default, tetapi Anda dapat mengubahnya menjadi HDD Dalam kondisi berikut:

- Jenis deployment sistem file adalah Multi-AZ atau Single-AZ 2.
- Kapasitas penyimpanan adalah sedikitnya 2.000 GiB.

4. Selesaikan wizard seperti yang Anda lakukan ketika Anda membuat sistem file baru.
5. Pilih Periksa dan buat.
6. Tinjau pengaturan yang Anda pilih untuk sistem FSx file Amazon Anda, lalu pilih Buat sistem file.

   Amazon FSx membuat sistem file baru, dan setelah statusnya berubah`AVAILABLE`, Anda dapat menggunakan sistem file seperti biasa.

Melindungi data Anda dengan salinan bayangan

Shadow copy Microsoft Windows adalah snapshot dari sistem file Windows pada suatu titik waktu. Dengan salinan bayangan diaktifkan, pengguna dapat dengan cepat memulihkan file yang dihapus atau diubah yang disimpan di jaringan, dan membandingkan versi file. Administrator penyimpanan dapat dengan mudah menjadwalkan salinan bayangan untuk diambil secara berkala menggunakan PowerShell perintah Windows.

Salinan bayangan disimpan bersama data sistem file Anda, dan menggunakan kapasitas penyimpanan sistem file hanya untuk bagian file yang diubah. Semua salinan bayangan yang disimpan dalam sistem file Anda disertakan dalam pencadangan sistem file.

> **Note**
>
> Salinan bayangan tidak diaktifkan FSx untuk Windows File Server secara default. Untuk melindungi data pada sistem file Anda menggunakan salinan bayangan, Anda harus mengaktifkan salinan bayangan dan mengatur jadwal salinan bayangan pada sistem file Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi salinan bayangan untuk menggunakan penyimpanan dan jadwal default.

> **Warning**
>
> Shadow copy bukan pengganti untuk backup. Jika Anda mengaktifkan shadow copy, pastikan bahwa Anda tetap melakukan backup biasa.

Topik

Praktik terbaik saat menggunakan salinan bayangan

Anda dapat mengaktifkan salinan bayangan untuk sistem file Anda untuk memungkinkan pengguna akhir melihat dan memulihkan file atau folder individual dari snapshot sebelumnya di Windows File Explorer. Amazon FSx menggunakan fitur salinan bayangan seperti yang disediakan oleh Microsoft Windows Server. Gunakan praktik terbaik ini untuk salinan bayangan:

- Pastikan sistem file Anda memiliki sumber daya kinerja yang memadai: Microsoft Windows menggunakan copy-on-write metode untuk merekam perubahan sejak titik salinan bayangan terbaru, dan copy-on-write aktivitas ini dapat menghasilkan hingga tiga operasi I/O untuk setiap operasi penulisan file.
- Gunakan penyimpanan SSD dan tingkatkan kapasitas throughput: Karena Windows memerlukan kinerja I/O tingkat tinggi untuk mempertahankan salinan bayangan, kami merekomendasikan

penggunaan penyimpanan SSD dan meningkatkan kapasitas throughput hingga nilai setinggi tiga kali lipat dari beban kerja yang Anda harapkan. Ini membantu memastikan bahwa sistem file Anda memiliki sumber daya yang cukup untuk menghindari masalah seperti penghapusan salinan bayangan yang tidak diinginkan.

- Pertahankan hanya jumlah salinan bayangan yang Anda butuhkan: Jika Anda memiliki sejumlah besar salinan bayangan — misalnya, lebih dari 64 salinan bayangan terbaru — atau salinan bayangan yang menempati sejumlah besar penyimpanan (skala TB) pada satu sistem file, proses seperti failover dan failback mungkin membutuhkan waktu ekstra. Ini karena kebutuhan Windows FSx untuk menjalankan pemeriksaan konsistensi pada penyimpanan salinan bayangan. Anda mungkin juga mengalami latensi operasi I/O yang lebih tinggi karena kebutuhan Windows FSx untuk melakukan copy-on-write aktivitas sambil mempertahankan salinan bayangan. Untuk meminimalkan ketersediaan dan dampak kinerja dari salinan bayangan, hapus salinan bayangan yang tidak digunakan secara manual atau konfigurasikan skrip untuk menghapus salinan bayangan lama di sistem file Anda secara otomatis.

> **Note**
>
> Selama peristiwa failover untuk sistem file multi-AZ, FSx untuk Windows menjalankan pemeriksaan konsistensi yang memerlukan pemindaian penyimpanan salinan bayangan pada sistem file Anda sebelum server file aktif baru online. Durasi pemeriksaan konsistensi terkait dengan jumlah salinan bayangan pada sistem file Anda serta penyimpanan yang dikonsumsi. Untuk mencegah kejadian failover dan failback yang tertunda, sebaiknya simpan kurang dari 64 salinan bayangan pada sistem file Anda dan ikuti langkah-langkah di bawah ini untuk memantau dan menghapus salinan bayangan tertua Anda secara teratur.

Menyiapkan salinan bayangan

Anda mengaktifkan dan menjadwalkan salinan bayangan berkala pada sistem file Anda menggunakan PowerShell perintah Windows yang ditentukan oleh Amazon FSx. Berikut ini adalah tiga pengaturan utama saat mengonfigurasi salinan bayangan pada sistem file Windows File Server Anda FSx :

- Mengatur jumlah maksimum penyimpanan yang dapat dikonsumsi salinan bayangan pada sistem file Anda

- (Opsional) Mengatur jumlah maksimum salinan bayangan yang dapat disimpan di sistem file Anda. Nilai defaultnya adalah 20.
- (Opsional) Menetapkan jadwal yang menentukan waktu dan interval untuk mengambil salinan bayangan, seperti harian, mingguan, dan bulanan

Anda dapat menyimpan maksimal 500 salinan bayangan per sistem file kapan saja; Namun, kami sarankan untuk mempertahankan kurang dari 64 salinan bayangan setiap saat untuk memastikan ketersediaan dan kinerja. Ketika Anda mencapai batas ini, shadow copy berikutnya yang Anda ambil akan menggantikan shadow copy terlama. Demikian pula, ketika jumlah maksimum penyimpanan shadow copy tercapai, satu atau lebih shadow copy terlama dihapus untuk memberikan ruang penyimpanan yang cukup untuk shadow copy berikutnya.

Untuk informasi tentang cara mengaktifkan dan menjadwalkan salinan bayangan periodik dengan cepat menggunakan FSx setelan Amazon default, lihatMengkonfigurasi salinan bayangan untuk menggunakan penyimpanan dan jadwal default.

Pertimbangan untuk mengalokasikan penyimpanan shadow copy

Shadow copy adalah salinan level blok pada perubahan file yang dibuat sejak shadow copy terakhir. Seluruh file tidak disalin, hanya perubahannya. Oleh karena itu, file versi sebelumnya biasanya tidak memakan ruang penyimpanan sebanyak file saat ini. Jumlah ruang volume yang digunakan untuk menyimpan file yang diubah dapat bervariasi sesuai dengan beban kerja Anda. Ketika sebuah file diubah, ruang penyimpanan yang digunakan oleh shadow copy tergantung pada beban kerja Anda. Ketika Anda menentukan berapa banyak ruang penyimpanan untuk mengalokasikan shadow copy, Anda harus menyusun pola penggunaan sistem file menurut beban kerja Anda.

Bila Anda mengaktifkan shadow copy, Anda dapat menentukan jumlah maksimum penyimpanan yang dapat shadow copy konsumsi pada sistem file. Batas default adalah 10 persen dari sistem file Anda. Kami menyarankan agar Anda meningkatkan limit jika pengguna Anda sering menambahkan atau mengubah file. Menetapkan batas yang terlalu kecil dapat mengakibatkan shadow copy terdahulu lebih sering terhapus daripada yang diharapkan pengguna.

Anda dapat mengatur penyimpanan shadow copy sebagai tak terbatas (`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`). Namun, konfigurasi tak terbatas dapat mengakibatkan sejumlah besar shadow copy memakan penyimpanan sistem file Anda. Hal ini dapat membuat Anda tidak memiliki kapasitas penyimpanan yang cukup untuk beban kerja Anda. Jika Anda mengatur penyimpanan tak terbatas, pastikan untuk mengukur kapasitas penyimpanan Anda saat shadow copy mencapat batasnya. Untuk informasi tentang mengkonfigurasi penyimpanan shadow copy Anda ke ukuran

tertentu atau sebagai tidak terbatas, lihat Mengatur jumlah maksimum penyimpanan salinan bayangan.

Setelah Anda mengaktifkan shadow copy, Anda dapat memantau jumlah ruang penyimpanan yang dikonsumsi oleh shadow copy. Untuk informasi selengkapnya, lihat Melihat penyimpanan salinan bayangan.

Pertimbangan saat mengatur jumlah maksimum salinan bayangan

Saat Anda mengaktifkan salinan bayangan, Anda dapat menentukan jumlah maksimum salinan bayangan yang disimpan di sistem file. Batas default adalah 20, dan untuk meminimalkan ketersediaan dan dampak kinerja dari salinan bayangan, Microsoft merekomendasikan untuk mengonfigurasi jumlah maksimum salinan bayangan menjadi kurang dari 64. Karena Windows membutuhkan kinerja I/O tingkat tinggi untuk mempertahankan salinan bayangan, kami merekomendasikan penggunaan penyimpanan SSD dan meningkatkan kapasitas throughput hingga nilai setinggi tiga kali lipat dari beban kerja yang Anda harapkan. Ini membantu memastikan bahwa sistem file Anda memiliki sumber daya yang cukup untuk menghindari masalah seperti penghapusan salinan bayangan yang tidak diinginkan.

Anda dapat mengatur jumlah maksimum salinan bayangan hingga 500. Namun, jika Anda memiliki sejumlah besar salinan bayangan atau salinan bayangan yang menempati sejumlah besar penyimpanan (skala TB) pada satu sistem file, proses seperti failover dan failback mungkin memakan waktu lebih lama dari yang diharapkan. Ini karena Windows perlu menjalankan pemeriksaan konsistensi pada penyimpanan salinan bayangan. Anda mungkin juga mengalami latensi operasi I/O yang lebih tinggi karena kebutuhan Windows untuk melakukan copy-on-write aktivitas sambil mempertahankan salinan bayangan.

Rekomendasi sistem file untuk shadow copy

Berikut ini adalah rekomendasi sistem file untuk menggunakan shadow copy.

- Pastikan Anda menyediakan kapasitas kinerja yang memadai untuk memenuhi kebutuhan beban kerja Anda pada sistem file Anda. Amazon FSx memberikan fitur Shadow Copies seperti yang disediakan oleh Microsoft Windows Server. Secara desain, Microsoft Windows menggunakan copy-on-write metode untuk merekam perubahan sejak titik salinan bayangan terbaru, dan copy-on-write aktivitas ini dapat menghasilkan hingga tiga operasi I/O untuk setiap operasi penulisan file. Jika Windows tidak dapat mengikuti laju masuk operasi I/O per detik, itu dapat menyebabkan semua salinan bayangan dihapus karena tidak dapat lagi mempertahankan salinan bayangan melalui. copy-on-write Oleh karena itu, penting bagi Anda untuk mengadakan kapasitas kinerja I/

O yang cukup untuk memenuhi kebutuhan beban kerja Anda pada sistem file Anda (baik dimensi kapasitas throughput yang menentukan kinerja I/O server file, maupun jenis penyimpanan dan kapasitas yang menentukan kinerja penyimpanan I/O).

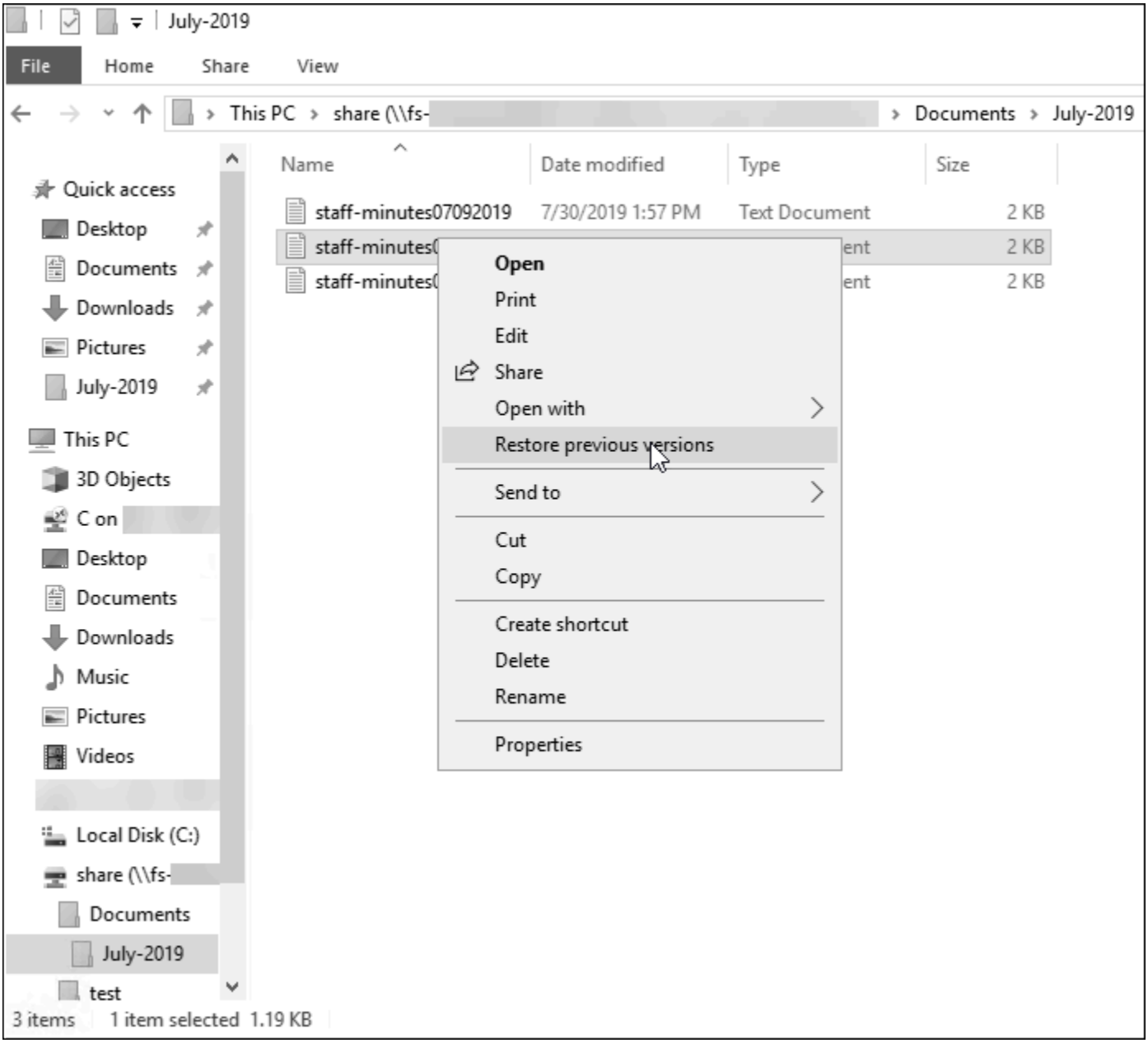
- Umumnya, kami lebih menyarankan agar Anda menggunakan sistem file yang terkonfigurasi dengan penyimpanan SSD daripada penyimpanan HDD ketika Anda mengaktifkan shadow copy, mengingat bahwa Windows membutuhkan kinerja I/O yang lebih tinggi untuk mempertahankan shadow copy, dan mengingat bahwa penyimpanan HDD menyediakan kapasitas kinerja yang lebih rendah untuk pengoperasian I/O.
- Sistem file Anda harus memiliki ruang kosong setidaknya sebesar 320 MB, selain jumlah penyimpanan shadow copy maksimum yang dikonfigurasi (`MaxSpace`). Misalnya, jika Anda mengalokasikan 5 GB `MaxSpace` untuk shadow copy, sistem file Anda harus selalu memiliki setidaknya 320 MB ruang bebas selain 5 GB `MaxSpace`.

> **Warning**
>
> Saat mengkonfigurasi jadwal shadow copy, pastikan Anda tidak menjadwalkan shadow copy saat melakukan migrasi data atau saat pekerjaan deduplikasi data dijadwalkan untuk berjalan. Sebaiknya Anda menjadwalkan shadow copy ketika Anda memperkirakan sistem file Anda menjadi siaga. Untuk informasi tentang cara mengatur konfigurasi jadwal khusus shadow copy Anda, lihat Membuat sebuah jadwal salinan bayangan kustom.

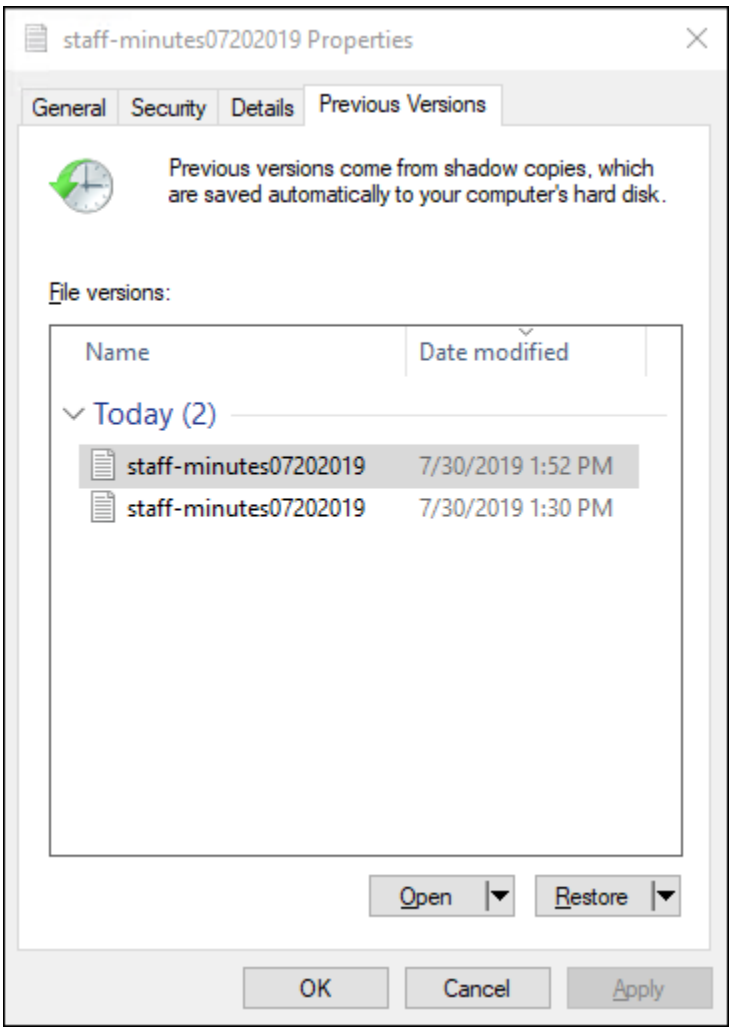
Memulihkan file dan folder terpisah

Setelah Anda mengonfigurasi salinan bayangan pada sistem FSx file Amazon Anda, pengguna Anda dapat dengan cepat memulihkan versi sebelumnya dari masing-masing file atau folder, dan memulihkan file yang dihapus.

Para pengguna memulihkan file ke versi sebelumnya menggunakan antarmuka Windows File Explorer yang familiar. Untuk memulihkan sebuah file, pilihlah file yang akan dipulihkan, lalu pilih dari menu konteks (klik kanan) Pulihkan versi sebelumnya.



Pengguna kemudian dapat melihat dan memulihkan ke versi sebelumnya dari daftar Versi sebelumnya.



Mengkonfigurasi salinan bayangan untuk menggunakan penyimpanan dan jadwal default

Anda dapat dengan cepat mengatur salinan bayangan pada sistem file Anda dengan menggunakan pengaturan dan jadwal penyimpanan salinan bayangan default. Pengaturan penyimpanan salinan bayangan default memungkinkan salinan bayangan mengkonsumsi maksimal 10 persen dari kapasitas penyimpanan sistem file Anda. Jika Anda meningkatkan kapasitas penyimpanan sistem file Anda, jumlah penyimpanan salinan bayangan yang saat ini dialokasikan tidak meningkat sama.

Jadwal default otomatis mengambil shadow copy setiap Senin, Selasa, Rabu, Kamis, dan Jumat, pukul 7:00 AM dan 12:00 PM UTC.

Untuk mengatur tingkat default penyimpanan salinan bayangan

1. Connect ke instans komputasi Windows yang memiliki konektivitas jaringan dengan sistem file Anda.
2. Log in ke instans komputasi Windows sebagai anggota grup administrator sistem file. Di AWS Managed Microsoft AD, grup itu adalah FSx Administrator AWS Delegasi. Di Microsoft AD swakelola Anda, grup tersebut adalah Admin Domain atau grup kustom yang Anda tentukan untuk administrasi ketika Anda membuat sistem file Anda. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
3. Aturlah jumlah default penyimpanan bayangan menggunakan perintah berikut. Ganti *FSxFileSystem-Remote-PowerShell-Endpoint* dengan PowerShell endpoint Windows Remote dari sistem file yang ingin Anda kelola. Anda dapat menemukan PowerShell endpoint Windows Remote di FSx konsol Amazon, di bagian Jaringan & Keamanan pada layar detail sistem file, atau dalam respons operasi `DescribeFileSystem` API.

   ```
   PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
   PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
   FsxShadowStorage -Default}
   ```

   Respon tersebut terlihat seperti berikut.

   ```
   FSx Shadow Storage Configuration

   AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
   -------------- ---------    -------- -------------------
                0         0 10737418240                  20
   ```

Untuk mengatur jadwal salinan bayangan default

1. Connect ke instans komputasi Windows yang memiliki konektivitas jaringan dengan sistem file Anda.
2. Log in ke instans komputasi Windows sebagai anggota grup administrator sistem file. Di AWS Managed Microsoft AD, grup itu adalah FSx Administrator AWS Delegasi. Di Microsoft AD swakelola Anda, grup tersebut adalah Admin Domain atau grup kustom yang Anda tentukan untuk administrasi ketika Anda membuat sistem file Anda. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
3. Atur jadwal salinan bayangan default dengan menggunakan perintah berikut.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowCopySchedule -Default}
```

Tanggapan tersebut menampilkan jadwal default yang sekarang ditetapkan.

```
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Untuk mempelajari tentang opsi tambahan dan membuat jadwal kustom shadow copy, lihat Membuat sebuah jadwal salinan bayangan kustom.

Mengatur jumlah maksimum penyimpanan salinan bayangan

Anda menentukan jumlah maksimum penyimpanan yang dapat dikonsumsi salinan bayangan pada sistem file menggunakan PowerShell perintah `Set-FsxShadowStorage` khusus. Anda dapat menentukan ukuran maksimum yang dapat ditumbuhkan oleh salinan bayangan dengan menggunakan parameter `-Maxsize` atau `-Default` parameter. Menggunakan `Default` set maksimum hingga 10% dari kapasitas penyimpanan sistem file. Anda tidak dapat menentukan `-Default` parameter `-Maxsize` dan dalam perintah yang sama.

Dengan menggunakan `-Maxsize`, Anda dapat menentukan penyimpanan salinan bayangan sebagai berikut:

- Dalam byte: `Set-FsxShadowStorage -Maxsize 2500000000`
- Dalam kilobyte, megabyte, gigabyte, atau unit lain: `Set-FsxShadowStorage -Maxsize (2500MB)` atau `Set-FsxShadowStorage -Maxsize (2.5GB)`
- Sebagai persentase dari penyimpanan keseluruhan: `Set-FsxShadowStorage -Maxsize "20%"`
- Sebagai tak terbatas: `Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

Gunakan `-Default` untuk mengatur penyimpanan bayangan untuk menggunakan hingga 10 persen dari sistem file: `Set-FsxShadowStorage -Default`. Untuk mempelajari lebih lanjut tentang penggunaan opsi default, lihat Mengkonfigurasi salinan bayangan untuk menggunakan penyimpanan dan jadwal default.

Untuk mengatur jumlah penyimpanan salinan bayangan pada sistem file FSx untuk Windows File Server

1. Connect ke instans komputasi yang memiliki konektivitas jaringan dengan sistem file Anda sebagai pengguna yang merupakan anggota dari grup administrator sistem file. Di AWS Managed Microsoft AD, grup itu adalah FSxAdministrator AWS Delegasi. Di Microsoft AD swakelola Anda, grup tersebut adalah Admin Domain atau grup kustom yang Anda tentukan untuk administrasi ketika Anda membuat sistem file Anda. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon.
2. Buka PowerShell jendela Windows pada instance komputasi.
3. Gunakan perintah berikut untuk membuka PowerShell sesi jarak jauh di sistem FSx file Amazon Anda. Ganti *`FSxFileSystem-Remote-PowerShell-Endpoint`* dengan PowerShell endpoint Windows Remote dari sistem file yang ingin Anda kelola. Anda dapat menemukan PowerShell endpoint Windows Remote di FSx konsol Amazon, di bagian Jaringan & Keamanan pada layar detail sistem file, atau dalam respons operasi `DescribeFileSystem` API.

   ```
   PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
   PowerShell-Endpoint -configurationname fsxremoteadmin
   ```

4. Verifikasi bahwa penyimpanan salinan bayangan tidak dikonfigurasi pada sistem file menggunakan perintah berikut.

   ```
   [fs-1234567890abcef12]: PS>Get-FsxShadowStorage
   No Fsx Shadow Storage Configured
   ```

5. Atur jumlah penyimpanan bayangan menjadi 10 persen dari volume dan jumlah maksimum shadow copes menjadi 20 menggunakan `-Default` opsi.

   ```
   [fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
   FSx Shadow Storage Configuration

   AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
   -------------- ---------    -------- -------------------
                0         0 32530536858                  20
   ```

Anda dapat membatasi jumlah maksimum salinan bayangan yang diizinkan pada sistem file Anda dengan menggunakan `Set-FSxShadowStorage` perintah dengan `-MaxShadowCopyNumber` parameter dan menentukan nilai dari 1-500. Secara default, jumlah maksimum salinan bayangan diatur ke 20, seperti yang direkomendasikan oleh Microsoft untuk beban kerja aktif.

Melihat penyimpanan salinan bayangan

Anda dapat melihat jumlah penyimpanan yang saat ini dikonsumsi oleh salinan bayangan pada sistem file Anda menggunakan `Get-FsxShadowStorage` perintah dalam PowerShell sesi jarak jauh pada sistem file Anda. Untuk petunjuk tentang meluncurkan PowerShell sesi jarak jauh pada sistem file Anda, lihatMenggunakan Amazon FSx CLI untuk PowerShell.

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

Outputnya menunjukkan konfigurasi penyimpanan bayangan, sebagai berikut:

- `AllocatedSpace`— Jumlah penyimpanan pada sistem file dalam byte yang saat ini dialokasikan untuk salinan bayangan. Awalnya, nilai ini adalah 0.
- `UsedSpace`— Jumlah penyimpanan, dalam byte, saat ini digunakan oleh salinan bayangan. Awalnya, nilai ini adalah 0.
- `MaxSpace`— Jumlah penyimpanan maksimum, dalam byte, tempat penyimpanan bayangan dapat tumbuh. Ini adalah nilai yang Anda tetapkan untuk penyimpanan penyalinan bayangan dengan menggunakan perintah `Set-FsxShadowStorage`.
- `MaxShadowCopyNumber`— Jumlah maksimum salinan bayangan yang dapat dimiliki sistem file, dari 1-500.

Ketika `UsedSpace` jumlah mencapai jumlah penyimpanan salinan bayangan maksimum yang dikonfigurasi (`MaxSpace`) atau jumlah salinan bayangan mencapai nomor salinan bayangan maksimum yang dikonfigurasi (`MaxShadowCopyNumber`), salinan bayangan berikutnya yang Anda ambil menggantikan salinan bayangan tertua. Jika Anda tidak ingin kehilangan salinan bayangan yang paling tua, pantau penyimpanan salinan bayangan Anda untuk memastikan bahwa Anda memiliki ruang penyimpanan yang cukup untuk salinan bayangan baru. Jika Anda membutuhkan

lebih banyak ruang, Anda dapat hapus salinan bayangan yang ada atau meningkatkan jumlah maksimum penyimpanan salinan bayangan.

> **Note**
>
> Ketika salinan bayangan dibuat secara otomatis atau manual, mereka menggunakan jumlah penyimpanan salinan bayangan yang Anda konfigurasikan sebagai batas penyimpanan. Salinan bayangan bertambah besar dari waktu ke waktu dan memanfaatkan ruang penyimpanan yang tersedia yang ditunjukkan oleh CloudWatch `FreeStorageCapacity` metrik hingga jumlah penyimpanan salinan bayangan maksimum yang dikonfigurasi (`MaxSpace`).

Membuat sebuah jadwal salinan bayangan kustom

Jadwal salinan bayangan menggunakan pemicu tugas terjadwal di Microsoft Windows untuk menentukan kapan salinan bayangan secara otomatis diambil. Jadwal salinan bayangan dapat memiliki beberapa pemicu, sehingga bisa memberi Anda banyak fleksibilitas penjadwalan. Hanya satu jadwal salinan bayangan saja yang dapat ada pada satu waktu. Sebelum Anda dapat membuat sebuah jadwal salinan bayangan, Anda harus terlebih dahulu menetapkan jumlah penyimpanan salinan bayangan.

Ketika Anda menjalankan perintah `Set-FsxShadowCopySchedule` pada sistem file, Anda menimpa setiap jadwal salinan bayangan yang ada. Jika komputer klien Anda berada di zona waktu UTC, Anda juga dapat menentukan zona waktu untuk pemicu menggunakan zona waktu Windows dan `-TimezoneId` opsi. Untuk daftar zona waktu Windows, lihat dokumentasi Zona Waktu Default Microsoft atau jalankan berikut ini pada command prompt Windows: `tzutil /l`. Untuk mempelajari lebih lanjut tentang pemicu tugas Windows, lihat Pemicu Tugas dalam dokumentasi Pusat Developer Windows.

Anda juga dapat menggunakan pilihan `-Default` untuk dengan cepat mengatur jadwal salinan bayangan default. Untuk mempelajari selengkapnya, lihat Mengkonfigurasi salinan bayangan untuk menggunakan penyimpanan dan jadwal default.

Untuk membuat jadwal salinan bayangan kustom

1. Membuat serangkaian pemicu tugas tugas terjadwal Windows untuk menentukan kapan salinan bayangan diambil dalam jadwal salinan bayangan. Gunakan `new-scheduledTaskTrigger` perintah PowerShell di mesin lokal Anda untuk mengatur beberapa pemicu.

Contoh berikut ini membuat sebuah jadwal salinan bayangan kustom yang mengambil salinan bayangan setiap Senin-Jumat, pukul 6:00 pagi dan pukul 6:00 sore UTC. Secara default, waktu menggunakan UTC, kecuali jika Anda menentukan zona waktu dalam pemicu tugas terjadwal Windows yang Anda buat.

```
PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
```

2. Gunakan `invoke-command` untuk menjalankan perintah `scriptblock`. Dengan demikian maka hal itu menulis skrip yang menetapkan jadwal salinan bayangan dengan nilai `new-scheduledTaskTrigger` yang baru saja Anda buat. Ganti *`FSxFileSystem-Remote-PowerShell-Endpoint`* dengan PowerShell endpoint Windows Remote dari sistem file yang ingin Anda kelola. Anda dapat menemukan PowerShell endpoint Windows Remote di FSx konsol Amazon, di bagian Jaringan & Keamanan pada layar detail sistem file, atau dalam respons operasi `DescribeFileSystem` API.

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. Masukkan baris berikut di prompt >> untuk mengatur jadwal salinan bayangan Anda menggunakan perintah `set-fsxshadowcopyschedule`.

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

Respons menampilkan jadwal salinan bayangan yang telah Anda konfigurasi pada sistem file.

```
FSx Shadow Copy Schedule


Start Time:    : 2019-07-16T06:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcde1
```

```
Start Time:    : 2019-07-16T18:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcdef
```

Melihat jadwal salinan bayangan

Untuk melihat jadwal salinan bayangan yang ada di sistem file Anda, masukkan perintah berikut dalam PowerShell sesi jarak jauh di sistem file Anda. Untuk petunjuk tentang meluncurkan PowerShell sesi jarak jauh pada sistem file Anda, lihatMenggunakan Amazon FSx CLI untuk PowerShell.

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Membuat sebuah salinan bayangan

Untuk membuat salinan bayangan secara manual, masukkan perintah berikut dalam PowerShell sesi jarak jauh di sistem file Anda. Untuk petunjuk tentang meluncurkan PowerShell sesi jarak jauh pada sistem file Anda, lihatMenggunakan Amazon FSx CLI untuk PowerShell.

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

Melihat salinan bayangan yang ada

Untuk melihat kumpulan salinan bayangan yang ada di sistem file Anda, masukkan perintah berikut dalam PowerShell sesi jarak jauh di sistem file Anda. Untuk petunjuk tentang meluncurkan PowerShell sesi jarak jauh pada sistem file Anda, lihatMenggunakan Amazon FSx CLI untuk PowerShell.

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
```

```
FSx Shadow Copies: 2 total

Shadow Copy ID                          Creation Time
--------------                          -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

Menghapus salinan bayangan

Anda dapat menghapus satu atau lebih salinan bayangan yang ada di sistem file Anda menggunakan `Remove-FsxShadowCopies` perintah dalam PowerShell sesi jarak jauh pada sistem file Anda. Untuk petunjuk tentang meluncurkan PowerShell sesi jarak jauh pada sistem file Anda, lihatMenggunakan Amazon FSx CLI untuk PowerShell.

Menentukan salinan bayangan yang akan dihapus dengan menggunakan salah satu opsi yang diperlukan berikut:

- `-Oldest` menghapus salinan bayangan paling tua
- `-All` menghapus semua salinan bayangan yang ada
- `-ShadowCopyId` menghapus salinan bayangan tertentu berdasarkan ID.

Anda hanya dapat menggunakan satu opsi dengan perintah tersebut. Terjadi kesalahan jika Anda tidak menentukan salinan bayangan mana yang akan dihapus, jika Anda menentukan beberapa salinan bayangan IDs, atau jika Anda menentukan ID salinan bayangan yang tidak valid.

Untuk menghapus salinan bayangan tertua di sistem file Anda, masukkan perintah berikut dalam PowerShell sesi jarak jauh di sistem file Anda.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

Untuk menghapus salinan bayangan tertentu pada sistem file Anda, masukkan perintah berikut dalam PowerShell sesi jarak jauh pada sistem file Anda.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

Untuk menghapus sejumlah salinan bayangan tertua di sistem file Anda, perbarui `-MaxShadowCopyNumber` parameter Anda ke jumlah salinan bayangan yang diinginkan yang ingin Anda sisakan. Namun, perubahan ini hanya akan berlaku setelah snapshot salinan bayangan berikutnya diambil, ketika sistem akan secara otomatis menghapus salinan bayangan berlebih. Gunakan perintah berikut dalam PowerShell sesi jarak jauh pada sistem file Anda.

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50

[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

Menghapus sebuah jadwal salinan bayangan

Untuk menghapus jadwal salinan bayangan yang ada di sistem file Anda, masukkan perintah berikut dalam PowerShell sesi jarak jauh di sistem file Anda. Untuk petunjuk tentang meluncurkan

PowerShell sesi jarak jauh pada sistem file Anda, lihatMenggunakan Amazon FSx CLI untuk PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

Menghapus penyimpanan salinan bayangan, jadwal, dan semua salinan bayangan

Anda dapat menghapus konfigurasi salinan bayangan Anda, termasuk semua salinan bayangan yang ada dan jadwal salinan bayangan. Pada saat yang sama, Anda juga dapat melepaskan penyimpanan salinan bayangan pada sistem file.

Untuk melakukan ini, masukkan `Remove-FsxShadowStorage` perintah dalam PowerShell sesi jarak jauh pada sistem file Anda. Untuk petunjuk tentang meluncurkan PowerShell sesi jarak jauh pada sistem file Anda, lihatMenggunakan Amazon FSx CLI untuk PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

Penyelesaian masalah shadow copy

Ada sejumlah potensi penyebab ketika shadow copy hilang atau tidak dapat diakses, seperti yang dijelaskan di bagian berikut.

Topik

Salinan bayangan tertua hilang

Salinan bayangan tertua dihapus dalam salah satu keadaan berikut:

- Jika Anda memiliki 500 shadow copy, shadow copy berikutnya menggantikan shadow copy tertua, terlepas dari ruang volume penyimpanan yang dialokasikan tersisa untuk shadow copy.
- Jika jumlah penyimpanan shadow copy maksimum yang dikonfigurasi tercapai, shadow copy berikutnya menggantikan satu atau lebih shadow copy tertua, bahkan jika Anda memiliki kurang dari 500 shadow copy.

Kedua hasil adalah perilaku yang diharapkan. Jika Anda memiliki cukup penyimpanan yang dialokasikan untuk shadow copy, pertimbangkan untuk meningkatkan penyimpanan yang telah dialokasikan.

Semua shadow copy saya hilang

Memiliki kapasitas kinerja I/O yang tidak mencukupi pada sistem file Anda (misalnya, karena Anda menggunakan penyimpanan HDD, karena penyimpanan HDD telah kehabisan kapasitas burst, atau karena kapasitas throughput tidak mencukupi) dapat menyebabkan semua salinan bayangan dihapus oleh Windows Server karena tidak dapat mempertahankan salinan bayangan dengan kapasitas kinerja I/O yang tersedia. Pertimbangkan rekomendasi berikut untuk membantu mencegah masalah ini:

- Jika Anda menggunakan penyimpanan HDD, gunakan FSx konsol Amazon atau Amazon FSx API untuk beralih menggunakan penyimpanan SSD. Untuk informasi selengkapnya, lihat Mengelola jenis penyimpanan sistem file Anda.
- Meningkatkan kapasitas throughput sistem file ke nilai tiga kali beban kerja yang diharapkan.
- Pastikan bahwa sistem file Anda memiliki setidaknya 320 MB ruang kosong, selain jumlah penyimpanan shadow copy maksimum yang dikonfigurasi.
- Jadwalkan shadow copy ketika Anda mengharapkan sistem file Anda menjadi siaga.

Untuk informasi selengkapnya, lihat Rekomendasi sistem file untuk shadow copy.

Tidak dapat membuat FSx cadangan Amazon atau mengakses salinan bayangan pada sistem file yang baru saja dipulihkan atau diperbarui

Ini adalah perilaku yang diharapkan. Amazon FSx membangun kembali status salinan bayangan pada sistem file yang baru saja dipulihkan dan tidak mengizinkan akses ke salinan bayangan atau cadangan saat pembangunan kembali masih berlangsung.

Replikasi terjadwal menggunakan AWS DataSync

Anda dapat menggunakan AWS DataSync untuk menjadwalkan replikasi berkala FSx untuk sistem file Windows File Server Anda ke sistem file kedua. Kemampuan ini tersedia untuk penyebaran dalam wilayah dan lintas wilayah. Untuk mempelajari lebih lanjut, lihat Memigrasi file yang ada ke FSx Windows File Server menggunakan AWS DataSync di panduan ini dan Transfer data antar layanan AWS penyimpanan di Panduan AWS DataSync Pengguna.

Menggunakan FSx untuk Windows File Server dengan Microsoft SQL Server

Microsoft SQL Server Ketersediaan Tinggi (HA) biasanya di-deploy di beberapa simpul database di Windows Server Failover Cluster (WSFC), dengan setiap simpul memiliki akses ke penyimpanan file bersama. Anda dapat menggunakan FSx Windows File Server sebagai penyimpanan bersama untuk penyebaran Microsoft SQL Server Ketersediaan Tinggi (HA) dengan dua cara: sebagai penyimpanan untuk file data aktif dan sebagai saksi berbagi file SMB.

> **Note**
>
> Saat ini, Amazon FSx tidak mendukung fitur Microsoft SQL Server IFI (Instant File Initialization).

Penyimpanan SSD direkomendasikan untuk SQL Server. Penyimpanan SSD dirancang untuk beban kerja dengan kinerja tertinggi dan paling sensitif terhadap latensi, termasuk database.

Untuk informasi tentang penggunaan Amazon FSx untuk mengurangi kompleksitas dan biaya untuk penerapan ketersediaan tinggi SQL Server Anda, lihat posting berikut di Blog Penyimpanan:AWS

- Sederhanakan penerapan ketersediaan tinggi Microsoft SQL Server Anda menggunakan FSx Amazon untuk Windows File Server
- Mengoptimalkan biaya untuk penerapan SQL Server dengan ketersediaan tinggi Anda AWS
- Sederhanakan penerapan SQL Server Selalu Aktif dengan Launch Wizard AWS dan Amazon FSx

Menggunakan Amazon FSx untuk File Data SQL Server Aktif

Microsoft SQL Server dapat di-deploy dengan berbagi berkas SMB sebagai opsi penyimpanan untuk file data aktif. Amazon FSx dioptimalkan untuk menyediakan penyimpanan bersama untuk database SQL Server dengan mendukung berbagi file yang tersedia terus menerus (CA). Berbagi file ini dirancang untuk aplikasi seperti SQL Server yang memerlukan akses tanpa gangguan ke data file bersama. Ketika Anda dapat membuat berbagi CA pada sistem file Single-AZ 2, Anda diharuskan menggunakan berbagi CA pada sistem file Multi-AZ untuk semua deployment SQL Server, baik HA atau tidak.

Membuat Pembagian yang Tersedia Secara Terus-Menerus

Anda dapat membuat saham CA menggunakan Amazon FSx CLI untuk Manajemen Jarak Jauh di. PowerShell Untuk menentukan bahwa pembagian tersebut adalah pembagian yang tersedia secara terus-menerus, gunakan `New-FSxSmbShare` dengan opsi `-ContinuouslyAvailable` yang diatur ke `$True`. Untuk informasi selengkapnya, lihat Untuk membuat share yang terus tersedia (CA).

Konfigurasikan pengaturan batas waktu SMB

Seperti dijelaskan dalamGagal dalam proses, failover dan failback untuk Multi-AZ dapat mengakibatkan jeda I/O yang biasanya selesai dalam waktu kurang dari 30 detik. Aplikasi SQL Server Anda mungkin memiliki sensitivitas yang berbeda terhadap pengaturan batas waktu tergantung pada bagaimana itu dikonfigurasi.

Anda dapat menyetel batas waktu sesi konfigurasi klien SMB untuk memastikan aplikasi Anda tahan terhadap failover sistem file multi-AZ. Anda dapat menguji perilaku aplikasi Anda selama failover dengan memperbarui kapasitas throughput sistem file Anda, yang memulai failover dan failback otomatis.

Menggunakan Amazon FSx sebagai Saksi Berbagi File SMB

Deployment kluster Windows Server Failover biasanya men-deploy saksi pembagian file SMB untuk mempertahankan kuorum sumber daya kluster. Saksi pembagian file hanya memerlukan sejumlah kecil penyimpanan untuk informasi kuorum. Sistem FSx file Amazon dapat digunakan sebagai saksi berbagi file SMB untuk penerapan Windows Server Failover Cluster.

Migrasi penyimpanan file yang ada ke Amazon FSx

Amazon FSx untuk Windows File Server memiliki fitur, kinerja, dan kompatibilitas untuk membantu Anda dengan mudah mengangkat dan mengalihkan aplikasi perusahaan ke Amazon Web Services Cloud. Proses untuk memigrasi penyimpanan Microsoft Windows File Server lokal ke FSx Windows File Server memiliki empat langkah utama berikut:

1. Migrasikan file Anda ke FSx Windows File Server. Untuk informasi selengkapnya, lihat Migrasi penyimpanan file yang ada ke FSx Windows File Server.
2. Migrasikan konfigurasi berbagi file Anda ke FSx Windows File Server. Untuk informasi selengkapnya, lihat Memigrasi konfigurasi berbagi file lokal ke Amazon FSx.
3. Kaitkan nama DNS Anda yang ada sebagai alias DNS untuk sistem file Amazon FSx Anda. Untuk informasi selengkapnya, lihat Mengaitkan alias DNS dengan Amazon. FSx
4. Potong FSx untuk Windows File Server. Untuk informasi selengkapnya, lihat Memotong operasi ke Amazon FSx untuk Windows File Server.

Anda dapat menemukan detail untuk setiap langkah dalam proses di bagian berikut.

Topik

- Migrasi penyimpanan file yang ada ke FSx Windows File Server
- Memigrasi konfigurasi berbagi file lokal ke Amazon FSx
- Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server
- Memotong operasi ke Amazon FSx untuk Windows File Server

Migrasi penyimpanan file yang ada ke FSx Windows File Server

Untuk memigrasikan file yang ada ke FSx sistem file Windows File Server, sebaiknya gunakan AWS DataSync, layanan transfer data online yang dirancang untuk menyederhanakan, mengotomatisasi, dan mempercepat penyalinan data dalam jumlah besar ke dan dari layanan penyimpanan. AWS DataSync menyalin data melalui internet atau AWS Direct Connect. Sebagai layanan yang dikelola sepenuhnya, DataSync menghilangkan banyak kebutuhan untuk memodifikasi aplikasi, mengembangkan skrip, atau mengelola infrastruktur. Untuk informasi selengkapnya, lihat Memigrasi file yang ada ke FSx Windows File Server menggunakan AWS DataSync.

Sebagai solusi alternatif, Anda dapat menggunakan Salinan Robust FIle, atau Robocopy, yang merupakan direktori baris perintah dan kumpulan perintah replikasi file untuk Microsoft Windows. Untuk prosedur terperinci tentang cara menggunakan Robocopy untuk memigrasi penyimpanan file ke FSx Windows File Server, lihat. Memigrasi file yang ada ke FSx Windows File Server menggunakan Robocopy

Praktik terbaik untuk memigrasi penyimpanan file yang ada ke FSx Windows File Server

Untuk memigrasikan sejumlah besar data ke FSx Windows File Server secepat mungkin, gunakan sistem FSx file Amazon yang dikonfigurasi dengan penyimpanan solid state drive (SSD). Setelah migrasi selesai, Anda dapat memindahkan data ke sistem FSx file Amazon menggunakan penyimpanan hard disk drive (HDD) jika itu adalah solusi terbaik untuk aplikasi Anda.

Untuk memindahkan data dari sistem FSx file Amazon menggunakan penyimpanan SSD ke penyimpanan HDD, Anda dapat mengambil langkah-langkah berikut. (Perhatikan bahwa sistem file HDD memiliki kapasitas penyimpanan minimum 2TB, dan Anda tidak dapat mengubah kapasitas penyimpanan saat memulihkan dari cadangan.)

1. Ambil cadangan sistem file SSD Anda. Untuk informasi selengkapnya, lihat Membuat backup yang diinisiasi pengguna.
2. Pulihkan cadangan ke sistem file menggunakan penyimpanan HDD. Untuk informasi selengkapnya, lihat Memulihkan backup ke sistem file baru.

Memigrasi file yang ada ke FSx Windows File Server menggunakan AWS DataSync

Kami merekomendasikan penggunaan AWS DataSync untuk mentransfer data antara FSx untuk sistem file Windows File Server. DataSync adalah layanan transfer data yang menyederhanakan, mengotomatisasi, dan mempercepat pemindahan dan replikasi data antara sistem penyimpanan lokal dan layanan AWS penyimpanan lainnya melalui internet atau. AWS Direct Connect DataSync dapat mentransfer data dan metadata sistem file Anda, seperti kepemilikan, stempel waktu, dan izin akses.

DataSync mendukung penyalinan daftar kontrol akses NTFS (ACLs), dan juga mendukung penyalinan informasi kontrol audit file, juga dikenal sebagai daftar kontrol akses sistem NTFS (SACLs), yang digunakan oleh administrator untuk mengontrol pencatatan audit upaya pengguna untuk mengakses file.

Anda dapat menggunakan DataSync untuk mentransfer file antara dua FSx untuk sistem file Windows File Server, dan juga memindahkan data ke sistem file di AWS akun yang berbeda Wilayah AWS atau. Anda dapat menggunakan DataSync dengan FSx untuk sistem file Windows File Server untuk tugas-tugas lain. Misalnya, Anda dapat melakukan migrasi data satu kali, secara berkala menyerap data untuk beban kerja yang terdistribusi, dan menjadwalkan replikasi untuk perlindungan dan pemulihan data.

Di AWS DataSync, lokasi FSx untuk Windows File Server adalah titik akhir FSx untuk Windows File Server. Anda dapat mentransfer file antara lokasi FSx untuk Windows File Server dan lokasi untuk sistem file lainnya. Untuk informasi lebih lanjut, lihat Bekerja dengan Lokasi dalam Panduan Pengguna AWS DataSync .

DataSync mengakses Server File FSx Windows Anda menggunakan protokol Server Message Block (SMB). Ini mengotentikasi dengan nama pengguna dan kata sandi yang Anda konfigurasikan di AWS DataSync konsol atau AWS CLI.

Prasyarat

Untuk memigrasikan data ke penyiapan Amazon FSx untuk Windows File Server, Anda memerlukan server dan jaringan yang memenuhi DataSync persyaratan. Untuk mempelajari lebih lanjut, lihat Persyaratan untuk DataSync di Panduan AWS DataSync Pengguna.

Jika Anda melakukan migrasi data besar, atau migrasi yang melibatkan banyak file kecil, sebaiknya gunakan Sistem FSx File Amazon dengan tipe penyimpanan SSD. Ini karena DataSync tugas melibatkan pemindaian metadata file yang dapat menghabiskan batas IOPS disk dari sistem file HDD, yang mengarah ke migrasi yang berjalan lama dan dampak kinerja sistem file. Untuk informasi lebih lanjut, lihat:Praktik terbaik untuk memigrasi penyimpanan file yang ada ke FSx Windows File Server.

Jika dataset Anda terdiri dari sebagian besar file kecil, dengan jumlah file dalam jutaan, atau jika Anda memiliki lebih banyak bandwidth jaringan yang tersedia daripada satu DataSync tugas yang dapat dikonsumsi, Anda juga dapat mempercepat transfer data Anda dengan skala arsitektur. Untuk informasi selengkapnya, lihat: Cara mempercepat transfer data Anda dengan AWS DataSync skala arsitektur.

Anda dapat memantau pemanfaatan disk I/O dari sistem file Anda menggunakan metrik FSx kinerja.

Langkah-langkah dasar untuk memigrasi file menggunakan DataSync

Untuk mentransfer file dari lokasi sumber ke lokasi tujuan menggunakan DataSync, lakukan langkah-langkah dasar berikut:

- Unduh dan deploy agen di lingkungan Anda dan aktifkan.
- Buat dan konfigurasi sumber dan lokasi tujuan.
- Buat dan konfigurasi tugas.
- Jalankan tugas untuk mentransfer file dari sumber ke tujuan.

Untuk mempelajari cara mentransfer file dari sistem file lokal yang ada ke Server File Windows, lihat Transfer data antara penyimpanan yang dikelola sendiri dan AWS, Membuat lokasi untuk SMB, dan Membuat lokasi untuk Amazon FSx untuk Windows File Server di Panduan Pengguna. FSx AWS DataSync

Untuk mempelajari cara mentransfer file dari sistem file in-cloud yang ada ke Server File Windows Anda FSx , lihat Menerapkan agen Anda sebagai EC2 instans Amazon di AWS DataSync Panduan Pengguna.

Migrasi antara dua sistem FSx file Amazon

Anda dapat menggunakan DataSync untuk memigrasikan data antara dua sistem FSx file Amazon. Ini dapat membantu jika Anda perlu memindahkan beban kerja Anda dari sistem file yang ada ke sistem file baru dengan konfigurasi yang berbeda, seperti dari Single-AZ ke konfigurasi multi-AZ. Anda juga dapat menggunakan DataSync untuk membagi beban kerja Anda antara dua sistem file.

Berikut adalah contoh ikhtisar proses migrasi:

1. Buat DataSync lokasi untuk sistem file sumber dan tujuan. Perhatikan bahwa sumber dan tujuan harus milik domain Active Directory (AD) yang sama, atau memiliki hubungan kepercayaan AD di antara domain mereka.
2. Buat dan konfigurasikan DataSync tugas untuk mentransfer data dari sumber ke tujuan. Anda dapat menjalankan tugas sebagai contoh satu kali, atau mengatur tugas untuk berjalan secara otomatis pada jadwal yang Anda konfigurasi.
3. Setelah tugas selesai dengan sukses, data dalam sistem file tujuan Anda adalah salinan persis dari sumber Anda. Perhatikan bahwa Anda perlu menghentikan sementara aktivitas tulis atau pembaruan file apa pun pada sistem file sumber Anda untuk menyelesaikan tugas. Anda kemudian dapat memotong ke sistem file tujuan Anda dan menghapus sistem file sumber.

Sebelum bermigrasi dari sistem file produksi, Anda dapat menguji proses migrasi pada sistem file yang dipulihkan dari cadangan terbaru. Hal ini memungkinkan Anda untuk memperkirakan berapa lama proses transfer data berlangsung, dan untuk memecahkan masalah DataSync kesalahan di muka.

Untuk meminimalkan waktu cutover Anda, Anda dapat menjalankan DataSync tugas terlebih dahulu, memindahkan sebagian besar data Anda dari sistem file sumber Anda ke sistem file tujuan Anda. Setelah menghentikan lalu lintas ke sistem file sumber Anda, Anda dapat menjalankan satu transfer tugas akhir untuk menyinkronkan data apa pun yang baru diperbarui sejak Anda menghentikan lalu lintas, dan kemudian memotong ke sistem file tujuan Anda.

Anda dapat mengonfigurasi DataSync tugas agar hanya berjalan di direktori tertentu, atau untuk menyertakan atau mengecualikan jalur tertentu. Ini dapat berguna jika Anda menjalankan beberapa tugas secara paralel, atau jika Anda ingin memigrasikan subset data Anda.

Anda dapat membuat alias DNS pada sistem file tujuan Anda yang sama dengan nama DNS dari sistem file sumber Anda. Ini memungkinkan pengguna akhir dan aplikasi Anda untuk terus mengakses data file menggunakan nama DNS dari sistem file sumber Anda. Untuk informasi selengkapnya tentang cara mengatur alias DNS, lihat:. Mengakses data menggunakan alias DNS

Saat melakukan jenis migrasi ini, kami merekomendasikan hal berikut:

- Jadwalkan migrasi Anda untuk menghindari pencadangan sistem file, jendela pemeliharaan mingguan Anda, dan `Data Deduplication` pekerjaan. Secara khusus, kami sarankan untuk menonaktifkan `Data Deduplication GarbageCollection` pekerjaan jika bertepatan dengan migrasi yang Anda rencanakan.
- Gunakan jenis penyimpanan SSD untuk sistem file sumber dan tujuan Anda. Anda dapat beralih antara jenis penyimpanan HDD dan SSD dengan memulihkan dari cadangan. Untuk informasi lebih lanjut lihat:Migrasi penyimpanan file yang ada ke FSx Windows File Server.
- Konfigurasikan sistem file sumber dan tujuan Anda dengan kapasitas throughput yang cukup untuk jumlah data yang perlu Anda transfer. Selama proses DataSync tugas, pantau pemanfaatan kinerja sistem file sumber dan tujuan. Untuk informasi lebih lanjut, lihat:Pemantauan CloudWatch dengan Amazon.
- Siapkan DataSync pemantauan untuk membantu Anda memahami kemajuan tugas yang sedang berlangsung. Anda juga dapat mengirim DataSync log ke grup Amazon CloudWatch Logs untuk membantu Anda men-debug tugas jika mengalami kesalahan.

Memigrasi file yang ada ke FSx Windows File Server menggunakan Robocopy

Dibangun di Microsoft Windows Server, Amazon FSx untuk Windows File Server memungkinkan Anda untuk memigrasikan kumpulan data yang ada sepenuhnya ke sistem file Amazon FSx Anda. Anda dapat memigrasikan data untuk setiap file. Anda juga dapat memigrasikan semua metadata file yang relevan termasuk atribut, stempel waktu, daftar kontrol akses (ACLs), informasi pemilik, dan informasi audit. Dengan dukungan migrasi total ini, Amazon FSx memungkinkan pemindahan beban kerja dan aplikasi berbasis Windows Anda dengan mengandalkan kumpulan data file ini ke Amazon Web Services Cloud.

Gunakan topik berikut sebagai panduan untuk melalui proses untuk menyalin data file yang ada. Saat Anda melakukan salinan ini, Anda menyimpan semua metadata file dari pusat data lokal atau dari server file yang dikelola sendiri di Amazon. EC2

Prasyarat untuk migrasi file dengan Robocopy

Sebelum memulai, pastikan Anda melakukan hal berikut:

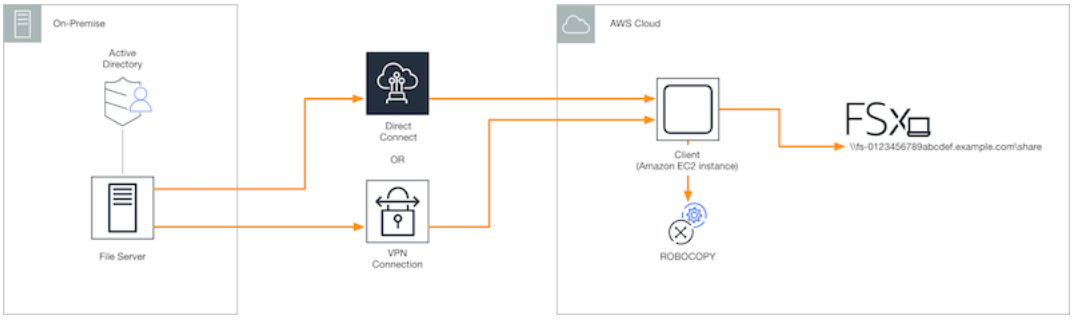
- Buat konektivitas jaringan (dengan menggunakan AWS Direct Connect atau VPN) antara Active Directory lokal dan VPC tempat Anda ingin membuat sistem file FSx Amazon.
- Buat akun layanan pada Direktori Aktif Anda dengan izin delegasi untuk menggabungkan komputer ke domain. Untuk informasi selengkapnya, lihat Mendelegasikan Keistimewaan ke Akun Layanan Anda di Panduan administrasi AWS Directory Service .
- Buat sistem FSx file Amazon, bergabung dengan direktori Microsoft AD yang dikelola sendiri (lokal).
- Perhatikan lokasi (misalnya,`\\Source\Share`) dari berbagi file (baik lokal maupun di AWS) yang berisi file yang ada yang ingin Anda transfer ke Amazon FSx.
- Perhatikan lokasi (misalnya,`\\Target\Share`) berbagi file di sistem FSx file Amazon yang ingin Anda transfer melalui file yang ada.

Tabel berikut merangkum persyaratan aksesibilitas sistem file sumber dan tujuan untuk tiga model akses pengguna migrasi.

Model akses pengguna migrasi	Persyaratan aksesibilitas sistem file sumber	Persyaratan aksesibilitas server FSx file tujuan
Model izin baca/tulis langsung	Pengguna harus memiliki setidaknya izin baca (NTFS ACLs) pada file dan folder yang dimigrasi.	Pengguna harus memiliki setidaknya izin tulis (NTFS ACLs) pada file dan folder yang dimigrasi.
Model keistimewaan backup/pulihkan untuk mengganti izin akses	Pengguna harus menjadi anggota grup Operator Cadangan Direktori Aktif lokal, dan menggunakan flag /b dengan. RoboCopy	Pengguna harus menjadi anggota grup administrator sistem FSx file Amazon*, dan menggunakan flag / b dengan. RoboCopy
Model hak istimewa (penuh) administrator domain untuk mengganti izin akses	Pengguna harus menjadi anggota grup Admin Domain dari Direktori Aktif on-premise.	Pengguna harus menjadi anggota grup administrator sistem FSx file Amazon*, dan menggunakan flag / b dengan RoboCopy

Note

* Untuk sistem file yang bergabung dengan Microsoft AD yang AWS Dikelola, grup administrator sistem FSx file Amazon adalah Administrator AWS Delegasi FSx . Di Microsoft AD yang dikelola sendiri, grup administrator sistem FSx file Amazon adalah Admin Domain atau grup kustom yang Anda tentukan untuk administrasi saat Anda membuat sistem file.



Migrasi file menggunakan Robocopy

Anda dapat memigrasikan file yang ada dari sistem file lokal ke FSx sistem file Windows File Server dengan menggunakan prosedur berikut.

Untuk memigrasi file yang ada ke Amazon FSx menggunakan Robocopy

1. Luncurkan EC2 instance Amazon Windows Server 2016 di VPC Amazon yang sama dengan sistem FSx file Amazon Anda.
2. Connect ke EC2 instans Amazon Anda. Untuk informasi selengkapnya, lihat Menghubungkan ke Instans Windows Anda di Panduan EC2 Pengguna Amazon untuk Instans Windows.
3. Buka Command Prompt dan petakan berbagi file sumber di server file yang ada (lokal atau di AWS) ke huruf drive (misalnya,*Y*:) sebagai berikut. Sebagai bagian dari hal ini, Anda sediakan kredensial untuk anggota dari grup Administrator domain dari Direktori Aktif On-Premise Anda.

   ```
   C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
   Enter the password for 'fileserver1.mydata.com': _

   Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

   The command completed successfully.
   ```

4. Petakan berbagi file target di sistem FSx file Amazon Anda ke huruf drive yang berbeda (misalnya,*Z*:) pada EC2 instance Amazon Anda sebagai berikut. Sebagai bagian dari ini, Anda memberikan kredensyal untuk akun pengguna yang merupakan anggota grup administrator domain Active Directory lokal dan grup administrator sistem FSx file Amazon Anda. Untuk sistem file yang bergabung dengan Microsoft AD yang AWS Dikelola, grup itu adalah **`AWS Delegated FSx Administrators`**. Di Microsoft AD yang dikelola sendiri, grup tersebut adalah **`Domain Admins`** atau grup kustom yang Anda tentukan untuk administrasi ketika Anda membuat sistem file Anda.

   Untuk informasi selengkapnya, lihat tabel persyaratan aksesibilitas sistem file sumber dan tujuan di Prasyarat untuk migrasi file dengan Robocopy.

   ```
   C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
   Enter the password for 'amznfsxabcdef1.mydata.com': _

   Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

   The command completed successfully.
   ```

5. Pilih Jalankan sebagai Administrator dari menu konteks. Buka Command Prompt atau Windows PowerShell sebagai administrator, dan jalankan perintah Robocopy berikut untuk menyalin file dari share sumber ke target share.

   Perintah ROBOCOPY adalah utilitas transfer file fleksibel dengan beberapa pilihan untuk mengontrol proses transfer data. Karena proses ROBOCOPY perintah ini, semua file dan direktori dari share sumber disalin ke pangsa FSx target Amazon. Salinan menyimpan file dan folder NTFS ACLs, atribut, stempel waktu, informasi pemilik, dan informasi audit.

   ```
   robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
   ```

   Contoh perintah sebelumnya menggunakan elemen dan opsi berikut:

   - Y — Mengacu pada Berbagi sumber yang terletak di mydata.com forest Direktori Aktif on-premise.
   - Z - Mengacu pada target share\\ amznfsxabcdef1.mydata.com\ share di Amazon. FSx
   - /copy — Tentukan properti file berikut untuk disalin:
     - D — data
     - A — atribut
     - T — timestamp
     - S - NTFS ACLs
     - O — informasi pemilik
     - U — mengaudit informasi.
   - /secfix — Memperbaiki keamanan file pada semua file, bahkan yang terlewat.
   - /e — Menyalin subdirektori, termasuk yang kosong.
   - /b — Menggunakan hak cadangan dan pemulihan di Windows untuk menyalin file bahkan jika NTFS mereka ACLs menolak izin untuk pengguna saat ini.
   - /MT:8 — Tentukan seberapa banyak benang yang digunakan untuk melakukan salinan multithreaded.

> **Note**
>
> Jika Anda menyalin file-file besar melalui koneksi yang lambat atau tidak dapat diandalkan, Anda dapat mengaktifkan mode yang dapat me-restart dengan menggunakan opsi /zb dengan robocopy untuk menggantikan opsi /b. Dengan mode yang dapat di-restart, jika transfer file besar terganggu, operasi Robocopy berikutnya dapat langsung lanjut dari pertengahan transfer dan tidak harus menyalin ulang seluruh file dari awal. Mengaktifkan mode yang dapat di-restart dapat mengurangi kecepatan transfer data.

Memigrasi konfigurasi berbagi file lokal ke Amazon FSx

Anda dapat memigrasi konfigurasi berbagi file yang ada ke Amazon FSx dengan menggunakan prosedur berikut. Dalam prosedur ini, server file sumber adalah server file yang konfigurasi berbagi file yang ingin Anda migrasikan ke Amazon FSx.

> **Note**
>
> Pertama memigrasikan file Anda ke Amazon FSx sebelum memigrasikan konfigurasi berbagi file Anda. Untuk informasi selengkapnya, lihat Migrasi penyimpanan file yang ada ke FSx Windows File Server.

Untuk memigrasi berbagi file yang ada ke FSx Windows File Server

1. Pada server file sumber, pilih Jalankan sebagai Administrator dari menu konteks. Buka Windows PowerShell sebagai administrator.
2. Ekspor berbagi file server file sumber ke file bernama `SmbShares.xml` dengan menjalankan perintah berikut di file PowerShell. Ganti F: dalam contoh ini dengan drive letter pada server file Anda tempat Anda mengekspor Berbagi file.

   ```
   $shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
   $shareFolder | Export-Clixml -Path F:\SmbShares.xml
   ```

3. Edit `SmbShares.xml` file, ganti semua referensi ke F: (huruf drive Anda) ke D:\share karena sistem FSx file Amazon berada di D:\share.
4. Impor konfigurasi berbagi file yang ada FSx untuk Windows File Server. Pada klien yang memiliki akses ke sistem FSx file Amazon tujuan Anda dan server file sumber, salin konfigurasi berbagi

file yang disimpan. Kemudian impor ke dalam sebuah variabel dengan menggunakan perintah berikut.

```
$shares = Import-Clixml -Path F:\SmbShares.xml
```

5. Siapkan objek kredensyal yang diperlukan untuk membuat berbagi file di server file Windows File Server Anda FSx menggunakan salah satu opsi berikut.

   Untuk membuat objek kredensial secara interaktif, gunakan perintah berikut.

   ```
   $credential = Get-Credential
   ```

   Untuk menghasilkan objek kredensyal menggunakan AWS Secrets Manager sumber daya, gunakan perintah berikut.

   ```
   $credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
    $AdminSecret).SecretString
   $FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
   SecureString $credential.Password -AsPlainText -Force)))
   ```

6. Migrasikan konfigurasi berbagi file ke server FSx file Amazon Anda menggunakan skrip berikut.

   ```
   $FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
    "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
    "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
    "Path", "Name", "EncryptData")
   ForEach ($item in $shares) {
       $param = @{};
       Foreach ($property in $item.psObject.properties) {
           if ($property.Name -In $FSxAcceptedParameters) {
               $param[$property.Name] = $property.Value
           }
       }
       Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
    amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
   Credential $Using:credential @Using:param }
   }
   ```

Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server

FSx untuk Windows File Server menyediakan nama Domain Name System (DNS) default untuk setiap sistem file yang dapat Anda gunakan untuk mengakses data pada sistem file Anda. Anda juga dapat mengakses sistem file Anda menggunakan nama DNS apa pun yang Anda pilih dengan mengonfigurasi nama DNS alternatif sebagai alias DNS untuk sistem file Amazon Anda. FSx

Dengan alias DNS, Anda dapat terus menggunakan nama DNS yang ada untuk mengakses data yang disimpan di Amazon FSx saat memigrasi penyimpanan sistem file dari lokal ke Amazon. FSx Ini membantu menghilangkan kebutuhan untuk memperbarui alat atau aplikasi apa pun yang menggunakan nama DNS Anda saat bermigrasi ke Amazon. FSx Anda dapat mengaitkan alias DNS dengan yang ada FSx untuk sistem file Windows File Server, saat Anda membuat sistem file baru, dan saat Anda membuat sistem file baru dari cadangan. Anda dapat mengaitkan hingga 50 alias DNS dengan sebuah sistem file pada satu waktu. Untuk informasi selengkapnya, lihat Mengelola alias DNS.

Nama alias DNS harus memenuhi persyaratan berikut:

- Harus diformat sebagai nama domain yang sepenuhnya memenuhi syarat (FQDN), misalnya, `accounting.example.com`.
- Dapat berisikan karakter alfanumerik dan tanda hubung (-).
- Tidak dapat memulai atau mengakhiri dengan sebuah tanda hubung.
- Dapat memulai dengan angka.

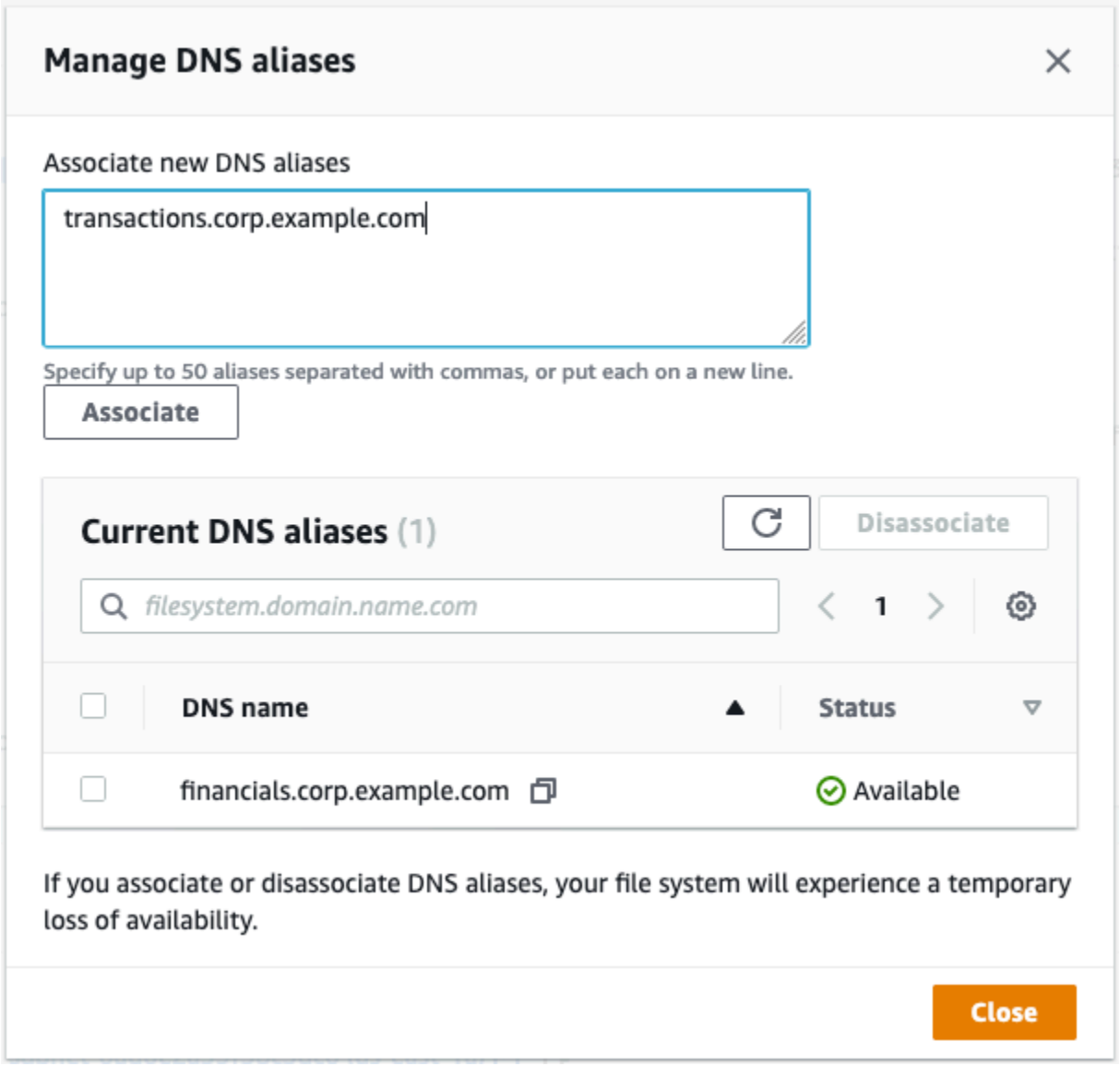
Untuk nama alias DNS, Amazon FSx menyimpan karakter alfabet sebagai huruf kecil (a-z), terlepas dari bagaimana Anda menentukannya: sebagai huruf besar, huruf kecil, atau huruf yang sesuai dalam kode pelarian.

Prosedur berikut menjelaskan cara mengaitkan alias DNS dengan sistem file Server File Windows yang sudah ada FSx menggunakan FSx konsol Amazon, CLI, dan API. Untuk informasi lebih lanjut tentang mengaitkan alias DNS saat membuat sistem file yang baru, termasuk sistem file baru dari cadangan, lihat Mengaitkan alias DNS dengan sistem file.

Untuk mengaitkan alias DNS dengan sistem file yang ada (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Arahkan ke Sistem file, dan pilih sistem file Windows yang ingin Anda ingin kaitkan dengan alias DNS Anda.

3. Pada tab Jaringan & keamanan, pilih Kelola untuk Alias DNS untuk membuka kotak dialog Kelola alias DNS.



4. Di kotak Kaitkan alias yang baru, masukkan alias DNS yang ingin Anda kaitkan.
5. Pilih Kaitkan untuk menambahkan alias ke sistem file.

   Anda dapat memantau status alias yang baru saja Anda kaitkan di daftar Alias saat ini. Saat status terbaca Tersedia, alias tersebut dikaitkan dengan sistem file (sebuah proses yang dapat memakan waktu hingga 2,5 menit).

Untuk mengaitkan alias DNS dengan sistem file yang ada (CLI)

- Gunakan perintah `associate-file-system-aliases` CLI atau operasi AssociateFileSystemAliasesAPI untuk mengaitkan alias DNS dengan sistem file yang ada.

  Permintaan CLI berikut mengaitkan dua alias dengan sistem file yang ditentukan.

  ```
  aws fsx associate-file-system-aliases \
      --file-system-id fs-0123456789abcdef0 \
      --aliases financials.corp.example.com transfers.corp.example.com
  ```

  Respons menunjukkan status alias yang FSx dikaitkan Amazon dengan sistem file.

  ```
  {
        "Aliases": [
            {
                "Name": "financials.corp.example.com",
                "Lifecycle": CREATING
            },
            {
                "Name": "transfers.corp.example.com",
                "Lifecycle": CREATING
            }
        ]
    }
  ```

  Untuk memantau status alias yang Anda kaitkan, gunakan perintah `describe-file-system-aliases` CLI (DescribeFileSystemAliasesadalah operasi API yang setara). Saat `Lifecycle` untuk sebuah alias berisi TERSEDIA, Anda dapat menggunakannya untuk mengakses sistem file (sebuah proses yang dapat memakan waktu hingga 2,5 menit).

Memotong operasi ke Amazon FSx untuk Windows File Server

Setelah memigrasikan penyimpanan file lokal, konfigurasi berbagi file, dan konfigurasi DNS, langkah selanjutnya adalah memotong operasi Anda ke sistem file FSx untuk Windows File Server. Untuk memotong ke sistem file Windows File Server Anda, Anda melakukan langkah-langkah berikut: FSx

- Bersiap untuk cut over.

  - Putuskan sambungan sementara klien SMB dari sistem file yang asli.
  - Lakukan sinkronisasi konfigurasi file akhir dan Berbagi file.
- Konfigurasikan nama utama layanan (SPNs) untuk sistem FSx file Amazon Anda.
- Perbarui catatan DNS CNAME untuk menunjuk ke sistem FSx file Amazon Anda.

Prosedur untuk melakukan setiap langkah ini disediakan di bagian-bagian berikut.

Topik

Mempersiapkan cutover ke Amazon FSx

Untuk mempersiapkan cutover ke sistem FSx file Amazon Anda, Anda harus melakukan hal berikut:

- Putuskan sambungan semua klien yang menulis ke sistem file yang asli.
- Lakukan sinkronisasi file akhir menggunakan AWS DataSync atau Robocopy. Untuk informasi selengkapnya, lihat Migrasi penyimpanan file yang ada ke FSx Windows File Server.
- Lakukan sinkronisasi konfigurasi Berbagi file akhir. Untuk informasi selengkapnya, lihat Memigrasi konfigurasi berbagi file lokal ke Amazon FSx.

Konfigurasikan SPNs untuk otentikasi Kerberos

Kami menyarankan Anda menggunakan otentikasi dan enkripsi berbasis Kerberos dalam perjalanan dengan Amazon. FSx Kerberos menyediakan autentikasi paling aman untuk klien yang mengakses sistem file Anda. Untuk mengaktifkan otentikasi Kerberos untuk klien yang mengakses Amazon FSx menggunakan alias DNS, Anda harus menambahkan nama utama layanan (SPNs) yang sesuai dengan alias DNS pada objek komputer Active Directory sistem file Amazon FSx Anda.

Ada dua yang diperlukan SPNs untuk otentikasi Kerberos.

```
HOST/alias
HOST/alias.domain
```

Sebagai contoh, jika alias adalah`finance.domain.com`, dua yang diperlukan SPNs adalah sebagai berikut.

```
HOST/finance
HOST/finance.domain.com
```

SPN hanya dapat dikaitkan dengan objek komputer direktori aktif tunggal pada satu waktu. Jika ada SPNs nama DNS yang dikonfigurasi untuk objek komputer Active Directory sistem file asli Anda, Anda harus menghapusnya sebelum membuat SPNs untuk sistem FSx file Amazon Anda.

Prosedur berikut menjelaskan cara menemukan yang ada SPNs, menghapusnya, dan membuat yang baru SPNs untuk objek komputer Active Directory sistem FSx file Amazon Anda.

Untuk menginstal modul PowerShell Active Directory yang diperlukan

1. Masuk ke instance Windows yang bergabung dengan Active Directory tempat sistem FSx file Amazon Anda bergabung.
2. Buka PowerShell sebagai administrator.
3. Instal modul PowerShell Active Directory menggunakan perintah berikut.

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

Untuk menemukan dan menghapus alias DNS yang ada SPNs pada objek komputer Active Directory sistem file asli

1. Temukan yang ada SPNs dengan menggunakan perintah berikut. Ganti *`alias_fqdn`* dengan alias DNS yang Anda kaitkan dengan sistem file di Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server.

   ```
   ## Find SPNs for original file system's AD computer object
   $ALIAS = "alias_fqdn"
   SetSPN /Q ("HOST/" + $ALIAS)
   SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
   ```
2. Hapus HOST yang ada SPNs kembali pada langkah sebelumnya dengan menggunakan contoh script berikut.

   - Ganti *`alias_fqdn`* dengan alias DNS penuh yang Anda kaitkan dengan sistem file di Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server.

- Ganti *file_system_DNS_name* dengan nama DNS dari sistem file yang asli.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Ulangi langkah-langkah untuk setiap alias DNS yang Anda kaitkan dengan sistem file di Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server.

Untuk mengatur SPNs objek komputer Active Directory sistem FSx file Amazon Anda

1. Tetapkan baru SPNs untuk sistem FSx file Amazon Anda dengan menjalankan perintah berikut.

   - Ganti *file_system_DNS_name* dengan nama DNS yang FSx ditetapkan Amazon ke sistem file.

     Untuk menemukan nama DNS sistem file Anda di FSx konsol Amazon, pilih Sistem file, dan pilih sistem file Anda. Pilih jendela Jaringan & keamanan di halaman detail sistem file. Anda juga bisa mendapatkan nama DNS sebagai respons operasi DescribeFileSystemsAPI.

   - Ganti *alias_fqdn* dengan alias DNS penuh yang Anda kaitkan dengan sistem file di Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
```

```
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> Menyetel SPN untuk sistem FSx file Amazon Anda akan gagal jika SPN untuk alias DNS ada di AD untuk objek komputer sistem file asli. Untuk informasi tentang menemukan dan menghapus yang ada SPNs, lihatUntuk menemukan dan menghapus alias DNS yang ada SPNs pada objek komputer Active Directory sistem file asli.

2. Verifikasi bahwa SPNs yang baru dikonfigurasi untuk alias DNS menggunakan contoh skrip berikut. Pastikan bahwa respons mencakup dua HOST SPNs, `HOST/`*`alias`* dan`HOST/`*`alias_fqdn`*.

   Ganti *`file_system_DNS_name`* dengan nama DNS yang FSx ditetapkan Amazon ke sistem file Anda. Untuk menemukan nama DNS sistem file Anda di FSx konsol Amazon, pilih Sistem file, pilih sistem file Anda, lalu pilih panel Jaringan & keamanan pada halaman detail sistem file.

   Anda juga bisa mendapatkan nama DNS sebagai respons operasi DescribeFileSystemsAPI.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Ulangi langkah-langkah sebelumnya untuk setiap alias DNS yang telah dikaitkan dengan sistem file di Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server.

> **Note**
>
> Anda dapat menerapkan otentikasi dan enkripsi Kerberos dalam perjalanan dengan klien yang terhubung ke sistem file Anda menggunakan alias DNS dengan menyetel Objek Kebijakan Grup berikut () GPOs di Direktori Aktif Anda:
>
> - Membatasi NTLM: Lalu lintas NTLM Outgoing ke server jarak jauh
> - Membatasi NTLM: Menambahkan pengecualian server jarak jauh untuk autentikasi NTLM

Untuk informasi selengkapnya, lihat Menegakkan otentikasi Kerberos menggunakan Objek Kebijakan Grup () GPOs di Panduan 5: Menggunakan alias DNS untuk mengakses sistem file Anda.

Perbarui catatan DNS CNAME untuk sistem file Amazon FSx

Setelah Anda mengkonfigurasi dengan benar SPNs untuk sistem file Anda, Anda dapat memotong ke Amazon FSx dengan mengganti setiap catatan DNS yang diselesaikan ke sistem file asli dengan catatan DNS yang menyelesaikan ke nama DNS default dari sistem file Amazon. FSx

Untuk menginstal PowerShell cmdlet yang diperlukan

1. Masuk ke instans Windows yang bergabung dengan Direktori Aktif tempat sistem FSx file Amazon Anda bergabung sebagai pengguna yang merupakan anggota grup yang memiliki izin administrasi DNS (Administrator Sistem Nama Domain AWS Delegasi di Direktori Aktif AWS Microsoft Terkelola, dan Admin Domain atau grup lain tempat Anda telah mendelegasikan izin administrasi DNS di Direktori Aktif yang dikelola sendiri)

   Untuk informasi selengkapnya, lihat Menyambungkan ke instans Windows Anda di Panduan EC2 Pengguna Amazon.
2. Buka PowerShell sebagai administrator.
3. Modul server PowerShell DNS diperlukan untuk melakukan instruksi dalam prosedur ini. Instal menggunakan perintah berikut.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Untuk memperbarui catatan DNS CNAME yang ada

1. Skrip berikut memperbarui catatan CNAME DNS yang ada untuk *alias_fqdn* objek komputer sistem FSx file Amazon Anda. Jika tidak ada yang ditemukan, itu membuat catatan CNAME DNS baru untuk alias DNS *alias_fqdn* yang menyelesaikan nama DNS default untuk sistem file Amazon Anda. FSx

   Untuk menjalankan skrip tersebut:

- Ganti *alias_fqdn* dengan alias DNS yang Anda kaitkan dengan sistem file.
- Ganti *file_system_DNS_name* dengan nama DNS default yang FSx telah ditetapkan Amazon ke sistem file.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)[0]

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

2. Ulangi langkah-langkah sebelumnya untuk setiap alias DNS yang Anda kaitkan dengan sistem file di Memigrasi konfigurasi DNS lokal Anda ke Windows File FSx Server.

Pemantauan FSx untuk sistem file Windows File Server

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja FSx untuk Windows File Server dan AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan jika terjadi. Namun, sebelum Anda mulai memantau FSx untuk Windows File Server, Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan-pertanyaan berikut:

- Apa saja sasaran pemantauan Anda?
- Sumber daya apa yang akan Anda pantau?
- Seberapa sering Anda akan memantau sumber daya ini?
- Alat pemantauan apa yang akan Anda gunakan?
- Siapa yang akan melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

Untuk informasi selengkapnya tentang pencatatan dan pemantauan FSx untuk Windows File Server, lihat topik berikut.

Topik

- Pemantauan otomatis dan manual
- Pemantauan CloudWatch dengan Amazon
- Logging Amazon FSx untuk panggilan API Server File Windows menggunakan AWS CloudTrail

Pemantauan otomatis dan manual

AWS menyediakan berbagai alat yang dapat Anda gunakan FSx untuk memantau Windows File Server. Anda dapat mengonfigurasi beberapa alat ini untuk melakukan pemantauan untuk Anda, sementara itu beberapa alat memerlukan campur tangan manual. Sebaiknya Anda mengotomatisasi tugas pemantauan sebanyak mungkin.

Alat pemantauan otomatis

Anda dapat menggunakan alat pemantauan otomatis berikut FSx untuk mengawasi Windows File Server dan melaporkan ketika ada sesuatu yang salah:

- CloudWatch Alarm Amazon — Tonton satu metrik selama periode waktu yang Anda tentukan, dan lakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakannya adalah pemberitahuan yang dikirim ke topik Amazon Simple Notification Service (Amazon SNS) atau kebijakan Amazon Auto EC2 Scaling. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.
- Amazon CloudWatch Logs — Pantau, simpan, dan akses file log Anda dari AWS CloudTrail atau sumber lain. Untuk informasi selengkapnya, lihat Apa itu Amazon CloudWatch Logs? di Panduan Pengguna CloudWatch Log Amazon.
- AWS CloudTrail Pemantauan Log - Bagikan file log antar akun, pantau file CloudTrail log secara real time dengan mengirimkannya ke CloudWatch Log, menulis aplikasi pemrosesan log di Java, dan validasi bahwa file log Anda tidak berubah setelah pengiriman oleh CloudTrail. Untuk informasi selengkapnya, lihat Bekerja dengan File CloudTrail Log di Panduan AWS CloudTrail Pengguna.

Alat-alat pemantauan manual

Bagian penting lainnya dari pemantauan FSx untuk Windows File Server melibatkan pemantauan secara manual item-item yang tidak dicakup oleh CloudWatch alarm Amazon. FSx Untuk Windows File Server, CloudWatch, dan dasbor AWS konsol lainnya memberikan at-a-glance tampilan status AWS lingkungan Anda.

Dasbor FSx Pemantauan & kinerja Amazon menunjukkan:

- Peringatan dan CloudWatch alarm saat ini
- Ringkasan aktivitas sistem file
- Kapasitas penyimpanan dan pemanfaatan sistem file
- Server file dan kinerja volume penyimpanan
- CloudWatch alarm

CloudWatch Dasbor Amazon menunjukkan:

- Alarm dan status saat ini
- Grafik alarm dan sumber daya
- Status kesehatan layanan

Selain itu, Anda dapat menggunakan CloudWatch untuk melakukan hal berikut:

- Buat dasbor yang disesuaikan untuk memantau layanan yang Anda gunakan.
- Data metrik grafik untuk memecahkan masalah dan mengungkap tren.
- Cari dan telusuri semua metrik AWS sumber daya Anda.
- Membuat dan mengedit alarm untuk menerima notifikasi terkait masalah.

Untuk informasi selengkapnya tentang dasbor FSx Pemantauan & kinerja Amazon, lihatMenggunakan metrik sistem file.

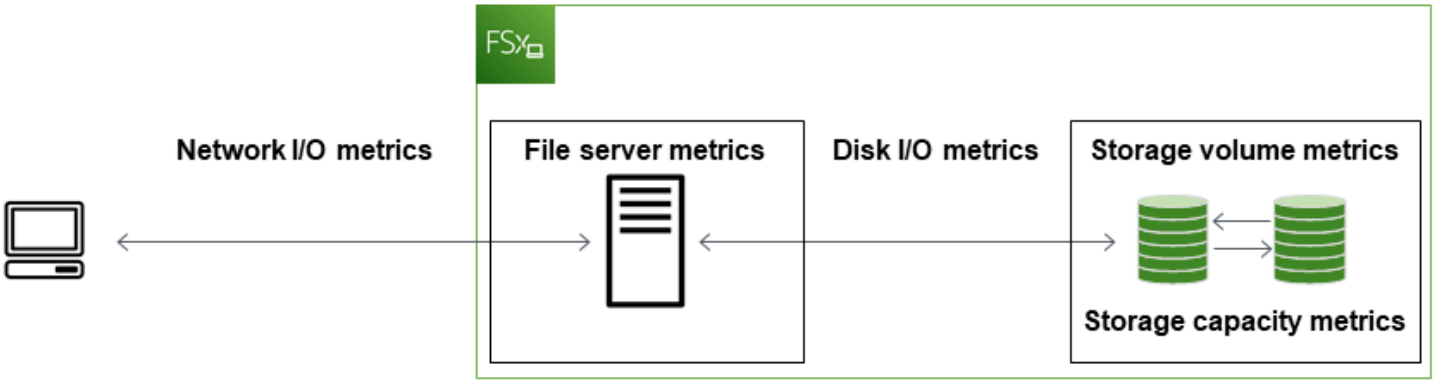
Pemantauan CloudWatch dengan Amazon

Amazon CloudWatch mengumpulkan dan memproses data mentah dari sistem file Windows File Server Anda FSx menjadi metrik hampir real-time yang dapat dibaca. Statistik ini disimpan untuk jangka waktu 15 bulan, memberi Anda akses informasi historis untuk membantu mendapatkan perspektif tentang kinerja alur kerja atau sistem file Anda.

FSx untuk Windows File Server menerbitkan CloudWatch metrik dalam domain berikut:

- Metrik I/O jaringan mengukur aktivitas antara klien yang mengakses sistem file dan server file.
- Metrik server file mengukur pemanfaatan throughput jaringan, CPU dan memori server file, dan throughput disk server file dan pemanfaatan IOPS.
- Metrik I/O disk mengukur aktivitas antara server file dan volume penyimpanan.
- Metrik volume penyimpanan mengukur pemanfaatan throughput disk untuk volume penyimpanan HDD, dan pemanfaatan IOPS untuk volume penyimpanan SSD.
- Metrik kapasitas penyimpanan mengukur penggunaan penyimpanan, termasuk penghematan penyimpanan karena Deduplikasi Data.

Diagram berikut mengilustrasikan FSx untuk sistem file Windows File Server, komponennya, dan domain metrik.



Secara default, Amazon FSx untuk Windows File Server mengirimkan data CloudWatch metrik ke periode 1 menit, dengan pengecualian berikut yang dipancarkan dalam interval 5 menit:

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

Untuk informasi selengkapnya CloudWatch, lihat Apa itu Amazon CloudWatch? di Panduan CloudWatch Pengguna Amazon.

Metrik mungkin tidak dipublikasikan untuk sistem file AZ tunggal selama pemeliharaan sistem file atau penggantian komponen infrastruktur, dan untuk sistem file multi-AZ selama failover dan failback antara server file primer dan sekunder.

Beberapa FSx CloudWatch metrik Amazon dilaporkan sebagai Byte mentah. Byte tidak dibulatkan baik ke desimal atau biner ganda unit.

Topik

- CloudWatch metrik dan dimensi
- Menggunakan metrik sistem file
- Peringatan dan rekomendasi kinerja
- Mengakses metrik sistem file
- Membuat CloudWatch alarm

CloudWatch metrik dan dimensi

FSx untuk Windows File Server menerbitkan metrik berikut ke `AWS/FSx` namespace di CloudWatch Amazon untuk semua sistem file:

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

FSx untuk Windows File Server menerbitkan metrik yang dijelaskan di bagian berikut ke dalam `AWS/FSx` namespace di CloudWatch Amazon untuk sistem file yang dikonfigurasi dengan kapasitas throughput minimal 32. MBps

Metrik I/O jaringan

`AWS/FSx`Namespace mencakup metrik I/O jaringan berikut.

Metrik	Deskripsi
`DataReadBytes`	Jumlah byte untuk operasi baca untuk klien yang mengakses sistem file. Unit: Byte Statistik valid: `Sum`
`DataWriteBytes`	Jumlah byte untuk operasi tulis untuk klien yang mengakses sistem file. Unit: Byte Statistik valid: `Sum`
`DataReadOperations`	Jumlah operasi baca untuk klien yang mengakses sistem file. Unit: Hitungan Statistik valid: `Sum`
`DataWriteOperations`	Jumlah operasi tulis untuk klien yang mengakses sistem file. Unit: Hitungan

Metrik	Deskripsi
	Statistik valid: `Sum`
`MetadataOperations`	Jumlah operasi metadata untuk klien yang mengakses sistem file. Unit: Hitungan Statistik valid: `Sum`
`ClientConnections`	Jumlah koneksi aktif antara klien dan server file. Unit: Hitungan

Metrik server file

`AWS/FSx`Namespace mencakup metrik server file berikut.

Metrik	Deskripsi
`NetworkThroughputUtilization`	Throughput jaringan untuk klien yang mengakses sistem file, sebagai persentase dari batas yang disediakan. Unit: Persen
`CPUUtilization`	Persentase pemanfaatan sumber daya CPU server file Anda. Unit: Persen
`MemoryUtilization`	Persentase pemanfaatan sumber daya memori server file Anda. Unit: Persen
`FileServerDiskThroughputUtilization`	Throughput disk antara server file Anda dan volume penyimpanannya, sebagai persentase dari batas yang disediakan ditentukan oleh kapasitas throughput. Unit: Persen

Metrik	Deskripsi
`FileServerDiskThroughputBalance`	Persentase kredit burst yang tersedia untuk throughput disk antara server file Anda dan volume penyimpanannya. Berlaku untuk sistem file yang disediakan dengan kapasitas throughput 256 MBps atau kurang. Unit: Persen
`FileServerDiskIopsUtilization`	IOPS disk antara server file dan volume penyimpanan, sebagai persentase dari batas yang disediakan ditentukan oleh kapasitas throughput. Unit: Persen
`FileServerDiskIopsBalance`	Persentase kredit burst yang tersedia untuk IOPS disk antara server file Anda dan volume penyimpanannya. Berlaku untuk sistem file yang disediakan dengan kapasitas throughput 256 MBps atau kurang. Unit: Persen

Metrik I/O disk

`AWS/FSx`Namespace mencakup metrik disk I/O berikut.

Metrik	Deskripsi
`DiskReadBytes`	Jumlah byte untuk operasi baca yang mengakses volume penyimpanan. Unit: Byte Statistik yang valid: Jumlah
`DiskWriteBytes`	Jumlah byte untuk operasi tulis yang mengakses volume penyimpanan. Unit: Byte Statistik yang valid: Jumlah

Metrik	Deskripsi
`DiskReadOperations`	Jumlah operasi baca untuk server file yang mengakses volume penyimpanan. Unit: Hitungan Statistik valid: `Sum`
`DiskWriteOperations`	Jumlah operasi tulis untuk server file yang mengakses volume penyimpanan. Unit: Hitungan Statistik valid: `Sum`

FSx untuk metrik volume penyimpanan Windows

`AWS/FSx`Namespace menyertakan metrik volume penyimpanan berikut.

Metrik	Deskripsi
`DiskThroughputUtilization`	(Hanya HDD) Throughput disk antara server file Anda dan volume penyimpanannya, sebagai persentase dari batas yang disediakan yang ditentukan oleh volume penyimpanan. Unit: Persen
`DiskThroughputBalance`	(Hanya HDD) Persentase kredit burst yang tersedia untuk throughput disk dan IOPS disk untuk volume penyimpanan. Unit: Persen
`DiskIopsUtilization`	(Hanya SSD) IOPS disk antara server file Anda dan volume penyimpanan, sebagai persentase dari batas IOPS yang disediakan yang ditentukan oleh volume penyimpanan.

Metrik	Deskripsi
	Unit: Persen

Metrik kapasitas penyimpanan

`AWS/FSx`Namespace mencakup metrik kapasitas penyimpanan berikut.

Metrik	Deskripsi
`FreeStorageCapacity`	Jumlah kapasitas penyimpanan yang tersedia. Unit: Byte Statistik yang valid: `Average`, `Minimum`
`StorageCapacityUtilization`	Kapasitas penyimpanan fisik digunakan sebagai persentase dari total kapasitas penyimpanan. Unit: Persen
`DeduplicationSavedStorage`	Jumlah ruang penyimpanan yang disimpan oleh deduplikasi data, jika diaktifkan. Unit: Byte

Namespace dan dimensi FSx untuk metrik Windows File Server

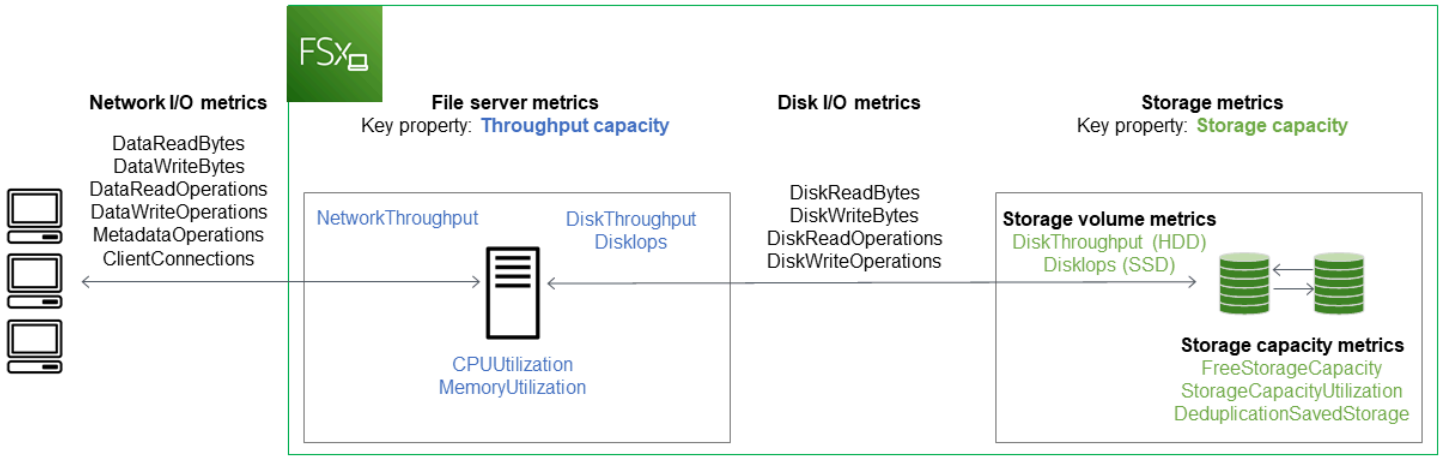
FSx untuk metrik Windows File Server menggunakan `FSx` namespace dan menyediakan metrik untuk satu dimensi,. `FileSystemId` Anda dapat menemukan ID sistem file menggunakan describe-file-systems AWS CLI perintah atau perintah DescribeFileSystemsAPI. ID sistem file mengambil bentuk*`fs-0123456789abcdef0`*.

Menggunakan metrik sistem file

Ada dua komponen arsitektur utama dari setiap sistem FSx file Amazon:

- Server file yang menyajikan data ke klien yang mengakses sistem file.
- Volume penyimpanan yang meng-host data dalam sistem file Anda.

FSx untuk Windows File Server melaporkan metrik CloudWatch yang melacak kinerja dan pemanfaatan sumber daya untuk server file sistem file dan volume penyimpanan Anda. Diagram berikut mengilustrasikan sistem FSx file Amazon dengan komponen arsitekturnya, serta CloudWatch metrik kinerja dan sumber daya yang tersedia untuk pemantauan. Properti kunci yang ditampilkan untuk satu set metrik adalah properti sistem file yang menentukan kapasitas untuk metrik tersebut. Menyesuaikan properti itu memodifikasi kinerja sistem file untuk kumpulan metrik tersebut.



Gunakan panel Pemantauan & kinerja di FSx konsol Amazon untuk melihat CloudWatch metrik Windows File Server yang dijelaskan dalam tabel berikut. FSx

Panel pemantaan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
Ringkasan	... menentukan IOPS total sistem file saya?	Jumlah IOPS	SUM (`DataReadOperations + DataWriteOperations +MetadataOperations`) /Periode (dalam detik)
	... menentukan total throughput sistem file saya?	Total throughput	SUM (`DataReadBytes +DataWriteBytes`) /Periode (dalam detik)
	... menentukan jumlah kapasitas penyimpanan yang tersedia pada sistem file saya?	Kapasitas penyimpan	`FreeStorageCapacity`

Panel pemantau n & kinerja	Bagaimana saya...	Bagan	Metrik terkait
		an yang tersedia	
	... menentukan jumlah koneksi yang dibuat antara klien dan server file?	Koneksi klien	`ClientConnections`
Penyimpanan	... menentukan jumlah ruang disk fisik yang digunakan sebagai persentase dari total kapasitas penyimpanan sistem file?	Pemanfaatan kapasitas penyimpanan	`StorageCapacityUtilization`
	... menentukan jumlah ruang disk fisik yang disimpan oleh deduplikasi data?	Penyimpanan disimpan dari Deduplikasi Data	`DeduplicationSavedStorage`
Kinerja - Server file	... menentukan throughput jaringan untuk klien yang mengakses sistem file, sebagai persentase dari throughput yang disediakan sistem file?	Pemanfaatan throughput jaringan	`NetworkThroughputUtilization` [1]
	... menentukan throughput disk antara file server dan volume penyimpanannya, sebagai persentase dari batas yang disediakan ditentukan oleh Kapasitas Throughput?	Pemanfaatan throughput disk	`FileServerDiskThroughputUtilization` [1]

Panel pemantau n & kinerja	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan persentase kredit burst yang tersedia untuk throughput disk antara server file dan volume penyimpanannya?	Keseimbangan burst throughput disk	`FileServerDiskThroughputBalance`
	... menentukan jumlah IOPS disk antara server file dan volume penyimpanan, sebagai persentase dari batas yang disediakan ditentukan oleh Kapasitas Throughput?	Pemanfaatan Disk IOPS	`FileServerDiskIopsUtilization`
	... menentukan persentase kredit burst yang tersedia untuk IOPS disk antara server file dan volume penyimpanan?	Keseimbangan burst IOPS Disk	`FileServerDiskIopsBalance`
	... menentukan persentase pemanfaatan CPU file server?	Pemanfaatan CPU	`CPUUtilization`
	... menentukan persentase pemanfaatan memori file server?	Pemanfaatan memori	`MemoryUtilization`
Kinerja - Volume penyimpanan	... menentukan throughput untuk operasi yang mengakses volume penyimpanan, sebagai persentase dari batas yang disediakan yang ditentukan oleh Kapasitas Penyimpanan HDD?	Pemanfaatan throughput disk (HDD)	`DiskThroughputUtilization`

Panel pemantaan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan persentase throughput yang tersedia dan kredit burst IOPS untuk operasi yang mengakses volume penyimpanan HDD?	Keseimbangan burst throughput disk (HDD)	`DiskThroughputBalance` [2]
	... menentukan IOPS untuk operasi yang mengakses volume penyimpanan, sebagai persentase dari batas yang disediakan yang ditentukan oleh Kapasitas Penyimpanan HDD?	Pemanfaatan Disk IOPS (HDD)	SUM (`DiskReadOperations` `+DiskWriteOperations`)/`Period`(dalam hitungan detik)/(12 * kapasitas penyimpanan HDD yang disediakan di TiB)
	... menentukan IOPS untuk operasi yang mengakses volume penyimpanan, sebagai persentase dari batas yang ditentukan oleh Kapasitas Penyimpanan SSD?	Pemanfaatan Disk IOPS (SSD)	`DiskIopsUtilization`

Note

[1] Kami menyarankan Anda mempertahankan pemanfaatan kapasitas throughput rata-rata di bawah 50% untuk memastikan bahwa Anda memiliki kapasitas throughput cadangan yang cukup untuk lonjakan tak terduga dalam beban kerja Anda, serta untuk setiap operasi penyimpanan Windows latar belakang (seperti sinkronisasi penyimpanan, deduplikasi, atau salinan bayangan).

[2] Volume penyimpanan HDD dapat mengalami variasi kinerja yang signifikan tergantung pada beban kerja. Lonjakan mendadak dalam IOPS atau throughput dapat menyebabkan penurunan kinerja disk. Untuk informasi selengkapnya, lihat Kinerja HDD burst.

Peringatan dan rekomendasi kinerja

FSx untuk Windows memberi Anda peringatan kinerja untuk sistem file yang dikonfigurasi dengan kapasitas throughput minimal 32. MBps Amazon FSx menampilkan peringatan untuk satu set CloudWatch metrik setiap kali salah satu metrik ini mendekati atau melewati ambang batas yang telah ditentukan untuk beberapa titik data berturut-turut. Peringatan ini memberi Anda rekomendasi yang dapat ditindaklanjuti yang dapat Anda gunakan untuk mengoptimalkan kinerja sistem file Anda.

Peringatan dapat diakses di beberapa area dasbor Pemantauan & kinerja. Semua peringatan FSx kinerja Amazon aktif atau terbaru dan CloudWatch alarm apa pun yang dikonfigurasi untuk sistem file yang berada dalam status ALARM muncul di panel Pemantauan & kinerja di bagian Ringkasan. Peringatan juga muncul di bagian dasbor bahwa grafik metrik ditampilkan.

Anda dapat membuat CloudWatch alarm untuk salah satu FSx metrik Amazon. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm.

Gunakan peringatan kinerja untuk meningkatkan kinerja sistem file

Amazon FSx memberikan rekomendasi yang dapat ditindaklanjuti yang dapat Anda gunakan untuk mengoptimalkan kinerja sistem file Anda. Rekomendasi ini menjelaskan bagaimana Anda dapat mengatasi leher botol kinerja potensial. Anda dapat mengambil tindakan yang disarankan jika Anda mengharapkan aktivitas berlanjut, atau jika itu menyebabkan dampak pada kinerja sistem file Anda. Bergantung pada metrik mana yang memicu peringatan, Anda dapat menyelesaikannya dengan meningkatkan kapasitas throughput atau kapasitas penyimpanan sistem file, seperti yang dijelaskan dalam tabel berikut.

Jika ada peringatan untuk metrik ini	Lakukan hal berikut
Throughput jaringan - pemanfaatan	Meningkatkan kapasitas throughput
Server file > Disk IOPS - pemanfaatan	
File server > Disk throughput — pemanfaatan	
Server file > Disk IOPS - keseimbangan burst	
Server file > Throughput disk - keseimbangan burst	
Pemanfaatan kapasitas penyimpanan	Meningkatkan kapasitas penyimpanan

Jika ada peringatan untuk metrik ini	Lakukan hal berikut
Volume penyimpanan> Throughput disk - pemanfaatan (HDD)	Meningkatkan kapasitas penyimpanan atau beralih ke jenis penyimpanan SDD
Volume penyimpanan> Throughput disk - keseimbangan burst (HDD)	
Volume penyimpanan> Disk IOPS - pemanfaatan (SSD)	Tingkatkan IOPS SSD

> **Note**
>
> Peristiwa sistem file tertentu dapat menggunakan sumber daya kinerja I/O disk dan berpotensi memicu peringatan kinerja. Misalnya:
>
> - Fase optimasi penskalaan kapasitas penyimpanan dapat menghasilkan peningkatan throughput disk, seperti yang dijelaskan dalam Kapasitas penyimpanan meningkat dan performa sistem file
> - Untuk sistem file multi-AZ, peristiwa seperti penskalaan kapasitas throughput, penggantian perangkat keras, atau gangguan Availability Zone menghasilkan peristiwa failover dan failback otomatis. Setiap perubahan data yang terjadi selama waktu ini perlu disinkronkan antara server file primer dan sekunder, dan Windows Server menjalankan pekerjaan sinkronisasi data yang dapat menggunakan sumber daya I/O disk. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Untuk informasi selengkapnya performa sistem berkas, lihatFSx untuk kinerja Windows File Server.

Mengakses metrik sistem file

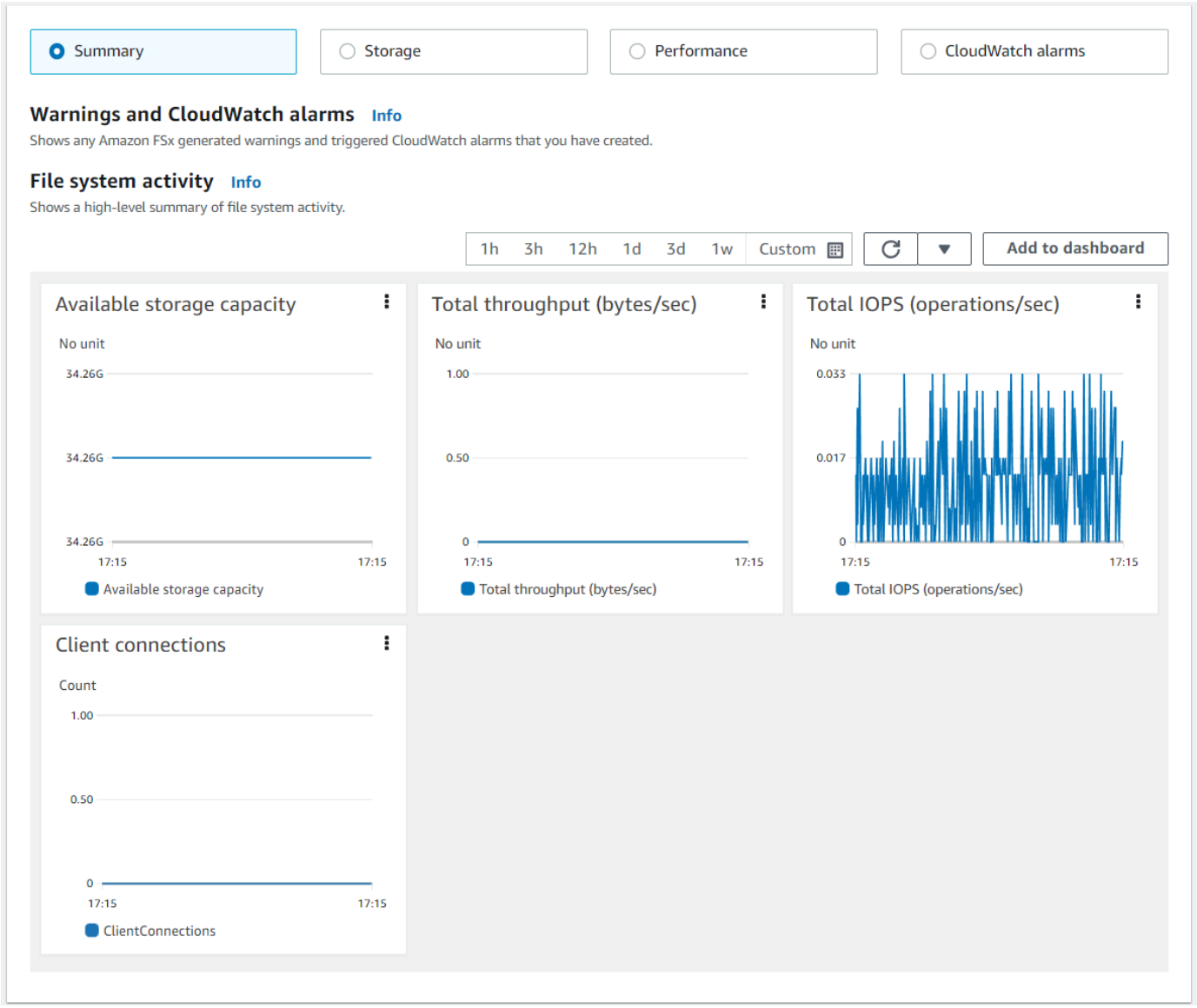
Anda dapat melihat FSx metrik Amazon dengan CloudWatch cara berikut.

- FSx Konsol Amazon
- CloudWatch Konsol
- CloudWatch CLI
- CloudWatch API

Prosedur berikut menjelaskan cara mengakses metrik sistem file Anda menggunakan berbagai alat ini.

Untuk melihat metrik sistem file menggunakan konsol Amazon FSx

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Untuk menampilkan halaman Detail sistem berkas, pilih Sistem berkas di panel navigasi.
3. Pilih sistem file yang metriknya ingin Anda lihat.
4. Untuk melihat grafik metrik sistem file, pilih Pemantauan & kinerja pada panel kedua.



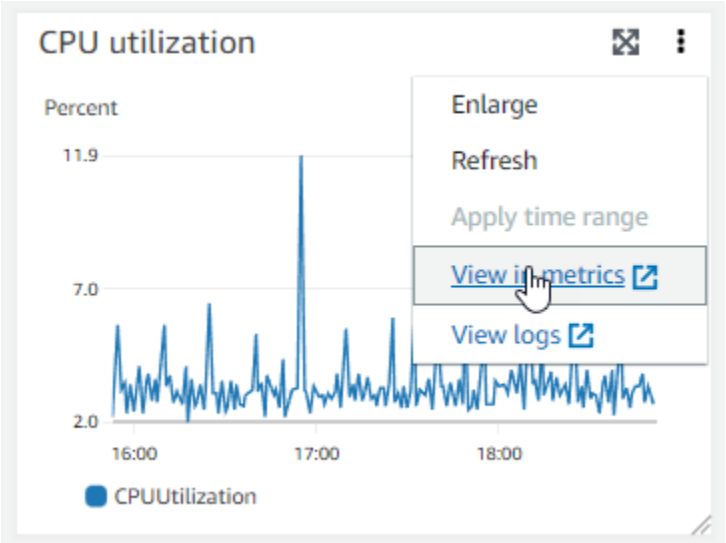
- Metrik Ringkasan ditampilkan secara default, menampilkan peringatan dan CloudWatch alarm aktif apa pun bersama dengan metrik aktivitas sistem File.

- Pilih Penyimpanan untuk melihat kapasitas penyimpanan dan metrik pemanfaatan.
- Pilih Kinerja untuk melihat metrik kinerja server file dan penyimpanan
- Pilih CloudWatch alarm untuk melihat grafik alarm apa pun yang dikonfigurasi untuk sistem file.

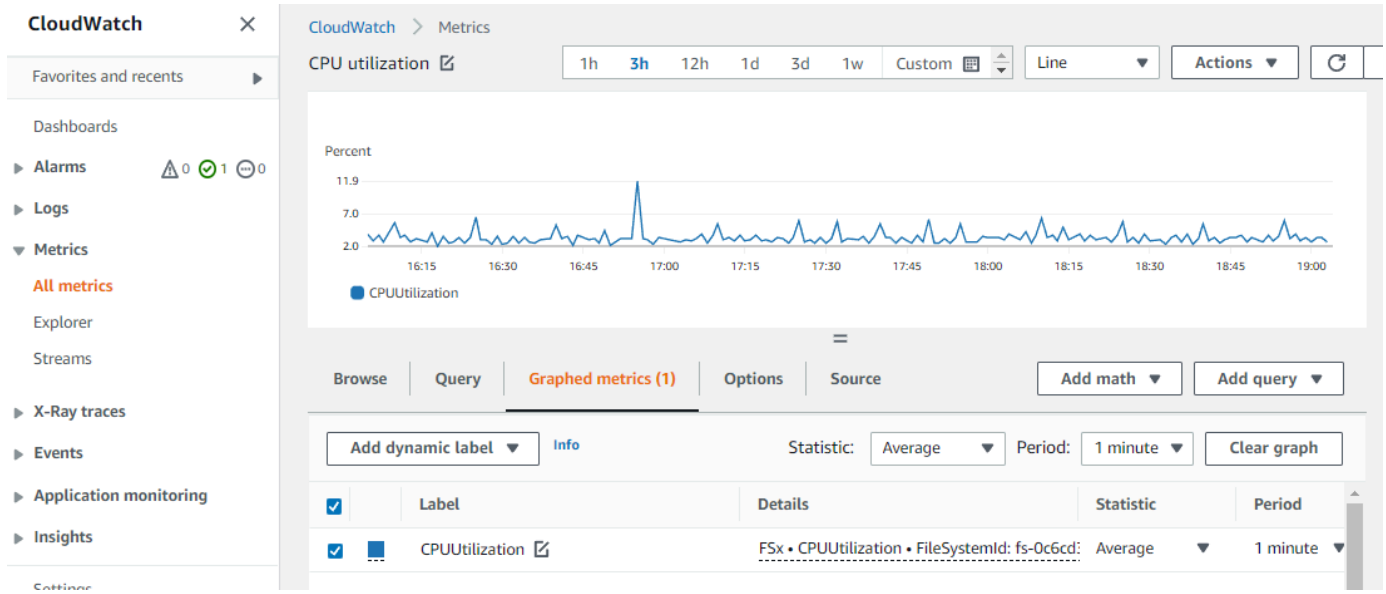
Untuk informasi selengkapnya, lihat Menggunakan metrik sistem file

Untuk melihat metrik di konsol CloudWatch

1. Untuk melihat metrik sistem file di halaman Metrik CloudWatch konsol Amazon, navigasikan ke metrik di panel Pemantauan & kinerja FSx konsol Amazon.
2. Pilih Lihat dalam metrik dari menu tindakan di kanan atas grafik metrik, seperti yang ditunjukkan pada gambar berikut.



Ini membuka halaman Metrik di CloudWatch konsol, menampilkan grafik metrik, seperti yang ditunjukkan pada gambar berikut.



Untuk menambahkan metrik ke dasbor CloudWatch

1. Untuk menambahkan satu FSx set metrik sistem file Windows ke dasbor di CloudWatch konsol, pilih kumpulan metrik (Ringkasan, Penyimpanan, atau Kinerja) di panel Pemantauan & kinerja konsol Amazon FSx .
2. Pilih Tambahkan ke dasbor di kanan atas panel, ini membuka CloudWatch konsol.
3. Pilih CloudWatch dasbor yang ada dari daftar, atau buat dasbor baru. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch dasbor Amazon di Panduan CloudWatch Pengguna Amazon.

Untuk mengakses metrik dari AWS CLI

- Gunakan perintah `list-metrics` dengan perintah namespace `--namespace "AWS/FSx"`. Untuk informasi selengkapnya, lihat Referensi Perintah AWS CLI.

```
$ aws cloudwatch list-metrics --namespace "AWS/FSx"
aws cloudwatch list-metrics --namespace "AWS/FSx"
{
    "Metrics": [
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DataWriteOperationTime",
            "Dimensions": [
                {
```

```
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CapacityPoolWriteBytes",
            "Dimensions": [
                {
                    "Name": "VolumeId",
                    "Value": "fsvol-0cb2281509f5db3c2"
                },
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DiskReadBytes",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CompressionRatio",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-0f84c9a176a4d7c92"
                }
            ]
        },
.
.
.
}
```

Menggunakan CloudWatch API

Untuk mengakses metrik dari API CloudWatch

- Panggil `GetMetricStatistics`. Untuk informasi selengkapnya, lihat Referensi Amazon CloudWatch API.

Membuat CloudWatch alarm

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon SNS saat alarm berubah status. Alarm mengawasi satu metrik selama jangka waktu yang Anda tentukan, dan melakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama jangka waktu tertentu. Tindakan ini adalah notifikasi yang dikirim ke topik Amazon SNS atau kebijakan Penskalaan Otomatis.

Alarm memanggil tindakan untuk perubahan status berkelanjutan saja. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Anda dapat membuat alarm dari FSx konsol Amazon atau CloudWatch konsol.

Prosedur berikut menjelaskan cara membuat alarm untuk Amazon FSx menggunakan konsol, AWS CLI, dan API.

Untuk mengatur CloudWatch alarm (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Dari panel navigasi kiri, pilih Sistem file, lalu pilih sistem file yang ingin Anda pasang alarm.
3. Pilih menu Tindakan, dan pilih Lihat detail.
4. Pada halaman Ringkasan, pilih Pemantauan dan kinerja.
5. Pilih CloudWatch alarm.
6. Pilih Buat CloudWatch alarm. Anda dialihkan ke konsol CloudWatch.
7. Pilih Pilih metrik, dan pilih Selanjutnya.
8. Di bagian Metrik, pilih FSX.
9. Pilih Metrik Sistem File, pilih metrik yang ingin Anda atur alarm untuknya, lalu pilih Pilih metrik.
10. Di bagian Kondisi, pilih kondisi yang Anda inginkan untuk alarm, dan pilih Selanjutnya.

> **Note**
>
> Metrik mungkin tidak dipublikasikan selama pemeliharaan sistem file untuk sistem file Single-AZ, atau selama failover dan failback ke atau dari server primer atau sekunder untuk sistem file multi-AZ. Untuk mencegah perubahan kondisi alarm yang tidak perlu dan menyesatkan dan mengonfigurasi alarm Anda agar tahan terhadap titik data yang hilang, lihat Mengonfigurasi cara CloudWatch alarm menangani data yang hilang di Panduan Pengguna Amazon. CloudWatch

11. Jika Anda CloudWatch ingin mengirimi Anda email atau pemberitahuan SNS saat status alarm memicu tindakan, pilih status alarm untuk Kapan pun status alarm ini terjadi.

    Untuk pilih sebuah topik SNS, pilih topik SNS yang sudah ada. Jika memilih Buat topik, Anda dapat mengatur nama dan alamat email untuk daftar langganan email baru. Daftar ini disimpan dan muncul dalam bidang isian untuk alarm selanjutnya. Pilih Selanjutnya.

    > **Note**
    >
    > Jika Anda menggunakan Buat topik untuk membuat topik Amazon SNS yang baru, alamat email harus diverifikasi sebelum menerima pemberitahuan. Email hanya dikirimkan saat alarm berada dalam status alarm. Jika perubahan status alarm ini terjadi sebelum alamat email diverifikasi, alamat email tidak akan menerima pemberitahuan.

12. Isi nilai Nama, Deskripsi, dan Kapan pun untuk metrik, dan pilih Selanjutnya.
13. Pada halaman Pratinjau dan buat, tinjau alarm yang akan Anda buat, lalu pilih Buat Alarm.

Untuk mengatur alarm menggunakan konsol CloudWatch

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Buat Alarm Untuk memulai Wizard Buat Alarm.
3. Pilih FSx Metrik, dan gulir FSx metrik Amazon untuk menemukan metrik yang ingin Anda gunakan alarm. Untuk menampilkan hanya FSx metrik Amazon di kotak dialog ini, cari di ID sistem file dari sistem file Anda. Pilih metrik untuk mengaktifkan sebuah alarm lalu pilih Selanjutnya.
4. Masukkan nilai Nama, Deskripsi, dan Kapan pun untuk metrik.

5. Jika Anda ingin CloudWatch mengirimi Anda email ketika status alarm tercapai, untuk Setiap kali alarm ini, pilih Status adalah ALARM. Untuk Mengirimkan notifikasi ke, pilih topik SNS yang sudah ada. Jika Anda memilih Buat topik, Anda dapat mengatur nama dan alamat email untuk daftar langganan email baru. Daftar ini disimpan dan muncul dalam bidang isian untuk alarm selanjutnya.

   > **Note**
   >
   > Jika Anda menggunakan Buat topik untuk membuat topik Amazon SNS baru, alamat email harus diverifikasi sebelum menerima pemberitahuan. Email hanya dikirimkan saat alarm berada dalam status alarm. Jika perubahan status alarm ini terjadi sebelum alamat email diverifikasi, alamat email tidak akan menerima pemberitahuan.

6. Pada titik ini, area Pratinjau Alarm memberi Anda kesempatan untuk melakukan pratinjau alarm yang akan Anda buat. Pilih Buat Alarm.

Untuk mengatur CloudWatch alarm (CLI)

- Panggil `put-metric-alarm`. Untuk informasi selengkapnya, lihat Referensi Perintah AWS CLI.

Untuk mengatur alarm (API)

- Panggil `PutMetricAlarm`. Untuk informasi selengkapnya, lihat Referensi Amazon CloudWatch API.

Logging Amazon FSx untuk panggilan API Server File Windows menggunakan AWS CloudTrail

Amazon FSx untuk Windows File Server terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon FSx. CloudTrail menangkap semua panggilan API untuk Amazon FSx sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari FSx konsol Amazon dan panggilan kode ke operasi Amazon FSx API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Amazon. FSx 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 Amazon FSx, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

FSx Informasi Amazon di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Amazon FSx, 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 situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Amazon FSx, 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 Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua FSx tindakan Amazon dicatat oleh CloudTrail dan didokumentasikan dalam Referensi FSx API Amazon. Misalnya, panggilan ke`CreateFileSystem`, `CreateBackup` dan `TagResource` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.

- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file FSx log Amazon

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 `TagResource` operasi ketika tag untuk sistem file dibuat dari konsol.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
```

```
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `UntagResource` tindakan ketika tag untuk sistem file dihapus dari konsol.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
```

```
}
```

Keamanan di Amazon FSx

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 menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di Amazon Web Services Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon FSx untuk Windows File Server, lihat AWS Layanan dalam Lingkup berdasarkan 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 Amazon FSx untuk Windows File Server. Topik berikut menunjukkan cara mengonfigurasi Amazon FSx untuk Windows File Server untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon FSx untuk Windows File Server Anda.

Topik

Perlindungan data di Amazon FSx untuk Windows File Server

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon FSx untuk Windows File Server. 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 sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan FSx untuk Windows File Server 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 FSx untuk Windows File Server

Amazon FSx untuk Windows File Server mendukung enkripsi data saat istirahat dan enkripsi data dalam perjalanan. Enkripsi data saat istirahat diaktifkan secara otomatis saat membuat sistem FSx file Amazon. Enkripsi data dalam transit di-support pada akses berbagi file yang dipetakan pada instans komputasi yang men-support protokol SMB 3.0 atau yang lebih baru. Amazon FSx secara otomatis mengenkripsi data dalam perjalanan menggunakan enkripsi SMB saat Anda mengakses sistem file Anda tanpa perlu memodifikasi aplikasi Anda.

Kapan menggunakan enkripsi

Jika organisasi Anda tunduk pada kebijakan perusahaan atau peraturan yang memerlukan enkripsi data dan metadata saat istirahat, sebaiknya buat sistem file terenkripsi yang memasang sistem file Anda menggunakan enkripsi data saat transit.

Jika organisasi Anda tunduk pada kebijakan perusahaan atau peraturan yang memerlukan enkripsi data dan metadata saat istirahat, data Anda secara otomatis dienkripsi saat istirahat. Kami juga menyarankan Anda mengaktifkan enkripsi data dalam perjalanan dengan memasang sistem file Anda menggunakan enkripsi data dalam perjalanan.

Enkripsi data saat tidak digunakan

Semua sistem FSx file Amazon dienkripsi saat istirahat dengan kunci yang dikelola menggunakan AWS Key Management Service ()AWS KMS. Data dienkripsi secara otomatis sebelum ditulis ke sistem file, dan secara otomatis didekripsi saat dibaca. Proses ini ditangani secara transparan oleh Amazon FSx, jadi Anda tidak perlu memodifikasi aplikasi Anda.

Amazon FSx menggunakan algoritma enkripsi AES-256 standar industri untuk mengenkripsi FSx data Amazon dan metadata saat istirahat. Untuk informasi selengkapnya, lihat Dasar-dasar Kriptografi di Panduan Developer AWS Key Management Service .

> **Note**
>
> Infrastruktur manajemen AWS kunci menggunakan Federal Information Processing Standards (FIPS) 140-2 algoritma kriptografi yang disetujui. Infrastruktur ini konsisten dengan rekomendasi National Institute of Standard and Technology (NIST) 800-57.

Bagaimana Amazon FSx menggunakan AWS KMS

Amazon FSx terintegrasi dengan AWS KMS untuk manajemen kunci. Amazon FSx menggunakan file AWS KMS key untuk mengenkripsi sistem file Anda. Anda memilih kunci KMS yang digunakan untuk mengenkripsi dan mendekripsi sistem file (baik data maupun metadata). Anda dapat mengaktifkan, menonaktifkan, atau mencabut hibah pada kunci KMS ini. Kunci KMS ini dapat menjadi salah satu dari dua jenis berikut:

- Kunci yang dikelola AWS— Ini adalah kunci KMS default, dan gratis untuk digunakan.
- Kunci terkelola pelanggan - Ini adalah kunci KMS yang paling fleksibel untuk digunakan, karena Anda dapat mengonfigurasi kebijakan dan hibah utamanya untuk beberapa pengguna atau layanan. Untuk informasi selengkapnya tentang membuat kunci terkelola pelanggan, lihat Membuat kunci di Panduan AWS Key Management Service Pengembang.

Jika Anda menggunakan kunci yang dikelola pelanggan sebagai kunci KMS Anda untuk enkripsi dan dekripsi data file, Anda dapat mengaktifkan rotasi kunci. Bila Anda mengaktifkan rotasi kunci, AWS KMS secara otomatis akan merotasi kunci Anda satu kali per tahun. Selain itu, dengan kunci yang dikelola pelanggan, Anda dapat memilih kapan harus menonaktifkan, mengaktifkan kembali, menghapus, atau mencabut akses ke kunci KMS Anda kapan saja. Untuk informasi selengkapnya, lihat Memutar AWS KMS keys di Panduan AWS Key Management Service Pengembang.

Kebijakan Amazon FSx Key untuk AWS KMS

Kebijakan utama adalah cara utama untuk mengontrol akses ke kunci KMS. Untuk informasi selengkapnya tentang kebijakan kunci, lihat Menggunakan kebijakan kunci di AWS KMS dalam Panduan Developer AWS Key Management Service . Daftar berikut menjelaskan semua izin AWS KMS terkait yang didukung oleh Amazon FSx untuk sistem file terenkripsi saat istirahat:

- kms:Encrypt – (Opsional) Mengenkripsi plaintext ke ciphertext. Izin ini termasuk dalam kebijakan kunci default.

- kms:Decrypt – (Wajib) Mendekripsi ciphertext. Ciphertext adalah plaintext yang telah dienkripsi sebelumnya. Izin ini termasuk dalam kebijakan kunci default.
- kms: ReEncrypt — (Opsional) Mengenkripsi data di sisi server dengan kunci KMS baru, tanpa mengekspos plaintext data di sisi klien. Data pertama kali didekripsi dan kemudian dienkripsi ulang. Izin ini termasuk dalam kebijakan kunci default.
- kms: GenerateDataKeyWithoutPlaintext — (Diperlukan) Mengembalikan kunci enkripsi data yang dienkripsi di bawah kunci KMS. Izin ini disertakan dalam kebijakan kunci default di bawah kms: GenerateDataKey *.
- kms: CreateGrant — (Diperlukan) Menambahkan hibah ke kunci untuk menentukan siapa yang dapat menggunakan kunci dan dalam kondisi apa. Hibah adalah mekanisme izin lainnya untuk kebijakan kunci. Untuk informasi selengkapnya tentang hibah, lihat Menggunakan hibah di Panduan AWS Key Management Service Pengembang. Izin ini termasuk dalam kebijakan kunci default.
- kms: DescribeKey - (Diperlukan) Memberikan informasi rinci tentang kunci KMS yang ditentukan. Izin ini termasuk dalam kebijakan kunci default.
- kms: ListAliases — (Opsional) Daftar semua alias kunci di akun. Saat Anda menggunakan konsol untuk membuat sistem file terenkripsi, izin ini mengisi daftar kunci KMS. Kami merekomendasikan untuk menggunakan izin ini untuk memberikan pengalaman pengguna yang terbaik. Izin ini termasuk dalam kebijakan kunci default.

Mengenkripsi data saat transit

Enkripsi data dalam transit di-support pada akses berbagi file yang dipetakan pada instans komputasi yang men-support protokol SMB 3.0 atau yang lebih baru. Ini termasuk semua versi Windows mulai dari Windows Server 2012 dan Windows 8, dan semua Linux client dengan Samba client versi 4.2 atau yang lebih baru. Amazon FSx untuk Windows File Server secara otomatis mengenkripsi data dalam perjalanan menggunakan enkripsi SMB saat Anda mengakses sistem file Anda tanpa perlu memodifikasi aplikasi Anda.

Enkripsi SMB menggunakan AES-128-GCM atau AES-128-CCM (dengan varian GCM yang terpilih jika klien men-support SMB 3.1.1) sebagai algoritme enkripsinya, dan juga menyediakan integritas data dengan penandaan menggunakan kunci sesi SMB Kerberos. Penggunaan AES-128-GCM mengarah pada performa yang lebih baik, misalnya, hingga peningkatan kinerja 2x ketika menyalin file besar melalui koneksi SMB terenkripsi.

Untuk memenuhi persyaratan kepatuhan untuk selalu mengenkripsi data-in-transit, Anda dapat membatasi akses sistem file untuk hanya mengizinkan akses ke klien yang mendukung enkripsi SMB. Anda juga dapat mengaktifkan atau me-nonaktifkan enkripsi dalam transit per Berbagi file atau ke seluruh sistem file. Hal ini memungkinkan Anda untuk memiliki campuran Berbagi file yang terenkripsi dan tidak terenkripsi pada sistem file yang sama.

Mengelola enkripsi in transit

Anda dapat menggunakan serangkaian PowerShell perintah khusus untuk mengontrol enkripsi data Anda dalam perjalanan antara sistem file Windows File Server dan klien Anda FSx . Anda dapat membatasi akses sistem file hanya untuk klien yang mendukung enkripsi SMB sehingga selalu data-in-transit dienkripsi. Ketika penegakan dihidupkan untuk enkripsi data-in-transit, pengguna yang mengakses sistem file dari klien yang tidak mendukung enkripsi SMB 3.0 tidak akan dapat mengakses berbagi file yang enkripsi dihidupkan.

Anda juga dapat mengontrol enkripsi data-in-transit pada tingkat berbagi file, bukan tingkat server file. Anda dapat menggunakan kontrol enkripsi tingkat pembagian file untuk memiliki gabungan pembagian file terenkripsi dan tidak terenkripsi pada sistem file yang sama jika Anda ingin memberlakukan enkripsi di-transit untuk beberapa pembagian file yang memiliki data sensitif, dan mengizinkan semua pengguna untuk mengakses beberapa pembagian file lainnya. Enkripsi seluruh server memiliki prioritas atas enkripsi tingkat pembagian. Jika enkripsi global diaktifkan, Anda tidak dapat memilih menonaktifkan enkripsi untuk pembagian tertentu.

Anda dapat mengelola enkripsi dalam transit pada sistem file Anda menggunakan Amazon FSx CLI untuk manajemen jarak jauh. PowerShell Untuk mempelajari cara menggunakan CLI ini, lihat Menggunakan Amazon FSx CLI untuk PowerShell.

Berikut ini adalah perintah yang dapat Anda gunakan untuk mengelola enkripsi in-transit pengguna pada sistem file Anda.

Perintah Enkripsi in Transit	Deskripsi
Get-FSxSmbServerConfiguration	Mengambil konfigurasi server Server Message Block (SMB). Dalam respons sistem, Anda dapat menentukan enkripsi dalam pengaturan transit untuk sistem file Anda berdasarkan nilai untuk properti dan`EncryptData` .`RejectUnencryptedAccess`

Perintah Enkripsi in Transit	Deskripsi
Set-FSxSmbServerConfiguration	Perintah ini memiliki dua opsi untuk mengonfigurasi enkripsi in-transit secara global pada sistem file: • `-EncryptData $True\|$False` — Atur parameter ini `True` untuk mengaktifkan enkripsi data dalam transit. Setel parameter ini `False` untuk mematikan enkripsi data dalam transit. • `-RejectUnencryptedAccess $True\|$False` — Tetapkan parameter ini `True` untuk melarang klien yang tidak mendukung enkripsi untuk mengakses sistem file. Tetapkan parameter ini `False` untuk memungkinkan klien yang tidak mendukung enkripsi untuk mengakses sistem file.
Set-FSxSmbShare -name ***name*** -EncryptData $True	Setel parameter ini `True` untuk mengaktifkan enkripsi data dalam transit untuk berbagi. Setel parameter ini `False` untuk mematikan enkripsi data dalam transit untuk berbagi.

Bantuan online untuk setiap perintah memberikan referensi dari semua opsi perintah. Untuk mengakses bantuan ini, jalankan perintah dengan -?, misalnya Get-FSxSmbServerConfiguration -?.

Kontrol akses tingkat file dan folder menggunakan Windows ACLs

Amazon FSx untuk Windows File Server mendukung otentikasi berbasis identitas melalui protokol Server Message Block (SMB) melalui Microsoft Active Directory. Direktori Aktif adalah layanan direktori Microsoft untuk menyimpan informasi tentang objek pada jaringan dan membuat informasi ini mudah ditemukan dan digunakan oleh administrator dan pengguna. Objek ini biasanya mencakup sumber daya bersama seperti server file, dan pengguna jaringan dan akun komputer. Untuk mempelajari selengkapnya tentang dukungan Direktori Aktif di Amazon FSx, lihatBekerja dengan Microsoft Active Directory.

Instans komputasi yang bergabung dengan domain Anda dapat mengakses pembagian file FSx Amazon menggunakan kredenal Direktori Aktif. Anda menggunakan daftar kontrol akses Windows standar (ACLs) untuk kontrol akses tingkat file dan folder berbutir halus. Sistem FSx file Amazon secara otomatis memverifikasi kredensil pengguna yang mengakses data sistem file untuk menegakkan Windows ini. ACLs

Setiap sistem FSx file Amazon dilengkapi dengan file share Windows default yang disebut`share`. Windows ACLs untuk folder bersama ini dikonfigurasi untuk memungkinkan akses baca/tulis ke pengguna domain. ACL juga mengizinkan kendali penuh untuk grup administrator yang terdelegasi di Direktori Aktif yang didelegasikan untuk melakukan tindakan administratif pada sistem file Anda. Jika Anda mengintegrasikan sistem file Anda dengan Microsoft AD yang AWS Dikelola, grup ini adalah Administrator AWS Delegasi FSx . Jika Anda mengintegrasikan sistem file Anda dengan pengaturan Microsoft AD yang dikelola sendiri, grup ini dapat menjadi Admin Domain. Atau bisa juga menjadi grup administrator terdelegasi kustom yang Anda tentukan saat membuat sistem file. Untuk mengubah ACLs, Anda dapat memetakan share sebagai pengguna yang merupakan anggota grup administrator yang didelegasikan.

> **Warning**
>
> Amazon FSx mengharuskan pengguna SYSTEM memiliki kontrol penuh izin NTFS ACL pada semua folder dalam sistem file Anda. Jangan mengubah izin ACL NTFS untuk pengguna ini di folder Anda. Melakukannya dapat membuat berbagi file Anda tidak dapat diakses dan mencegah pencadangan sistem file agar tidak dapat digunakan.

Tautan Terkait

- Apa itu AWS Directory Service? dalam Panduan AWS Directory Service Administrasi.
- Buat direktori Microsoft AD yang AWS Dikelola Anda di Panduan AWS Directory Service Administrasi.
- Kapan Membuat Hubungan Kepercayaan dalam Panduan Administrasi AWS Directory Service .
- Langkah 1. Menyiapkan Direktori Aktif.

Kontrol akses sistem file dengan Amazon VPC

Anda mengakses sistem FSx file Amazon Anda melalui elastic network interface. Antarmuka jaringan ini berdiam di virtual private cloud (VPC) berdasarkan layanan Amazon Virtual Private Cloud (Amazon VPC) yang Anda kaitkan dengan sistem file Anda. Anda terhubung ke sistem FSx file Amazon Anda melalui nama Domain Name Service (DNS). Nama DNS memetakan ke alamat IP privat dari antarmuka jaringan elastis dari sistem file di VPC Anda. Hanya sumber daya dalam VPC terkait, sumber daya yang terhubung dengan VPC terkait oleh AWS Direct Connect atau VPN, atau

sumber daya dalam peered yang VPCs dapat mengakses antarmuka jaringan sistem file Anda. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan Amazon VPC? dalam Panduan Pengguna Amazon VPC.

> **Warning**
>
> Anda tidak harus mengubah atau menghapus antarmuka jaringan elastis yang dikaitkan dengan sistem file Anda. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan hilangnya koneksi secara permanen antara VPC Anda dan sistem file Anda.

FSx untuk Windows File Server mendukung berbagi VPC, yang memungkinkan Anda untuk melihat, membuat, memodifikasi, dan menghapus sumber daya di subnet bersama di VPC yang dimiliki oleh akun lain. AWS Untuk informasi lebih lanjut, lihat Bekerja dengan VPCs Bersama di Panduan Pengguna Amazon VPC.

Grup keamanan Amazon VPC

Untuk lebih mengontrol lalu lintas jaringan melalui elastic network interface (s) sistem file Anda dalam VPC Anda, gunakan grup keamanan untuk membatasi akses ke sistem file Anda. Grup keamanan adalah firewall stateful yang mengendalikan lalu lintas ke dan dari antarmuka jaringan yang dikaitkan padanya. Dalam hal ini, sumber daya terkait adalah antarmuka jaringan sistem file Anda.

Untuk menggunakan grup keamanan untuk mengontrol akses ke sistem FSx file Amazon Anda, tambahkan aturan masuk dan keluar. Aturan jalur masuk mengendalikan lalu lintas yang masuk, dan aturan jalur keluar mengendalikan lalu lintas yang keluar dari sistem file Anda. Pastikan Anda memiliki aturan lalu lintas jaringan yang benar di grup keamanan untuk memetakan FSx file file sistem file Amazon Anda ke folder pada instance komputasi yang didukung.

Untuk informasi selengkapnya tentang aturan grup keamanan, lihat Aturan Grup Keamanan di Panduan EC2 Pengguna Amazon.

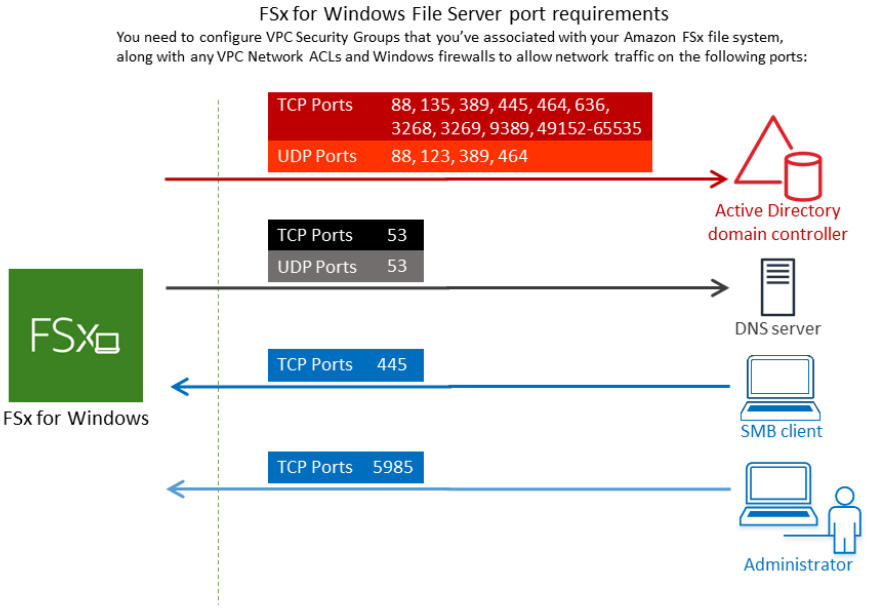
Untuk membuat grup keamanan untuk Amazon FSx

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2.
2. Di panel navigasi, pilih Security Groups (Grup Keamanan).
3. Pilih Create Security Group (Buat Grup Keamanan).
4. Tentukan nama dan deskripsi untuk grup keamanan.

5. Untuk VPC, pilih Amazon VPC yang ter-associate dengan sistem file Anda untuk membuat grup keamanan dalam VPC tersebut.

6. Tambahkan aturan berikut untuk memungkinkan lalu lintas jaringan jalur keluar pada port berikut:

   a. Untuk Grup keamanan VPC, grup keamanan default untuk Amazon VPC default Anda sudah ditambahkan ke sistem file Anda di konsol. Harap pastikan bahwa grup keamanan dan Jaringan VPC ACLs untuk subnet tempat Anda membuat sistem FSx file memungkinkan lalu lintas di port dan petunjuk yang ditunjukkan pada diagram berikut.



Tabel berikut mengidentifikasi peran masing-masing port.

Protokol	Port	Peran
TCP/UDP	53	Sistem Nama Domain (DNS)
TCP/UDP	88	Autentikasi Kerberos
TCP/UDP	464	Ubah/Atur kata sandi
TCP/UDP	389	Protokol Akses Direktori Ringan (LDAP)

Protokol	Port	Peran
UDP	123	Protokol Waktu Jaringan (NTP)
TCP	135	Lingkungan Komputasi Terdistribusi/Pemeta Titik Akhir (DCE/EPMAP)
TCP	445	Pembagian file SMB Layanan Direktori
TCP	636	Protokol Akses Direktori Ringan melalui TLS/SSL (LDAPS)
TCP	3268	Katalog Global Microsoft
TCP	3269	Katalog Global Microsoft melalui SSL
TCP	5985	WinRM 2.0 (Pengelolaan Jarak Jauh Microsoft Windows)
TCP	9389	Layanan Web Microsoft AD DS, PowerShell
TCP	49152 - 65535	Port ephemeral untuk RPC

> **Important**
>
> Mengizinkan lalu lintas keluar pada TCP port 9389 diperlukan untuk single-AZ 2 dan semua deployment sistem file Multi-AZ.

b. Pastikan bahwa peraturan lalu lintas ini juga tercermin pada firewall yang berlaku untuk masing-masing pengontrol domain AD, server DNS, klien, dan administrator. FSx FSx

> **Important**
>
> Sementara grup keamanan Amazon VPC mengharuskan port dibuka hanya ke arah lalu lintas jaringan dimulai, sebagian besar firewall Windows dan ACLs jaringan VPC memerlukan port untuk dibuka di kedua arah.

> **Note**
>
> Jika Anda memiliki situs Direktori Aktif yang ditentukan, Anda harus yakin bahwa subnet di VPC yang terkait dengan sistem file FSx Amazon Anda didefinisikan di situs Direktori Aktif, dan tidak ada konflik antara subnet di VPC Anda dan subnet di situs Anda yang lain. Anda dapat melihat dan mengubah pengaturan ini menggunakan Situs dan Layanan Direktori Aktif snap-in MMC.

> **Note**
>
> Dalam beberapa kasus, Anda mungkin telah mengubah aturan grup keamanan AWS Managed Microsoft AD dari pengaturan default. Jika demikian, pastikan grup keamanan ini memiliki aturan masuk yang diperlukan untuk mengizinkan lalu lintas dari sistem FSx file Amazon Anda. Untuk informasi selengkapnya tentang aturan jalur masuk yang diperlukan, lihat Prasyarat AWS Managed Microsoft AD dalam Panduan Administrasi AWS Directory Service .

Sekarang setelah Anda membuat grup keamanan, Anda dapat mengaitkannya dengan elastic network interface sistem FSx file Amazon Anda.

Untuk mengaitkan grup keamanan dengan sistem FSx file Amazon Anda

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Pada dasbor, pilih sistem file Anda untuk melihat detailnya.
3. Pilih tab Jaringan & Keamanan, dan pilih antarmuka jaringan sistem file Anda; misalnya, ENI-01234567890123456. Untuk sistem file Single-AZ, Anda akan melihat antarmuka jaringan tunggal. Untuk sistem file Multi-AZ, Anda akan melihat satu antarmuka jaringan di subnet Preferred dan satu di subnet Standby.
4. Untuk setiap antarmuka jaringan, pilih antarmuka jaringan dan dalam Tindakan, pilih Ubah Grup Keamanan.
5. Dalam kotak dialog Ubah Grup Keamanan, pilih grup keamanan yang akan digunakan, lalu pilih Simpan.

Melarang Akses ke Sistem File

Untuk sementara melarang akses jaringan ke sistem file Anda dari semua klien, Anda dapat menghapus semua grup keamanan yang dikaitkan dengan antarmuka jaringan elastis dari sistem file Anda dan menggantinya dengan grup yang tidak memiliki aturan jalur masuk/jalur keluar.

Jaringan VPC Amazon ACLs

Pilihan lain untuk mengamankan akses ke sistem file dalam VPC Anda adalah membuat daftar kontrol akses jaringan (ACLsjaringan). Jaringan ACLs terpisah dari grup keamanan, tetapi memiliki fungsi serupa untuk menambahkan lapisan keamanan tambahan ke sumber daya di VPC Anda. Untuk informasi selengkapnya tentang jaringan ACLs, lihat Jaringan ACLs di Panduan Pengguna Amazon VPC.

Mencatat akses pengguna akhir dengan audit akses file

Amazon FSx untuk Windows File Server mendukung audit akses pengguna akhir ke file, folder, dan berbagi file. Anda dapat memilih untuk mengirim log peristiwa audit sistem file ke AWS layanan lain yang menawarkan serangkaian fitur yang kaya. Ini termasuk memungkinkan kueri, pemrosesan, penyimpanan dan pengarsipan log, penerbitan pemberitahuan, dan tindakan pemicu untuk lebih memajukan tujuan keamanan dan kepatuhan Anda.

Untuk informasi selengkapnya tentang penggunaan audit akses file untuk mendapatkan wawasan tentang pola akses dan menerapkan pemberitahuan keamanan untuk aktivitas pengguna akhir, lihat Wawasan pola akses penyimpanan file dan Menerapkan pemberitahuan keamanan untuk aktivitas pengguna akhir.

> **Note**
>
> Audit akses file hanya didukung FSx untuk sistem file Windows dengan kapasitas throughput 32 MBps atau lebih besar. Anda dapat memodifikasi kapasitas throughput pada sistem file yang ada. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Audit akses file memungkinkan Anda merekam akses pengguna akhir atas file tunggal, folder, dan akses berbagi file berdasarkan kendali audit yang telah Anda tentukan. Kontrol audit juga dikenal sebagai daftar kontrol akses sistem NTFS ()SACLs. Jika Anda sudah memiliki kontrol audit yang

disiapkan pada data file yang ada, Anda dapat memanfaatkan audit akses file dengan membuat sistem file Amazon FSx untuk Windows File Server baru dan memigrasikan data Anda.

Amazon FSx mendukung peristiwa audit Windows berikut untuk akses file, folder, dan file share:

- Untuk akses file, akses file men-support: Semua, Melintasi folder / Jalankan file, Mencantumkan folder / Membaca data, Membaca atribut, Membuat file / Menulis data, Membuat folder / Menambahkan data, Menulis atribut, Menghapus subfolder dan file, Hapus Izin, Baca izin, Ubah izin, dan Ambil kepemilikan.
- Untuk akses berbagi file, ini mendukung: Connect to a file share.

Di seluruh akses file, folder, dan berbagi file, Amazon FSx mendukung pencatatan upaya yang berhasil (seperti pengguna dengan izin yang cukup berhasil mengakses file atau berbagi file), upaya gagal, atau keduanya.

Anda dapat mengkonfigurasi apakah Anda ingin melakukan audit akses hanya pada file dan folder, hanya pada akses berbagi file, atau keduanya. Anda juga dapat mengkonfigurasi jenis akses mana yang harus dicatat (upaya berhasil saja, upaya gagal saja, atau keduanya). Anda juga dapat menonaktifkan audit akses file kapan saja.

> **Note**
>
> Pengauditan akses file mencatat data akses pengguna akhir hanya sejak diaktifkan. Artinya, audit akses file tidak menghasilkan log peristiwa audit dari file pengguna akhir, folder, dan aktivitas akses berbagi file yang terjadi sebelum audit akses file diaktifkan.

Tingkat maksimum event audit akses yang di-support adalah 5.000 event per detik. Akses event audit tidak dibuat untuk operasi baca dan tulis setiap file, tetapi dibuat satu kali per operasi metadata file, seperti ketika pengguna membuat, membuka, atau menghapus file.

Topik

Tujuan log event audit

Saat mengaktifkan audit akses file, Anda harus mengonfigurasi AWS layanan tempat Amazon FSx mengirimkan log peristiwa audit. Anda dapat mengirim log peristiwa audit ke aliran CloudWatch log Amazon Logs di grup CloudWatch log Log atau aliran pengiriman Amazon Data Firehose. Anda memilih tujuan log peristiwa audit baik saat membuat sistem file Amazon FSx untuk Windows File Server, atau kapan saja setelahnya dengan memperbarui sistem file yang ada. Untuk informasi selengkapnya, lihat Mengelola audit akses file.

Berikut ini adalah beberapa rekomendasi yang dapat membantu Anda memutuskan tujuan audit event log yang mana yang akan dipilih:

- Pilih CloudWatch Log jika Anda ingin menyimpan, melihat, dan mencari log peristiwa audit di CloudWatch konsol Amazon, jalankan kueri di CloudWatch log menggunakan Wawasan Log, dan memicu CloudWatch alarm atau fungsi Lambda.
- Pilih Amazon Data Firehose jika Anda ingin terus melakukan streaming peristiwa ke penyimpanan di Amazon S3, ke database di Amazon Redshift, ke OpenSearch Amazon Service, atau ke solusi Mitra seperti Splunk atau Datadog AWS untuk analisis lebih lanjut.

Secara default, Amazon FSx akan membuat dan menggunakan grup CloudWatch log Log default di akun Anda sebagai tujuan log peristiwa audit. Jika Anda ingin menggunakan grup CloudWatch log Log kustom atau menggunakan Firehose sebagai tujuan log peristiwa audit, berikut adalah persyaratan untuk nama dan lokasi tujuan log peristiwa audit:

- Nama grup CloudWatch log Log harus dimulai dengan `/aws/fsx/` awalan. Jika Anda tidak memiliki grup CloudWatch log Log saat membuat atau memperbarui sistem file di konsol, Amazon FSx dapat membuat dan menggunakan aliran log default di grup CloudWatch `/aws/fsx/windows` log Log. Jika Anda tidak ingin menggunakan grup log default, UI konfigurasi memungkinkan Anda membuat grup CloudWatch log Log saat membuat atau memperbarui sistem file di konsol.
- Nama aliran pengiriman Firehose harus dimulai dengan awalan. `aws-fsx-` Jika Anda tidak memiliki aliran pengiriman Firehose yang ada, Anda dapat membuatnya saat membuat atau memperbarui sistem file di konsol.
- Aliran pengiriman Firehose harus dikonfigurasi untuk digunakan `Direct PUT` sebagai sumbernya. Anda tidak dapat menggunakan aliran data Kinesis yang ada sebagai sumber data untuk aliran pengiriman Anda.

- Tujuan (baik grup CloudWatch log Log atau aliran pengiriman Firehose) harus berada di AWS partisi yang sama Wilayah AWS, dan Akun AWS sebagai sistem FSx file Amazon Anda.

Anda dapat mengubah tujuan log peristiwa audit kapan saja (misalnya, dari CloudWatch Log ke Firehose). Ketika Anda melakukannya, log event audit yang baru dikirimkan hanya ke tujuan yang baru.

Upaya terbaik pengiriman log event audit

Biasanya, catatan log peristiwa audit dikirim ke tujuan dalam hitungan menit, tetapi terkadang bisa memakan waktu lebih lama. Pada kesempatan yang sangat langka, catatan log event audit mungkin hilang. Jika kasus penggunaan Anda membutuhkan semantik khusus (misalnya, pastikan bahwa tidak ada event audit yang terlewatkan), sebaiknya Anda mempertimbangkan event yang terlewat saat merancang alur kerja Anda. Anda dapat melakukan audit untuk event yang terlewat dengan memindai struktur file dan folder pada sistem file Anda.

Memigrasi kendali audit Anda

Jika Anda memiliki kontrol audit (SACLs) yang sudah diatur pada data file yang ada, Anda dapat membuat sistem FSx file Amazon dan memigrasikan data ke sistem file baru Anda. Sebaiknya gunakan AWS DataSync untuk mentransfer data dan yang SACLs terkait dengan sistem FSx file Amazon Anda. Sebagai solusi alternatif, Anda bisa menggunakan Robocopy (Salinan File Robust). Untuk informasi selengkapnya, lihat Migrasi penyimpanan file yang ada ke Amazon FSx.

Melihat log event

Anda dapat melihat log peristiwa audit setelah FSx Amazon mulai memancarkannya. Di mana dan bagaimana Anda melihat log tergantung pada tujuan log event audit:

- Anda dapat melihat CloudWatch log Log dengan membuka CloudWatch konsol dan memilih grup log dan aliran log tempat log peristiwa audit Anda dikirim. Untuk informasi selengkapnya, lihat Melihat data log yang dikirim ke CloudWatch Log di Panduan Pengguna CloudWatch Log Amazon.

  Anda dapat menggunakan Wawasan CloudWatch Log untuk mencari dan menganalisis data log secara interaktif. Untuk informasi selengkapnya, lihat Menganalisis Data CloudWatch Log dengan Wawasan Log, di Panduan Pengguna CloudWatch Log Amazon.

  Anda juga dapat mengekspor log event audit ke Amazon S3. Untuk informasi selengkapnya, lihat Mengekspor Data Log ke Amazon S3, juga di Panduan Pengguna CloudWatch Amazon Logs.

- Anda tidak dapat melihat log peristiwa audit di Firehose. Namun, Anda dapat mengonfigurasi Firehose untuk meneruskan log ke tujuan yang dapat Anda baca. Tujuannya meliputi Amazon S3, Amazon Redshift, OpenSearch Amazon Service, dan solusi mitra seperti Splunk dan Datadog, Untuk informasi selengkapnya, lihat Memilih tujuan di Panduan Pengembang Amazon Data Firehose.

Audit bidang event

Bagian ini menyediakan deskripsi informasi pada log event audit dan contoh event audit.

Berikut ini adalah deskripsi dari bidang yang menonjol dalam event audit Windows.

- EventID mengacu pada ID log acara event Windows yang ditentukan Windows. Lihat dokumentasi Microsoft untuk informasi tentang event sistem file dan event berbagi file.
- SubjectUserNamemengacu pada pengguna yang melakukan akses.
- ObjectNamemengacu pada file target, folder, atau berbagi file yang diakses.
- ShareNametersedia untuk acara yang dihasilkan untuk akses berbagi file. Misalnya, `EventID 5140` dibuat ketika objek berbagi jaringan diakses.
- IpAddressmengacu pada klien yang memulai acara untuk acara berbagi file.
- Kata Kunci, ketika tersedia, mengacu pada akses file apakah berhasil atau gagal. Untuk akses yang berhasil, nilainya adalah `0x8020000000000000`. Untuk akses yang gagal, nilainya adalah `0x8010000000000000`.
- TimeCreated SystemTimemengacu pada waktu peristiwa dihasilkan dalam sistem dan ditunjukkan dalam format <YYYY-MM-:MM : SS.S>Z. DDThh
- Komputer mengacu pada nama DNS dari sistem file Windows Remote PowerShell Endpoint dan dapat digunakan untuk mengidentifikasi sistem file.
- AccessMask, bila tersedia, mengacu pada jenis akses file yang dilakukan (misalnya, ReadData, WriteData).
- AccessListmengacu pada akses yang diminta atau diberikan ke Objek. Untuk detailnya, lihat tabel di bawah ini dan dokumentasi Microsoft (seperti dalam Event 4556).

Jenis Akses	Mask Akses	Nilai
Baca Data atau Cantumkan Direktori	0x1	%%4416
Menulis Data atau Tambah File	0x2	%%4417
Menambahkan Data atau Tambah Subdirektori	0x4	%%4418
Baca Atribut yang Diperluas	0x8	%%4419
Tulis Atribut yang Diperluas	0x10	%%4420
Eksekusi/Lewati	0x20	%%4421
Hapus Anak	0x40	%%4422
Baca Atribut	0x80	%%4423
Tulis Atribut	0x100	%%4424
Hapus	0x10000	%%1537
Baca ACL	0x20000	%%1538
Tulis ACL	0x40000	%%1539
Pemilik tulis	0x80000	%%1540
Sinkronisasi	0x100000	%%1541
Akses Keamanan ACL	0x1000000	%%1542

Berikut ini adalah beberapa peristiwa penting dengan contoh-contoh. Perhatikan bahwa XML diformat agar dapat dibaca.

ID Event 4660 tercatat ketika ada sebuah objek yang dihapus.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

ID Event 4659 tercatat ketika ada permintaan untuk menghapus file.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
```

```
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

ID Event 4663 tercatat ketika ada operasi tertentu dilakukan pada objek tersebut. Contoh berikut menunjukkan pembacaan data dari sebuah file, yang dapat ditafsirkan dari `AccessList %%4416`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

Contoh berikut menunjukkan penulisan/penambahan data dari sebuah file, yang dapat ditafsirkan dari `AccessList %%4417`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
```

```
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

ID Event 4656 mengindikasikan bahwa akses tertentu diminta untuk sebuah objek. Dalam contoh berikut, permintaan Baca dimulai ke ObjectName “permtest” dan merupakan upaya yang gagal, seperti yang terlihat pada nilai Kata Kunci. `0x8010000000000000`

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
```

```
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

ID Event 4670 tercatat ketika izin untuk sebuah objek berubah. Contoh berikut menunjukkan bahwa pengguna “admin” memodifikasi izin pada “permtest” untuk menambahkan izin ke SID ObjectName “S-1-5-21-658495921-4185342820-3824891517-1113". Lihat dokumentasi Microsoft untuk informasi lebih lanjut tentang cara menafsirkan izin.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

ID Event 5140 tercatat setiap kali akses berbagi file diakses.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
```

```
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

ID Event 5145 tercatat ketika akses ditolak pada tingkat berbagi file. Contoh berikut menunjukkan akses ke ShareName “demoshare01" ditolak.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

Jika Anda menggunakan Wawasan CloudWatch Log untuk mencari data log Anda, Anda dapat menjalankan kueri pada bidang peristiwa, seperti yang ditunjukkan oleh contoh berikut:

- Untuk melakukan kueri untuk ID event tertentu:

```
fields @message
   | filter @message like /4660/
```

- Untuk kueri semua event yang cocok dengan nama file tertentu:

```
fields @message
   | filter @message like /event.txt/
```

Untuk informasi selengkapnya tentang bahasa kueri Wawasan CloudWatch Log, lihat Menganalisis Data CloudWatch Log dengan Wawasan Log, di Panduan Pengguna CloudWatch Log Amazon.

Mengatur kontrol audit file dan folder

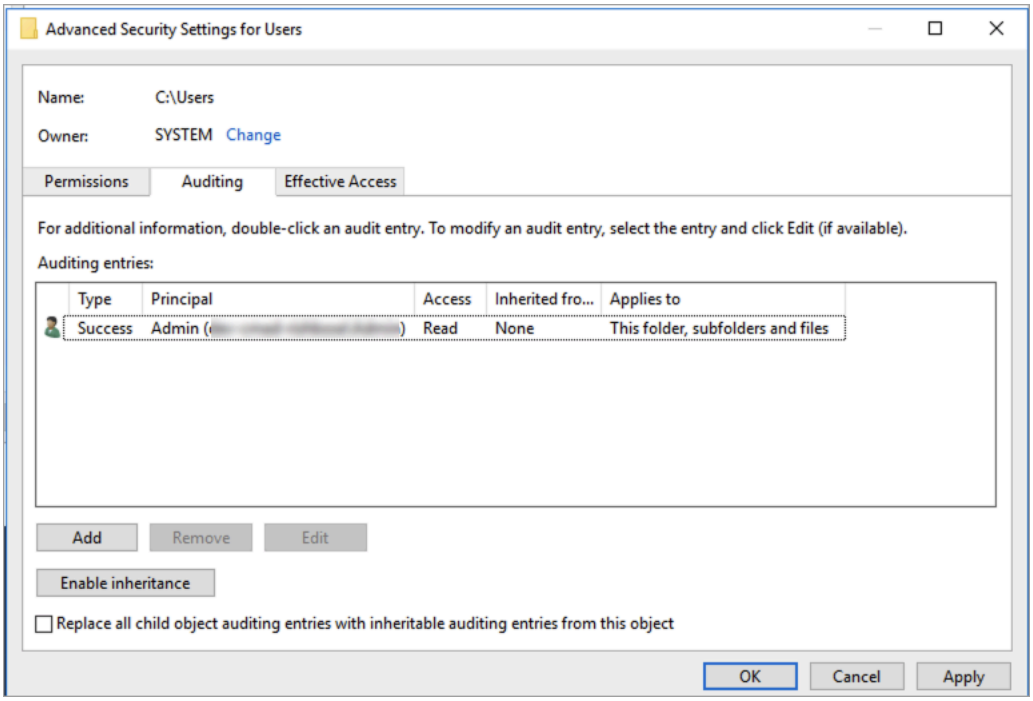
Anda perlu mengatur kendali audit pada file dan folder yang ingin Anda audit untuk upaya akses pengguna. Kontrol audit juga dikenal sebagai daftar kontrol akses sistem NTFS ()SACLs.

Anda mengonfigurasi kontrol audit menggunakan antarmuka GUI asli Windows atau secara terprogram menggunakan perintah Windows. PowerShell Jika pewarisan diaktifkan, Anda pada umumnya perlu mengatur kendali audit hanya pada folder tingkat atas yang log-nya hendak diakses.

Menggunakan Windows GUI untuk mengatur akses audit

Untuk menggunakan GUI untuk mengatur kendali audit pada file dan folder Anda, gunakan Windows File Explorer. Pada file atau folder tertentu, buka Windows File Explorer dan pilih tab Properties > Keamanan > Lanjutan > Audit.

Contoh kendali audit berikut mengaudit event yang berhasil atas sebuah folder. Sebuah entri log event Windows akan dirilis setiap kali bukaan terbuka setelah pengguna Admin berhasil membaca.



Bidang isian Jenis menunjukkan tindakan apa yang ingin Anda audit. Atur bidang isian ini menjadi Berhasil untuk men-gaudit upaya yang berhasil, Gagal untuk mengaudit upaya yang gagal, atau Semua untuk meng-audit semua upaya baik yang berhasil maupun yang gagal.

Untuk informasi lebih lanjut tentang bidang isian entri audit, lihat Menerapkan kebijakan audit dasar pada file atau folder dalam dokumentasi Microsoft.

Menggunakan PowerShell perintah untuk mengatur akses audit

Anda dapat menggunakan perintah `Set-Acl` Microsoft Windows untuk mengatur audit SACL pada setiap file atau folder. Untuk informasi tentang perintah ini, lihat dokumentasi Atur-Acl Microsoft.

Berikut ini adalah contoh menggunakan serangkaian PowerShell perintah dan variabel untuk mengatur akses audit untuk upaya yang berhasil. Anda dapat menyesuaikan contoh perintah ini agar sesuai dengan kebutuhan pada sistem file Anda.

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List

$AuditUser = "TESTDOMAIN\TestUser"
```

```
$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

Mengelola audit akses file

Anda dapat mengaktifkan audit akses file saat membuat sistem file Amazon FSx untuk Windows File Server baru. Audit akses file dimatikan secara default saat Anda membuat sistem file dari FSx konsol Amazon.

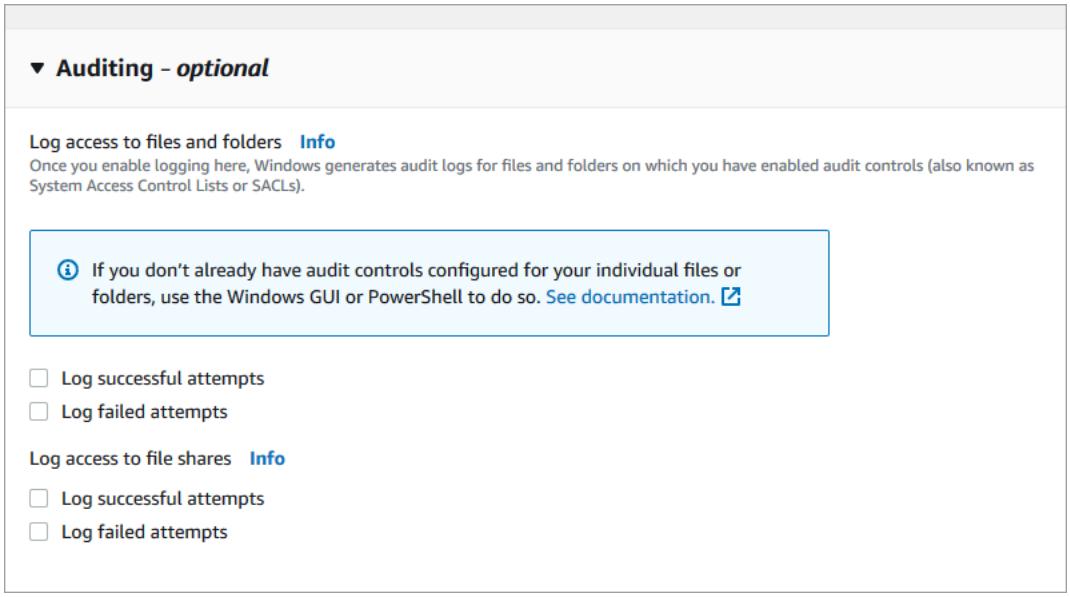
Pada sistem file yang ada yang proses audit aksesnya diaktifkan, Anda dapat mengubah pengaturan audit akses file, termasuk mengubah jenis upaya akses untuk file dan akses berbagi file, dan tujuan log event audit. Anda dapat melakukan tugas-tugas ini menggunakan FSx konsol Amazon, AWS CLI, atau API.

> **Note**
>
> Audit akses file hanya didukung di Amazon FSx untuk sistem file Windows File Server dengan kapasitas throughput 32 MBps atau lebih besar. Anda tidak dapat membuat atau memperbarui sistem file dengan kapasitas throughput kurang dari 32 MBps jika audit akses file diaktifkan. Anda dapat mengubah kapasitas throughput setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Untuk mengaktifkan audit akses file saat membuat sistem file (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Ikuti prosedur untuk membuat sistem file baru yang dijelaskan di Langkah 5. Buat sistem file Anda di bagian Memulai.

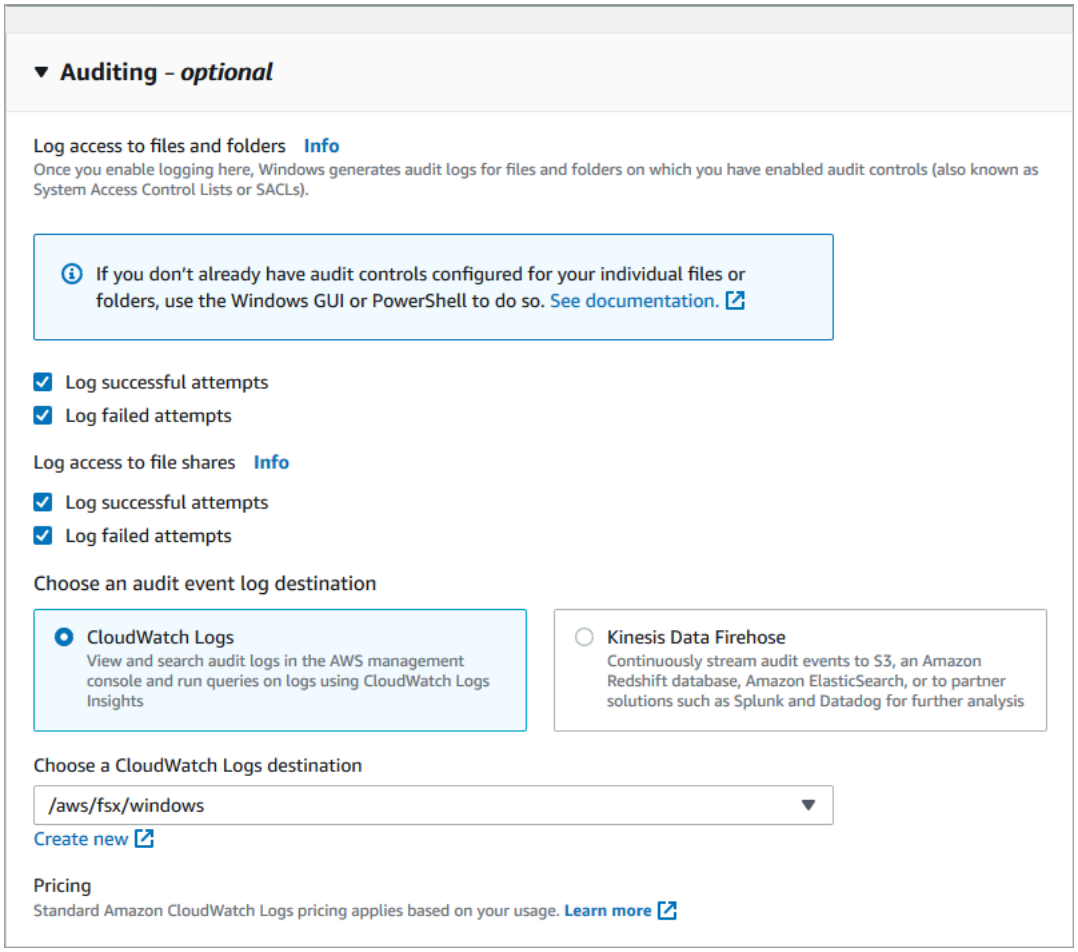
3. Buka bagian Audit - opsional. Audit akses file dinonaktifkan secara default.



4. Untuk mengaktifkan dan mengonfigurasi audit akses file, lakukan hal berikut.

   - Untuk Akses log ke file dan folder, pilih catatan upaya yang berhasil dan/atau yang gagal. Pencatatan akan dinonaktifkan untuk file dan folder jika Anda tidak membuat pilihan.
   - Untuk Akses log ke berbagi file, pilih pencatatan upaya yang berhasil dan/atau yang gagal. Pencatatan dinonaktifkan untuk fitur berbagi file jika Anda tidak membuat pilihan.
   - Untuk Pilih tujuan log peristiwa audit, pilih CloudWatch Log atau Firehose. Lalu pilih log yang ada atau aliran pengiriman atau buat yang baru. Untuk CloudWatch Log, Amazon FSx dapat membuat dan menggunakan aliran log default di grup CloudWatch `/aws/fsx/windows` log Log.

   Berikut ini adalah contoh dari konfigurasi audit akses file yang akan mengaudit upaya akses para pengguna akhir yang berhasil dan gagal atas akses file, folder, dan akses berbagi file. Log peristiwa audit akan dikirim ke tujuan grup CloudWatch `/aws/fsx/windows` log Log default.



5. Lanjutkan dengan bagian berikutnya dari wizard pembuatan sistem file.

Ketika sistem file Tersedia, fitur audit akses file diaktifkan.

Untuk mengaktifkan audit akses file saat membuat sistem file (CLI)

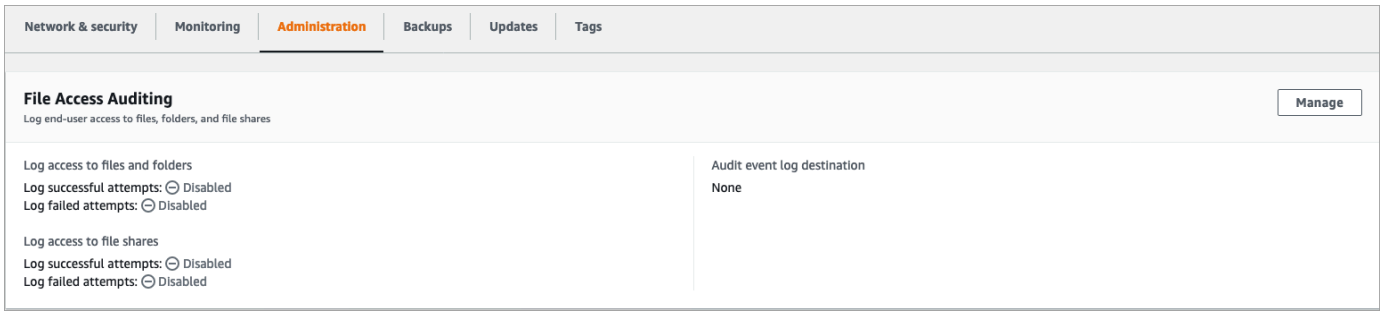
1. Saat membuat sistem file baru, gunakan `AuditLogConfiguration` properti dengan operasi CreateFileSystemAPI untuk mengaktifkan audit akses file untuk sistem file baru.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

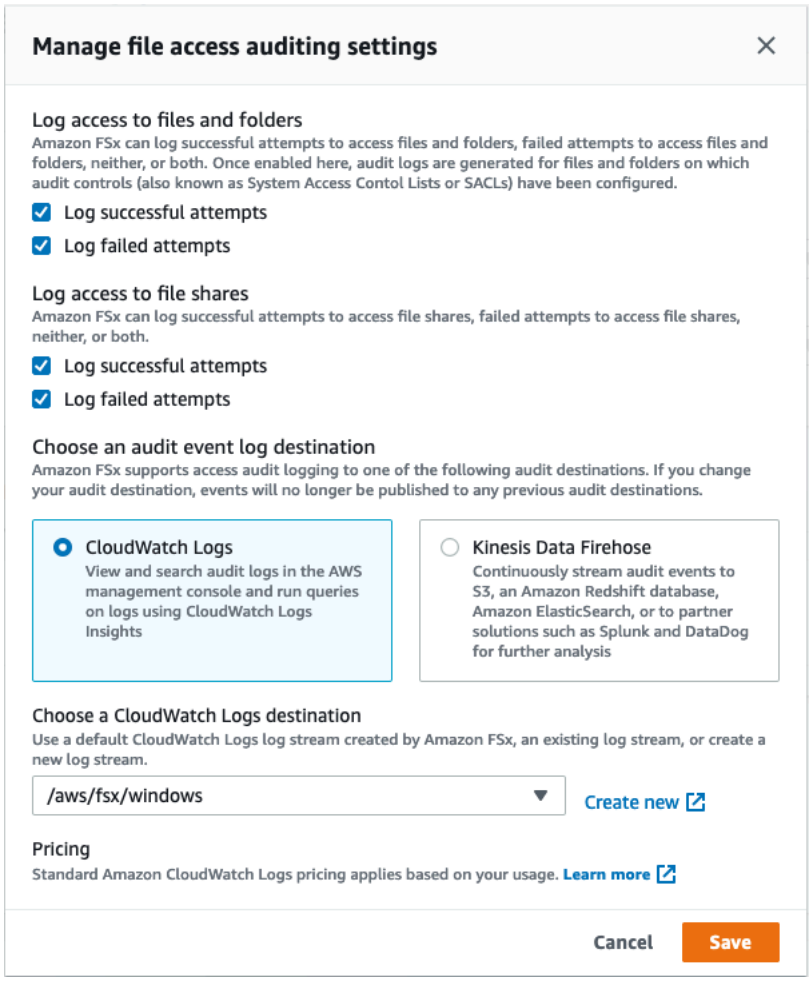
2. Ketika sistem file Tersedia, fitur audit akses file diaktifkan.

Untuk mengubah konfigurasi audit akses file (konsol)

1. Buka FSx konsol Amazon di https://console.aws.amazon.com/fsx/.
2. Arahkan ke Sistem file, dan pilih sistem file Windows yang ingin Anda kelola audit akses file-nya.
3. Pilih tab Administrasi.
4. Pada panel Audit Akses File, pilih Kelola.



5. Pada kotak dialog Mengelola pengaturan audit akses file, ubah pengaturan ke yang diinginkan.



- Untuk Akses log ke file dan folder, pilih catatan upaya yang berhasil dan/atau yang gagal. Pencatatan akan dinonaktifkan untuk file dan folder jika Anda tidak membuat pilihan.
- Untuk Akses log ke berbagi file, pilih pencatatan upaya yang berhasil dan/atau yang gagal. Pencatatan dinonaktifkan untuk fitur berbagi file jika Anda tidak membuat pilihan.
- Untuk Pilih tujuan log peristiwa audit, pilih CloudWatch Log atau Firehose. Lalu pilih log atau aliran pengiriman yang ada atau buat yang baru.

6. Pilih Simpan.

Untuk mengubah konfigurasi audit akses file (CLI)

- Gunakan perintah CLI `update-file-system` atau operasi API `UpdateFileSystem` yang setara.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
```

```
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

Manajemen identitas dan akses untuk Amazon FSx untuk Windows File Server

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 diotorisasi (memiliki izin) untuk digunakan FSx untuk sumber daya Windows File Server. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan FSx untuk Windows File Server.

Pengguna layanan - Jika Anda menggunakan layanan FSx untuk Windows File Server untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda

butuhkan. Saat Anda menggunakan lebih banyak FSx fitur Windows File Server untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur FSx untuk Windows File Server, lihatMemecahkan masalah Amazon FSx untuk identitas dan akses Server File Windows.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Windows File Server di perusahaan Anda, Anda mungkin memiliki akses penuh FSx untuk Windows File Server. FSx Tugas Anda adalah menentukan fitur dan sumber daya Windows File Server mana FSx yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari selengkapnya tentang bagaimana perusahaan Anda dapat menggunakan IAM FSx untuk Windows File Server, lihatBagaimana Amazon FSx untuk Windows File Server bekerja dengan IAM.

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke FSx Windows File Server. Untuk melihat FSx contoh kebijakan berbasis identitas Windows File Server yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Amazon FSx untuk Windows File Server

Mengautentikasi dengan identitas

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

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara

kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Autentikasi multi-faktor AWS di IAM dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

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

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI

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

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Daftar kontrol akses (ACLs)

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

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

Jenis-jenis kebijakan lain

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

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda

dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon FSx untuk Windows File Server bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke FSx Windows File Server, pelajari fitur IAM apa yang tersedia untuk digunakan FSx untuk Windows File Server.

Fitur IAM yang dapat Anda gunakan dengan Amazon FSx untuk Windows File Server

Fitur IAM	FSx dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Teruskan sesi akses	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

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

Kebijakan berbasis identitas untuk FSx

Mendukung kebijakan berbasis identitas: Ya

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

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

Contoh kebijakan berbasis identitas untuk FSx

Untuk melihat contoh kebijakan berbasis identitas Windows File Server, lihat. FSx Contoh kebijakan berbasis identitas untuk Amazon FSx untuk Windows File Server

Kebijakan berbasis sumber daya dalam FSx

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun

yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk FSx

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar FSx tindakan, lihat Tindakan yang ditentukan oleh Amazon FSx untuk Windows File Server di Referensi Otorisasi Layanan.

Tindakan kebijakan FSx menggunakan awalan berikut sebelum tindakan:

```
fsx
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

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

Untuk melihat contoh kebijakan berbasis identitas Windows File Server, lihat. FSx Contoh kebijakan berbasis identitas untuk Amazon FSx untuk Windows File Server

Sumber daya kebijakan untuk FSx

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya dan jenis FSx sumber daya ARNs, lihat Sumber daya yang ditentukan oleh Amazon FSx untuk Windows File Server di Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon FSx untuk Windows File Server.

Untuk melihat contoh kebijakan berbasis identitas Windows File Server, lihat. FSx Contoh kebijakan berbasis identitas untuk Amazon FSx untuk Windows File Server

Kunci kondisi kebijakan untuk FSx

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi

AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci FSx kondisi, lihat Kunci kondisi untuk Amazon FSx untuk Windows File Server di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon FSx untuk Windows File Server.

Untuk melihat contoh kebijakan berbasis identitas Windows File Server, lihat. FSx Contoh kebijakan berbasis identitas untuk Amazon FSx untuk Windows File Server

ACLs di FSx

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 FSx

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

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

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

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

Menggunakan kredensi sementara dengan FSx

Mendukung kredensial sementara: Ya

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

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk FSx

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan

izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk FSx

Mendukung peran layanan: Tidak

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 FSx fungsionalitas. Edit peran layanan hanya jika FSx memberikan panduan untuk melakukannya.

Peran terkait layanan untuk FSx

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 membuat atau mengelola FSx peran terkait layanan Windows File Server, lihat. Menggunakan peran terkait layanan FSx untuk Windows File Server

Contoh kebijakan berbasis identitas untuk Amazon FSx untuk Windows File Server

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi FSx sumber daya Windows File Server. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka

perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh FSx, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon FSx untuk Windows File Server dalam Referensi Otorisasi Layanan.

Topik

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

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus FSx sumber daya Windows File Server di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber

daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol FSx

Untuk mengakses konsol Amazon FSx untuk Windows File Server, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk daftar dan melihat rincian tentang sumber daya Windows File Server FSx untuk 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 FSx konsol, lampirkan juga kebijakan FSx `AmazonFSxConsoleReadOnlyAccess` 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": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk Amazon FSx untuk OpenZFS

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

Amazon FSx ServiceRolePolicy

Memungkinkan Amazon FSx mengelola AWS sumber daya atas nama Anda. Lihat Menggunakan peran terkait layanan FSx untuk Windows File Server untuk mempelajari selengkapnya.

AWS kebijakan terkelola: Amazon FSx DeleteServiceLinkedRoleAccess

Anda tidak dapat melampirkan `AmazonFSxDeleteServiceLinkedRoleAccess` ke entitas IAM Anda. Kebijakan ini ditautkan ke layanan dan hanya digunakan dengan peran terkait layanan untuk layanan tersebut. Anda tidak dapat melampirkan, melepaskan, memodifikasi, atau menghapus kebijakan ini. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan FSx untuk Windows File Server.

Kebijakan ini memberikan izin administratif yang memungkinkan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3, yang hanya digunakan oleh Amazon FSx untuk Lustre.

Detail izin

Kebijakan ini mencakup izin `iam` untuk mengizinkan Amazon FSx melihat, menghapus, dan melihat status penghapusan untuk akses Peran Tertaut FSx Layanan untuk Amazon S3.

Untuk melihat izin kebijakan ini, lihat Amazon FSx DeleteServiceLinkedRoleAccess di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Amazon FSx FullAccess

Anda dapat melampirkan Amazon FSx FullAccess ke entitas IAM Anda. Amazon FSx juga melampirkan kebijakan ini ke peran layanan yang memungkinkan Amazon FSx melakukan tindakan atas nama Anda.

Menyediakan akses penuh ke Amazon FSx dan akses ke AWS layanan terkait.

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx`— Memungkinkan kepala sekolah akses penuh untuk melakukan semua FSx tindakan Amazon, kecuali untuk. `BypassSnaplockEnterpriseRetention`
- `ds`— Memungkinkan kepala sekolah untuk melihat informasi tentang direktori. AWS Directory Service
- `ec2`
  - Memungkinkan prinsipal untuk membuat tag di bawah kondisi yang ditentukan.
  - Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
- `iam`— Memungkinkan prinsip untuk membuat peran terkait FSx layanan Amazon atas nama pengguna. Ini diperlukan agar Amazon FSx dapat mengelola AWS sumber daya atas nama pengguna.
- `firehose`— Memungkinkan kepala sekolah untuk menulis catatan ke Amazon Data Firehose. Ini diperlukan agar pengguna dapat memantau FSx akses sistem file Windows File Server dengan mengirimkan log akses audit ke Firehose.
- `logs` — Mengizinkan prinsipal untuk membuat grup log, aliran log, dan menulis peristiwa untuk aliran log. Ini diperlukan agar pengguna dapat memantau FSx akses sistem file Windows File Server dengan mengirimkan log akses audit ke CloudWatch Log.

Untuk melihat izin kebijakan ini, lihat Amazon FSx FullAccess di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Amazon FSx ConsoleFullAccess

Anda dapat melampirkan kebijakan `AmazonFSxConsoleFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh ke Amazon FSx dan akses ke AWS layanan terkait melalui. AWS Management Console

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx`— Memungkinkan kepala sekolah untuk melakukan semua tindakan di konsol FSx manajemen Amazon, kecuali untuk. `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Memungkinkan kepala sekolah untuk melihat CloudWatch Alarm dan metrik di konsol manajemen Amazon. FSx
- `ds`— Memungkinkan kepala sekolah untuk daftar informasi tentang direktori. AWS Directory Service
- `ec2`
  - Memungkinkan prinsipal untuk membuat tag pada tabel rute, daftar antarmuka jaringan, tabel rute, grup keamanan, subnet dan VPC yang terkait dengan sistem file Amazon. FSx
  - Memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
  - Memungkinkan prinsipal untuk melihat antarmuka jaringan elastis yang terkait dengan sistem file Amazon. FSx
- `kms`— Memungkinkan kepala sekolah untuk daftar alias untuk kunci. AWS Key Management Service
- `s3` – Mengizinkan prinsipal utama untuk mendaftar beberapa atau semua objek dalam bucket Amazon S3 (hingga 1000).
- `iam`Memberikan izin untuk membuat peran terkait layanan yang memungkinkan Amazon FSx melakukan tindakan atas nama pengguna.

Untuk melihat izin kebijakan ini, lihat Amazon FSx ConsoleFullAccess di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Amazon FSx ConsoleReadOnlyAccess

Anda dapat melampirkan kebijakan `AmazonFSxConsoleReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca ke FSx Amazon dan layanan AWS terkait sehingga pengguna dapat melihat informasi tentang layanan ini di. AWS Management Console

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx`— Memungkinkan kepala sekolah untuk melihat informasi tentang sistem FSx file Amazon, termasuk semua tag, di Konsol Manajemen Amazon FSx .
- `cloudwatch`— Memungkinkan kepala sekolah untuk melihat CloudWatch Alarm dan metrik di Amazon Management Console. FSx
- `ds`— Memungkinkan kepala sekolah untuk melihat informasi tentang AWS Directory Service direktori di Amazon FSx Management Console.
- `ec2`
  - Memungkinkan prinsipal untuk melihat antarmuka jaringan, grup keamanan, subnet, dan VPC yang terkait dengan sistem FSx file Amazon di Amazon Management Console. FSx
  - Memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
  - Memungkinkan prinsipal untuk melihat antarmuka jaringan elastis yang terkait dengan sistem file Amazon. FSx
- `kms`— Memungkinkan kepala sekolah untuk melihat alias untuk kunci AWS Key Management Service di Konsol Manajemen Amazon. FSx
- `log`— Memungkinkan kepala sekolah untuk menggambarkan grup CloudWatch log Amazon Log yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file Windows File Server. FSx
- `firehose`— Memungkinkan kepala sekolah untuk menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file Windows File Server. FSx

Untuk melihat izin kebijakan ini, lihat Amazon FSx ConsoleReadOnlyAccess di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Amazon FSx ReadOnlyAccess

Anda dapat melampirkan kebijakan `AmazonFSxReadOnlyAccess` ke identitas IAM Anda.

- `fsx`— Memungkinkan kepala sekolah untuk melihat informasi tentang sistem FSx file Amazon, termasuk semua tag, di Konsol Manajemen Amazon FSx .
- `ec2`— Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.

Untuk melihat izin kebijakan ini, lihat Amazon FSx ReadOnlyAccess di Panduan Referensi Kebijakan AWS Terkelola.

Amazon FSx memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon FSx sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Amazon FSx Riwayat dokumen.

Perubahan	Deskripsi	Tanggal
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:CreateAndAttachS3AccessPoint` yang memungkinkan prinsipal untuk membuat S3 dan melampirkannya ke volume. FSx	April 14, 2025
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:DescribeS3AccessPointAttachments` yang memungkinkan prinsipal untuk mencantumkan semua S3 dalam a Akun AWS Wilayah AWS	April 14, 2025

Perubahan	Deskripsi	Tanggal
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:UpdateS3AccessPointAttachments` yang memungkinkan prinsipal untuk memodifikasi S3 yang ada.	April 14, 2025
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:DetachAndDeleteS3AccessPoint` yang memungkinkan prinsipal untuk menghapus S3.	April 14, 2025
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:CreateAndAttachS3AccessPoint` yang memungkinkan prinsipal untuk membuat S3 dan melampirkannya ke volume. FSx	April 14, 2025
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:DescribeS3AccessPointAttachments` yang memungkinkan prinsipal untuk mencantumkan semua S3 dalam a Akun AWS Wilayah AWS	April 14, 2025

Perubahan	Deskripsi	Tanggal
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:UpdateS3AccessPointAttachments` yang memungkinkan prinsipal untuk memodifikasi S3 yang ada.	April 14, 2025
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `fsx:DetachAndDeleteS3AccessPoint` yang memungkinkan prinsipal untuk menghapus S3.	April 14, 2025
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:DescribeNetworkInterfaces` yang memungkinkan prinsipal untuk melihat antarmuka jaringan elastis yang terkait dengan sistem file mereka.	Februari 25, 2025
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:DescribeNetworkInterfaces` yang memungkinkan prinsipal untuk melihat antarmuka jaringan elastis yang terkait dengan sistem file mereka.	Februari 07, 2025

Perubahan	Deskripsi	Tanggal
Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024
Amazon FSx ReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024

Perubahan	Deskripsi	Tanggal
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, `ec2:GetSecurityGroupsForVpc` yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi data lintas wilayah dan lintas akun FSx untuk sistem file OpenZFS.	20 Desember 2023
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi data lintas wilayah dan lintas akun FSx untuk sistem file OpenZFS.	20 Desember 2023

Perubahan	Deskripsi	Tanggal
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi volume sesuai permintaan FSx untuk sistem file OpenZFS.	26 November 2023
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi volume sesuai permintaan FSx untuk sistem file OpenZFS.	26 November 2023
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat, mengaktifkan, dan menonaktifkan dukungan VPC bersama FSx untuk sistem file Multi-AZ ONTAP.	14 November 2023
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat, mengaktifkan, dan menonaktifkan dukungan VPC bersama FSx untuk sistem file Multi-AZ ONTAP.	14 November 2023
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon mengelola konfigurasi jaringan FSx untuk sistem file Multi-AZ OpenZFS. FSx	9 Agustus 2023

Perubahan	Deskripsi	Tanggal
AWS kebijakan terkelola : Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx memodifikasi `cloudwatch:PutMetricData` izin yang ada sehingga Amazon FSx menerbitkan CloudWatch metrik ke namespace. `AWS/FSx`	Juli 24, 2023
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus `fsx:*` izin dan menambahkan `fsx` tindakan tertentu.	13 Juli 2023
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus `fsx:*` izin dan menambahkan `fsx` tindakan tertentu.	13 Juli 2023
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat metrik kinerja yang ditingkatkan dan tindakan yang disarankan FSx untuk sistem file Windows File Server di konsol Amazon FSx .	21 September 2022
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat metrik kinerja yang ditingkatkan dan tindakan yang disarankan FSx untuk sistem file Windows File Server di konsol Amazon FSx .	21 September 2022

Perubahan	Deskripsi	Tanggal
Amazon FSx ReadOnlyAccess - Memulai kebijakan pelacakan	Kebijakan ini memberikan akses hanya-baca ke semua FSx sumber daya Amazon dan tag apa pun yang terkait dengannya.	4 Februari 2022
Amazon FSx DeleteServiceLinkedRoleAccess - Memulai kebijakan pelacakan	Kebijakan ini memberikan izin administratif yang memungkinkan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3.	7 Januari 2022
Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon mengelola konfigurasi jaringan FSx untuk Amazon FSx untuk sistem file NetApp ONTAP.	2 September 2021
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx membuat tag pada tabel EC2 rute untuk panggilan bawah cakupan.	2 September 2021
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon membuat Amazon FSx FSx untuk sistem file Multi-AZ NetApp ONTAP.	2 September 2021
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx membuat tag pada tabel EC2 rute untuk panggilan bawah cakupan.	2 September 2021

Perubahan	Deskripsi	Tanggal
Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mendeskripsikan dan menulis ke aliran CloudWatch log Log. Ini diperlukan agar pengguna dapat melihat log audit akses file FSx untuk sistem file Windows File Server menggunakan CloudWatch Log.	8 Juni 2021
Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mendeskripsikan dan menulis ke aliran pengiriman Amazon Data Firehose. Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file Windows File Server menggunakan Amazon Data Firehose. FSx	8 Juni 2021

Perubahan	Deskripsi	Tanggal
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan dan membuat grup log Log, aliran CloudWatch log, dan menulis peristiwa ke aliran log. Ini diperlukan agar prinsipal dapat melihat log audit akses file FSx untuk sistem file Windows File Server menggunakan Log. CloudWatch	8 Juni 2021
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan dan menulis catatan ke Amazon Data Firehose. Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file Windows File Server menggunakan Amazon Data Firehose. FSx	8 Juni 2021

Perubahan	Deskripsi	Tanggal
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan grup CloudWatch log Amazon Logs yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar kepala sekolah dapat memilih grup CloudWatch log Log yang ada saat mengonfigurasi audit akses file untuk sistem file Windows File FSx Server.	8 Juni 2021
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat memilih aliran pengiriman Firehose yang ada saat mengonfigurasi audit akses file untuk sistem file Windows File Server. FSx	8 Juni 2021

Perubahan	Deskripsi	Tanggal
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan grup CloudWatch log Amazon Logs yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file Windows File Server. FSx	8 Juni 2021
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan. Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file Windows File Server. FSx	8 Juni 2021
Amazon FSx mulai melacak perubahan	Amazon FSx mulai melacak perubahan untuk kebijakan yang AWS dikelola.	8 Juni 2021

Memecahkan masalah Amazon FSx untuk identitas dan akses Server File Windows

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan FSx Windows File Server dan IAM.

Topik

Saya tidak berwenang untuk melakukan tindakan di FSx

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 `fsx:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx: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 `fsx:`*`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 yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran FSx untuk Windows File Server.

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 FSx untuk Windows File Server. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

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

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

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses FSx sumber daya 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 mempelajari apakah FSx Windows File Server mendukung fitur-fitur ini, lihatBagaimana Amazon FSx untuk Windows File Server 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 dengan Amazon FSx

Anda dapat menggunakan tag untuk mengontrol akses ke FSx sumber daya Amazon dan menerapkan kontrol akses berbasis atribut (ABAC). Pengguna harus memiliki izin untuk menerapkan tag ke FSx sumber daya Amazon selama pembuatan.

Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat

Beberapa tindakan pembuatan sumber daya FSx untuk Windows File Server API memungkinkan Anda menentukan tag saat membuat sumber daya. Anda dapat menggunakan tag sumber daya untuk menerapkan kontrol akses berbasis atribut (ABAC). Untuk informasi selengkapnya, lihat Untuk apa ABAC AWS di Panduan Pengguna IAM.

Untuk memungkinkan para pengguna memberikan tanda pada sumber daya pada saat pembuatan, para pengguna tersebut harus memiliki izin untuk menggunakan tindakan-tindakan yang membuat sumber daya, seperti `fsx:CreateFileSystem` atau `fsx:CreateBackup`. Jika tanda-tanda ditentukan dalam tindakan yang digunakan untuk membuat sumber daya, maka Amazon akan melakukan otorisasi tambahan pada tindakan `fsx:TagResource` untuk melakukan verifikasi apakah pengguna memiliki izin untuk membuat tanda. Oleh karena itu, para pengguna juga harus memiliki izin eksplisit untuk menggunakan tindakan `fsx:TagResource`.

Contoh berikut menunjukkan kebijakan yang memungkinkan pengguna untuk membuat sistem file dan menerapkan tag ke sistem file selama pembuatan di tertentu Akun AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

Demikian pula, kebijakan berikut memungkinkan pengguna untuk membuat cadangan pada sistem file tertentu dan menerapkan tag apa pun ke cadangan selama pembuatan cadangan.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

Tindakan `fsx:TagResource` akan dievaluasi hanya jika tanda diterapkan selama tindakan pembuatan sumber daya. Oleh karena itu, seorang pengguna yang memiliki izin untuk membuat sumber daya (dengan asumsi tidak ada syarat untuk pemberian tanda) tidak memerlukan izin untuk menggunakan tindakan `fsx:TagResource` jika tidak ada tanda yang ditentukan dalam permintaan. Akan tetapi, jika pengguna tersebut mencoba untuk membuat sumber daya dengan tanda, maka permintaan akan gagal jika pengguna tidak memiliki izin untuk menggunakan tindakan `fsx:TagResource`.

Untuk informasi selengkapnya tentang menandai FSx sumber daya Amazon, lihatMenandai sumber daya Amazon FSx Anda. Untuk informasi selengkapnya tentang penggunaan tag untuk mengontrol akses ke FSx sumber daya, lihatMenggunakan tag untuk mengontrol akses ke FSx sumber daya Amazon Anda.

Menggunakan tag untuk mengontrol akses ke FSx sumber daya Amazon Anda

Untuk mengontrol akses ke FSx sumber daya dan tindakan Amazon, Anda dapat menggunakan kebijakan AWS Identity and Access Management (IAM) berdasarkan tag. Anda dapat memberikan kontrol dengan dua cara:

1. Kontrol akses ke FSx sumber daya Amazon 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 ke AWS sumber daya, lihat Mengontrol akses menggunakan tag di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang menandai FSx sumber daya Amazon saat pembuatan, lihatMemberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat. Untuk informasi selengkapnya tentang menandai sumber daya, lihatMenandai sumber daya Amazon FSx Anda.

Mengontrol akses berdasarkan tag pada sumber daya

Untuk mengontrol tindakan apa yang dapat dilakukan pengguna atau peran pada FSx sumber daya Amazon, Anda dapat menggunakan tag pada sumber daya. Misalnya, Anda mungkin ingin mengizinkan atau menolak operasi API tertentu pada sumber daya sistem file berdasarkan pasangan nilai kunci tag pada sumber daya.

Example kebijakan — Membuat sistem file pada saat memberikan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat sistem file hanya jika mereka menandainya dengan pasangan nilai kunci tag tertentu, dalam contoh ini,`key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example kebijakan - Buat cadangan hanya dari sistem FSx file Amazon dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat backup hanya dari sistem file yang ditandai dengan pasangan nilai kuncikey=Department, value=Finance, dan cadangan akan dibuat dengan tag. Deparment=Finance

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example kebijakan — Membuat sistem file dengan tag tertentu dari backup dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat sistem file yang ditandai dengan `Department=Finance` hanya dari backup yang ditandai dengan. `Department=Finance`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example kebijakan - Hapus sistem file dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk menghapus hanya sistem file yang diberi `Department=Finance` tag. Jika mereka membuat cadangan akhir, maka itu harus ditandai dengan`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Menggunakan peran terkait layanan FSx untuk Windows File Server

Amazon FSx untuk Windows File Server menggunakan peran AWS Identity and Access Management terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke Windows File FSx Server. Peran terkait layanan telah ditentukan sebelumnya oleh FSx untuk Windows File Server dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan FSx untuk Windows File Server lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. FSx untuk Windows File Server mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya FSx untuk Windows File Server yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Server File Windows Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya. FSx

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan FSx untuk Windows File Server

FSx untuk Windows File Server menggunakan peran terkait layanan bernama `AWSServiceRoleForAmazonFSx` - Yang melakukan tindakan tertentu di akun Anda, seperti membuat Antarmuka Jaringan Elastis untuk sistem file Anda di VPC Anda.

Kebijakan izin peran memungkinkan FSx Windows File Server menyelesaikan tindakan berikut pada semua AWS sumber daya yang berlaku:

Anda tidak dapat melampirkan Amazon FSx ServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Anda FSx mengelola AWS sumber daya atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan FSx untuk Windows File Server.

Untuk pembaruan kebijakan ini, lihat Amazon FSx ServiceRolePolicy

Kebijakan ini memberikan izin administratif yang memungkinkan FSx untuk mengelola AWS sumber daya atas nama pengguna.

Detail izin

Izin FSx ServiceRolePolicy peran Amazon ditentukan oleh kebijakan FSx ServiceRolePolicy AWS terkelola Amazon. Amazon FSx ServiceRolePolicy memiliki izin berikut:

> **Note**
>
> Amazon FSx ServiceRolePolicy digunakan oleh semua jenis sistem FSx file Amazon; beberapa izin yang tercantum mungkin tidak berlaku FSx untuk Windows.

- `ds`— Memungkinkan FSx untuk melihat, mengotorisasi, dan tidak mengotorisasi aplikasi di direktori Anda. AWS Directory Service
- `ec2`— Memungkinkan FSx untuk melakukan hal berikut:
  - Melihat, membuat, dan memisahkan antarmuka jaringan yang terkait dengan sistem FSx file Amazon.
  - Lihat satu atau beberapa alamat IP Elastis yang terkait dengan sistem FSx file Amazon.
  - Lihat Amazon VPCs, grup keamanan, dan subnet yang terkait dengan sistem FSx file Amazon.
  - Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.

  - Buat izin bagi pengguna AWS yang berwenang untuk melakukan operasi tertentu pada antarmuka jaringan.
- `cloudwatch`— Memungkinkan FSx untuk mempublikasikan titik data metrik ke CloudWatch bawah FSx namespace AWS/.
- `route53`— Memungkinkan FSx untuk mengaitkan VPC Amazon dengan zona host pribadi.
- `logs`— Memungkinkan FSx untuk mendeskripsikan dan menulis ke aliran CloudWatch log Log. Ini agar pengguna dapat mengirim log audit akses file untuk sistem file Windows File Server ke aliran CloudWatch Log. FSx
- `firehose`— Memungkinkan FSx untuk mendeskripsikan dan menulis ke aliran pengiriman Amazon Data Firehose. Ini agar pengguna dapat mempublikasikan log audit akses file untuk sistem file Windows File Server ke aliran pengiriman Amazon Data Firehose. FSx

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
```

```
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
```

```
}
```

Setiap pembaruan untuk kebijakan ini dijelaskan dalamAmazon FSx memperbarui kebijakan AWS terkelola.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan FSx untuk Windows File Server

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat sistem file di AWS Management Console, IAM CLI, atau IAM API FSx , untuk Windows File Server membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat sistem file, FSx untuk Windows File Server membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan FSx untuk Windows File Server

FSx untuk Windows File Server tidak memungkinkan Anda untuk mengedit peran terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan FSx untuk Windows File Server

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak perlu lagi memantau atau memelihara entitas yang tidak digunakan. Namun, Anda harus menghapus semua sistem file Anda sebelum Anda dapat menghapus peran tertaut layanan secara manual.

> **Note**
>
> Jika layanan FSx untuk Windows File Server menggunakan peran ketika Anda mencoba untuk menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, CLI IAM, atau API CLI untuk menghapus peran tertaut layanan . Untuk informasi selengkapnya, lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang didukung FSx untuk peran terkait layanan Windows File Server

FSx untuk Windows File Server mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah dan Titik Akhir AWS.

Validasi Kepatuhan untuk Amazon FSx untuk Windows File Server

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. 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 Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS

dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).

- 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— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Amazon FSx untuk Windows File Server dan titik akhir VPC antarmuka

Anda dapat meningkatkan postur keamanan VPC Anda dengan mengonfigurasi FSx Amazon untuk menggunakan titik akhir VPC antarmuka. Titik akhir VPC Antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses FSx APIs Amazon secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Amazon. FSx APIs Lalu lintas antara VPC dan Amazon Anda FSx tidak meninggalkan jaringan. AWS

Setiap antarmuka VPC endpoint diwakili oleh satu atau lebih antarmuka jaringan elastis di subnet Anda. Antarmuka jaringan menyediakan alamat IP pribadi yang berfungsi sebagai titik masuk untuk lalu lintas ke Amazon FSx API. Amazon FSx mendukung titik akhir VPC yang dikonfigurasi dengan IPv4 dan tipe alamat IP Dualstack (IPv4 dan IPv6). Untuk informasi selengkapnya, lihat Membuat titik akhir VPC antarmuka di Panduan Pengguna Amazon VPC.

Pertimbangan untuk titik akhir VPC FSx antarmuka Amazon

Sebelum menyiapkan titik akhir VPC antarmuka untuk Amazon FSx, pastikan untuk meninjau properti dan batasan titik akhir VPC Antarmuka di Panduan Pengguna Amazon VPC.

Anda dapat memanggil salah satu operasi Amazon FSx API dari VPC Anda. Misalnya, Anda dapat membuat sistem file FSx untuk Windows File Server dengan memanggil CreateFileSystem API dari dalam VPC Anda. Untuk daftar lengkap Amazon FSx APIs, lihat Tindakan di Referensi FSx API Amazon.

Pertimbangan mengintip VPC

Anda dapat menghubungkan yang lain VPCs ke VPC dengan titik akhir VPC antarmuka menggunakan VPC peering. VPC peering adalah koneksi jaringan antara dua. VPCs Anda dapat membuat koneksi peering VPC antara keduanya VPCs, atau dengan VPC di yang lain. Akun AWS VPCs Bisa juga dalam dua berbeda Wilayah AWS.

Lalu lintas antara peered VPCs tetap di AWS jaringan dan tidak melintasi internet publik. Setelah VPCs dipeer, sumber daya seperti instans Amazon Elastic Compute Cloud EC2 (Amazon) di keduanya VPCs dapat mengakses Amazon FSx API melalui titik akhir VPC antarmuka yang dibuat di salah satu. VPCs

Membuat titik akhir VPC antarmuka untuk Amazon API FSx

Anda dapat membuat titik akhir VPC untuk Amazon FSx API menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir VPC antarmuka di Panduan Pengguna Amazon VPC.

Untuk membuat titik akhir VPC antarmuka untuk Amazon FSx, gunakan salah satu dari berikut ini:

- **`com.amazonaws.`*`region`*`.fsx`**— Membuat titik akhir untuk operasi Amazon FSx API.
- **`com.amazonaws.`*`region`*`.fsx-fips`**— Membuat titik akhir untuk Amazon FSx API yang sesuai dengan Federal Information Processing Standard (FIPS) 140-2.

Untuk menggunakan opsi DNS pribadi, Anda harus mengatur `enableDnsHostnames` dan `enableDnsSupport` atribut VPC Anda. Untuk informasi selengkapnya, lihat Melihat dan memperbarui dukungan DNS untuk VPC Anda di Panduan Pengguna Amazon VPC.

Tidak termasuk Wilayah AWS di Tiongkok, jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Amazon dengan FSx titik akhir VPC menggunakan nama DNS default untuk, misalnya. Wilayah AWS`fsx.us-east-1.amazonaws.com` Untuk China (Beijing) dan Tiongkok (Ningxia Wilayah AWS), Anda dapat membuat permintaan API dengan titik akhir `fsx-api.cn-north-1.amazonaws.com.cn` VPC menggunakan dan, masing-masing. `fsx-api.cn-northwest-1.amazonaws.com.cn`

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir VPC antarmuka di Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk Amazon FSx

Untuk lebih mengontrol akses ke Amazon FSx API, Anda dapat melampirkan kebijakan AWS Identity and Access Management (IAM) secara opsional ke titik akhir VPC Anda. Kebijakan menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya di mana tindakan dapat dilakukan.

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Bekerja dengan layanan yang lain

Selain Amazon CloudWatch,, AWS Identity and Access Management, dan AWS CloudTrail AWS DataSync, FSx untuk Windows File Server juga terintegrasi dengan yang berikut: Layanan AWS

- Amazon AppStream 2.0 - AppStream 2.0 adalah layanan streaming aplikasi yang dikelola sepenuhnya yang menyediakan pengguna dengan akses instan ke aplikasi desktop mereka dari mana saja. AppStream 2.0 mengelola AWS sumber daya yang diperlukan untuk meng-host dan menjalankan aplikasi Anda, menskalakan secara otomatis, dan menyediakan akses ke pengguna sesuai permintaan. Pelajari cara membuat penyimpanan persisten untuk pengguna individual, dan berbagi penyimpanan di banyak pengguna di sistem file Windows File Server Anda FSx menggunakan AppStream 2.0. Untuk informasi selengkapnya, lihat Menggunakan Amazon FSx dengan Amazon AppStream 2.0.
- Amazon Kendra - Amazon Kendra adalah layanan pencarian cerdas yang menggunakan pemrosesan bahasa alami dan algoritme pembelajaran mesin canggih untuk mengembalikan jawaban spesifik atas pertanyaan penelusuran dari data Anda. Dengan Amazon Kendra, Anda dapat membuat pengalaman penelusuran terpadu dengan menghubungkan beberapa repositori data ke indeks dan menelan serta merayapi dokumen. Untuk informasi selengkapnya tentang menggunakan Amazon Kendra dengan FSx Windows File Server, lihat. Menggunakan FSx untuk Windows File Server dengan Amazon Kendra

Topik

Menggunakan Amazon FSx dengan Amazon AppStream 2.0

Dengan mendukung protokol Server Message Block (SMB), Amazon FSx untuk Windows File Server mendukung akses sistem file Anda dari instans Amazon EC2, VMware Cloud on WorkSpaces, AWS Amazon, dan Amazon AppStream 2.0. AppStream 2.0 adalah layanan streaming aplikasi yang dikelola sepenuhnya. Anda mengelola aplikasi desktop Anda secara terpusat pada AppStream 2.0 dan mengirimkannya dengan aman ke browser di komputer mana pun. Untuk informasi selengkapnya tentang AppStream 2.0, lihat Panduan Administrasi Amazon AppStream 2.0. Untuk petunjuk tentang bagaimana Anda dapat merampingkan pengelolaan gambar dan armada

Amazon AppStream 2.0 Anda, lihat posting AWS blog Secara otomatis membuat gambar Windows AppStream 2.0 yang disesuaikan.

Prosedur berikut menunjukkan kepada Anda cara menggunakan Amazon FSx dengan AppStream 2.0 untuk menyediakan penyimpanan persisten pribadi kepada setiap pengguna, dan untuk menyediakan folder bersama sehingga beberapa pengguna dapat mengakses file umum.

Menyediakan penyimpanan tetap pribadi untuk setiap pengguna

Anda dapat menggunakan Amazon FSx untuk menyediakan setiap pengguna di organisasi Anda drive penyimpanan unik dalam AppStream 2.0 sesi streaming. Pengguna akan memiliki izin hanya untuk mengakses foldernya saja. Hard disk dipasang secara otomatis pada awal sesi streaming dan file yang ditambahkan atau diperbarui ke hard disk akan disimpan secara otomatis di antara sesi streaming.

Ada tiga prosedur yang harus Anda lakukan untuk melakukan tugas ini.

Untuk membuat folder rumah bagi pengguna domain yang menggunakan Amazon FSx

1. Buat sistem FSx file Amazon. Untuk informasi selengkapnya, lihat Memulai Amazon FSx untuk Windows File Server.
2. Setelah sistem file tersedia, buat folder untuk setiap pengguna domain AppStream 2.0 dalam sistem FSx file Amazon Anda. Contoh berikut menggunakan nama pengguna domain dari pengguna sebagai nama folder yang sesuai. Dengan melakukan hal ini artinya Anda dapat membangun nama UNC dari berbagi file untuk memetakan dengan mudah menggunakan `%username%` variabel lingkungan Windows.
3. Bagikan setiap folder ini keluar sebagai sebuah folder bersama. Untuk informasi selengkapnya, lihat Membuat, memperbarui, menghapus berbagi file.

Untuk meluncurkan pembuat gambar 2.0 yang bergabung dengan domain AppStream

1. Masuk ke konsol AppStream 2.0: https://console.aws.amazon.com/appstream2
2. Pilih Config Direktori dari menu navigasi, dan buatlah sebuah objek Config Direktori. Untuk informasi selengkapnya, lihat Menggunakan Active Directory dengan AppStream 2.0 di Panduan Administrasi Amazon AppStream 2.0.
3. Pilih Gambar, Image Builder, dan luncurkan image builder baru.
4. Pilih objek config direktori yang dibuat sebelumnya di penuntun peluncuran image builder untuk menggabungkan image builder ke domain Direktori Aktif Anda.

5. Luncurkan pembuat gambar di VPC yang sama dengan sistem FSx file Amazon Anda. Pastikan untuk mengaitkan pembuat gambar dengan AWS Managed Microsoft AD direktori yang sama dengan sistem FSx file Amazon Anda bergabung. Grup keamanan VPC yang Anda kaitkan dengan pembuat gambar harus mengizinkan akses ke sistem FSx file Amazon Anda.
6. Setelah image builder tersedia, hubungkan ke image builder dan login menggunakan akun administrator domain Anda.
7. Instal aplikasi Anda.

Untuk menautkan berbagi FSx file Amazon dengan AppStream 2.0

1. Dalam image builder tersebut, buatlah skrip batch dengan perintah berikut dan simpan di lokasi file yang dikenal (misalnya: C:\Scripts\map-fs.bat). Contoh berikut menggunakan S: sebagai huruf drive untuk memetakan folder bersama pada sistem FSx file Amazon Anda. Anda menggunakan nama DNS sistem FSx file Amazon Anda atau alias DNS yang terkait dengan sistem file dalam skrip ini, yang bisa Anda dapatkan dari tampilan detail sistem file di konsol Amazon. FSx

   Jika Anda menggunakan nama DNS milik sistem file:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\users\%username%
   ```

   Jika Anda menggunakan alias DNS yang dikaitkan dengan sistem file:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\users\%username%
   ```
2. Buka PowerShell prompt dan jalankan`gpedit.msc`.
3. Dari Konfigurasi Pengguna, pilih Pengaturan Windows dan kemudian Logon.
4. Arahkan ke skrip batch yang Anda buat pada langkah pertama dalam prosedur ini, dan pilih itu.
5. Dari Konfigurasi Komputer, pilih Templat Administratif Windows, Sistem, dan kemudian Kebijakan Grup.
6. Pilih kebijakan Mengkonfigurasi penundaan Skrip Logon. Aktifkan kebijakan dan kurangi waktu tunda menjadi `0`. Pengaturan ini membantu untuk memastikan bahwa skrip logon pengguna dijalankan segera ketika pengguna memulai sebuah sesi streaming.

7. Buat gambar Anda dan tetapkan ke armada AppStream 2.0. Pastikan Anda juga bergabung dengan armada AppStream 2.0 ke domain Active Directory yang sama dengan yang Anda gunakan untuk pembuat gambar. Luncurkan armada di VPC yang sama yang digunakan oleh sistem FSx file Amazon Anda. Grup keamanan VPC yang Anda kaitkan dengan armada harus menyediakan akses ke sistem FSx file Amazon Anda.
8. Luncurkan sebuah sesi streaming menggunakan SAML SSO. Untuk terhubung ke armada yang digabungkan dengan Direktori Aktif, konfigurasikan federasi masuk tunggal menggunakan penyedia SAML. Untuk informasi selengkapnya, lihat Akses Masuk Tunggal ke AppStream 2.0 Menggunakan SAMP 2.0 di Panduan Administrasi Amazon AppStream 2.0.
9. Berbagi FSx file Amazon Anda dipetakan ke huruf drive S: dalam sesi streaming.

Menyediakan sebuah folder bersama di seluruh pengguna

Anda dapat menggunakan Amazon FSx untuk menyediakan folder bersama kepada pengguna di organisasi Anda. Sebuah folder bersama dapat digunakan untuk menyimpan file umum (misalnya, file demo, contoh kode, manual instruksi, dll.) yang dibutuhkan oleh semua pengguna.

Ada tiga prosedur yang harus Anda lakukan untuk melakukan tugas ini.

Untuk membuat folder bersama menggunakan Amazon FSx

1. Buat sistem FSx file Amazon. Untuk informasi selengkapnya, lihat Memulai Amazon FSx untuk Windows File Server.
2. Setiap sistem FSx file Amazon menyertakan folder bersama secara default yang dapat Anda akses menggunakan alamat*file-system-DNS-name*\ share, atau*fqdn-DNS-alias*\ share jika Anda menggunakan alias DNS. Anda dapat menggunakan berbagi default atau membuat sebuah folder bersama yang berbeda. Untuk informasi selengkapnya, lihat Membuat, memperbarui, menghapus berbagi file.

Untuk meluncurkan pembuat gambar AppStream 2.0

1. Dari konsol AppStream 2.0, luncurkan pembuat gambar baru atau sambungkan ke pembuat gambar yang ada. Luncurkan pembuat gambar di VPC yang sama yang digunakan oleh sistem FSx file Amazon Anda. Grup keamanan VPC yang Anda kaitkan dengan pembuat gambar harus mengizinkan akses ke sistem FSx file Amazon Anda.
2. Setelah image builder tersedia, hubungkan ke image builder sebagai pengguna Administrator.

3. Instal atau perbarui aplikasi Anda sebagai Administrator.

Untuk menautkan folder bersama dengan AppStream 2.0

1. Buatlah sebuah skrip batch, seperti yang dijelaskan dalam prosedur sebelumnya, untuk secara otomatis memasang folder bersama setiap kali pengguna meluncurkan sebuah sesi streaming. Untuk menyelesaikan skrip, Anda memerlukan nama DNS sistem file atau alias DNS yang terkait dengan sistem file (yang dapat Anda peroleh dari tampilan detail sistem file di FSx Konsol Amazon), dan kredensyal untuk mengakses folder bersama.

   Jika Anda menggunakan nama DNS milik sistem file:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   Jika Anda menggunakan alias DNS yang dikaitkan dengan sistem file:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. Membuat sebuah Kebijakan Grup untuk menjalankan skrip batch ini pada setiap logon pengguna. Anda dapat mengikuti petunjuk yang sama seperti yang dijelaskan pada bagian sebelumnya.
3. Buatlah gambar Anda dan tetapkan gambar tersebut ke armada Anda.
4. Luncurkan sebuah sesi streaming. Anda sekarang seharusnya melihat folder bersama secara otomatis dipetakan ke huruf kandar.

Menggunakan FSx untuk Windows File Server dengan Amazon Kendra

Amazon Kendra adalah layanan pencarian yang sangat akurat dan cerdas. FSx untuk sistem file Windows File Server dapat digunakan sebagai sumber data untuk Amazon Kendra, memungkinkan

Anda untuk mengindeks dan secara cerdas mencari informasi yang terkandung dalam dokumen yang disimpan di sistem file Anda.

- Untuk informasi selengkapnya tentang Amazon Kendra, lihat Apa itu Amazon Kendra di Panduan Pengembang Amazon Kendra.
- Untuk informasi selengkapnya tentang cara menambahkan sistem file Anda sebagai sumber data Amazon Kendra, lihat Memulai sumber FSx data Amazon (konsol) di Panduan Pengembang Amazon Kendra.
- Untuk informasi ikhtisar tentang Amazon Kendra, lihat situs web Amazon Kendra.
- Untuk panduan tentang cara mencari sistem file Anda menggunakan Amazon Kendra, lihat Cari data tidak terstruktur secara aman pada sistem file Windows dengan konektor Amazon Kendra untuk FSx Amazon untuk Windows File Server di Blog Machine Learning.AWS

Kinerja sistem file

Saat Anda menambahkan sistem file Windows File Server sebagai sumber data, Amazon Kendra merayapi file dan folder pada sistem file pada frekuensi sinkronisasi reguler untuk membuat dan mempertahankan indeks pencariannya. FSx (Anda dapat memilih frekuensi sinkronisasi saat Anda membuat integrasi.) Aktivitas akses file dari Amazon Kendra ini akan menggunakan sumber daya sistem file, mirip dengan aktivitas dari beban kerja Anda sendiri yang mengakses sistem file.

Pastikan sistem file Anda dikonfigurasi dengan sumber daya yang cukup sehingga kinerja beban kerja Anda tidak terpengaruh. Secara khusus, jika Anda berencana untuk mengindeks sejumlah besar file, kami sarankan menggunakan sistem file dengan tipe penyimpanan SSD, yang menyediakan throughput maksimum yang lebih tinggi dan tingkat IOPS untuk permintaan yang perlu mengakses volume penyimpanan. Untuk informasi selengkapnya tentang model FSx kinerja Amazon, lihatFSx untuk kinerja Windows File Server.

Kuota

Berikut ini, Anda dapat mengetahui tentang kuota saat bekerja dengan Amazon FSx untuk Windows File Server.

Topik

Kuota yang dapat Anda tingkatkan

Berikut ini adalah kuota untuk Amazon FSx untuk Windows File Server untuk masing-masing Akun AWS, per Wilayah AWS, yang dapat Anda tingkatkan.

Sumber Daya	Default	Deskripsi
Sistem file Windows	100	Jumlah maksimum sistem file Amazon FSx untuk Windows Server yang dapat Anda buat di akun ini.
Kapasitas throughput Windows	10240	Jumlah total kapasitas throughput (in MBps) yang diizinkan untuk semua sistem file Amazon FSx untuk Windows di akun ini.
Kapasitas penyimpanan Windows HDD	524288	Jumlah maksimum kapasitas penyimpanan HDD (dalam GiB) diizinkan untuk semua sistem file FSx Amazon untuk Windows File Server di akun ini.

Sumber Daya	Default	Deskripsi
Kapasitas penyimpanan SSD Windows	524288	Jumlah maksimum kapasitas penyimpanan SSD (dalam GiB) diizinkan untuk semua sistem file Amazon FSx untuk Windows File Server di akun ini.
Total SSD IOPS Windows	500.000	Jumlah total SSD IOPS diizinkan untuk semua sistem file Amazon FSx untuk Windows File Server di akun ini.
Cadangan Windows	500	Jumlah maksimum cadangan yang dimulai pengguna untuk semua sistem file FSx Amazon untuk Windows File Server yang dapat Anda miliki di akun ini.

Meminta untuk penambahan Kuota

1. Buka Konsol Service Quotas.
2. Di panel navigasi, pilih Layanan AWS .
3. Pilih Amazon FSx.
4. Pilih kuota.
5. Pilih Permintaan peningkatan kuota, dan ikuti petunjuk arahan untuk meminta peningkatan kuota.
6. Untuk melihat status permintaan kuota, pilih Riwayat permintaan kuota di panel navigasi konsol.

Untuk informasi lebih lanjut, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Kuota sumber daya untuk setiap sistem file

Berikut ini adalah kuota di Amazon FSx untuk sumber daya Windows File Server untuk setiap sistem file dalam file Wilayah AWS.

Sumber Daya	Batas per sistem file
Jumlah maksimum tag	50
Periode penyimpanan maksimum untuk cadangan otomatis	90 hari
Jumlah maksimum permintaan salinan cadangan yang sedang berlangsung ke satu Wilayah tujuan per akun.	5
Kapasitas penyimpanan minimum, sistem file SSD	32 GiB
Kapasitas penyimpanan minimum, sistem file HDD	2.000 GiB
Kapasitas penyimpanan maksimal, SSD dan HDD	64 TiB
IOPS SSD minimum	96
IOPS SSD maksimum	400.000
Kapasitas throughput minimum	8 MBps
Kapasitas throughput maksimum	12,288 MBps
Jumlah maksimum berbagi file	100.000

Pertimbangan tambahan

Selain itu, perhatikan hal berikut:

- Anda dapat menggunakan setiap tombol AWS Key Management Service (AWS KMS) hingga 125 sistem FSx file Amazon.
- Untuk daftar Wilayah AWS tempat Anda dapat membuat sistem file, lihat FSx Titik Akhir Amazon dan Kuota di. Referensi Umum AWS

- Anda memetakan pembagian file Anda dari EC2 instans Amazon di cloud pribadi virtual (VPC) Anda dengan nama Layanan Nama Domain (DNS) mereka.

Kuota khusus untuk Microsoft Windows

Untuk informasi lebih lanjut, lihat batas NTFS Microsoft Windows Dev Center.

Memecahkan Masalah Amazon FSx

Gunakan bagian berikut untuk membantu memecahkan masalah yang Anda miliki dengan Amazon. FSx

Jika Anda mengalami masalah yang tidak tercantum berikut saat menggunakan Amazon FSx, coba ajukan pertanyaan di FSx forum Amazon.

Topik

Anda tidak dapat mengakses sistem file Anda

Ada beberapa kemungkinan penyebab Anda tidak dapat mengakses sistem file Anda, masing-masing memiliki penyelesaian masalah sendiri, sebagai berikut.

Topik

- Tidak dapat mengakses sistem file menggunakan alamat IP

Antarmuka jaringan elastis sistem file telah dimodifikasi atau dihapus

Anda tidak boleh mengubah atau menghapus antarmuka jaringan elastis sistem file. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan koneksi hilang permanen antara VPC dan sistem file Anda. Buat sistem file baru, dan jangan memodifikasi atau menghapus antarmuka FSx elastis network Amazon. Untuk informasi selengkapnya, lihat Kontrol akses sistem file dengan Amazon VPC.

Alamat IP Elastis yang dilekatkan pada antarmuka jaringan elastis sistem file telah dihapus

Amazon FSx tidak mendukung akses sistem file dari internet publik. Amazon FSx secara otomatis melepaskan alamat IP Elastic, yang merupakan alamat IP publik yang dapat dijangkau dari internet, yang dilampirkan ke antarmuka network elastis sistem file. Untuk informasi selengkapnya, lihat Mengakses data Anda.

Grup keamanan sistem file tidak memiliki aturan masuk atau keluar yang diperlukan.

Tinjau aturan masuk yang ditentukan dalam Grup keamanan Amazon VPC, dan pastikan bahwa grup keamanan yang terkait dengan sistem file Anda memiliki aturan masuk yang sesuai.

Grup keamanan instans komputasi ini tidak memiliki aturan keluar yang diperlukan

Tinjau aturan keluar yang ditentukan dalam Grup keamanan Amazon VPC, dan pastikan bahwa grup keamanan yang terkait dengan instans komputasi Anda memiliki aturan keluar yang sesuai.

Instans komputasi tidak bergabung ke Direktori Aktif

Instans komputasi Anda mungkin tidak bergabung dengan benar ke salah satu dari dua jenis Direktori Aktif:

- AWS Managed Microsoft AD Direktori tempat sistem file Anda bergabung.
- Direktori Direktori Aktif Microsoft yang memiliki hubungan forest trust satu arah yang dibuat dengan direktori AWS Managed Microsoft AD .

Pastikan bahwa instans komputasi Anda bergabung ke salah satu dari dua jenis direktori. Salah satu jenisnya adalah AWS Managed Microsoft AD direktori tempat sistem file Anda bergabung. Jenis lainnya adalah direktori Microsoft Active Directory yang memiliki hubungan kepercayaan hutan satu arah yang dibuat dengan AWS Managed Microsoft AD direktori. Untuk informasi selengkapnya, lihat Menggunakan Amazon FSx dengan AWS Directory Service for Microsoft Active Directory.

Pembagian file tidak ada

Pembagian file Microsoft Windows yang sedang Anda coba akses tidak ada.

Jika Anda menggunakan pembagian file yang ada, pastikan bahwa nama DNS sistem file dan nama pembagian ditentukan dengan benar. Untuk mengelola pembagian file, lihat Membuat, memperbarui, menghapus berbagi file.

Pengguna Direktori Aktif tidak memiliki izin yang diperlukan

Pengguna Direktori Aktif yang pembagian filenya sedang Anda akses tidak memiliki izin akses yang diperlukan.

Pastikan bahwa izin akses untuk berbagi file dan daftar kontrol akses Windows (ACLs) untuk folder bersama memungkinkan akses ke pengguna Active Directory yang perlu mengaksesnya.

Izin Izinkan kontrol Penuh NTFS ACL dihapus

Jika Anda menghapus Izinkan izin NTFS ACL kontrol penuh untuk pengguna SYSTEM pada folder yang Anda bagikan, pembagian itu dapat menjadi tidak dapat diakses dan cadangan sistem file apa pun yang diambil sejak saat itu dan seterusnya mungkin tidak dapat digunakan.

Anda akan perlu membuat kembali pembagian file terdampak. Untuk informasi selengkapnya, lihat Membuat, memperbarui, menghapus berbagi file. Setelah Anda membuat kembali folder atau pembagian, Anda dapat memetakan dan menggunakan pembagian file Windows dari instans komputasi Anda.

Tidak dapat mengakses sistem file menggunakan klien on-premise

Anda menggunakan sistem FSx file Amazon dari penggunaan lokal AWS Direct Connect atau VPN, dan Anda menggunakan rentang alamat IP non-pribadi untuk klien lokal.

Amazon FSx hanya mendukung akses dari klien lokal dengan alamat IP non-pribadi pada sistem file yang dibuat setelah 17 Desember 2020.

Jika Anda perlu mengakses sistem file Windows File Server Anda FSx yang dibuat sebelum 17 Desember 2020 menggunakan rentang alamat IP non-pribadi, Anda dapat membuat sistem file baru dengan memulihkan cadangan sistem file. Untuk informasi selengkapnya, lihat Melindungi data Anda dengan backup.

Sistem file baru tidak terdaftar di DNS

Untuk sistem file yang bergabung dengan Active Directory yang dikelola sendiri, Amazon FSx tidak mendaftarkan DNS sistem file saat dibuat karena jaringan pelanggan tidak menggunakan Microsoft DNS.

Amazon FSx tidak mendaftarkan sistem file di DNS jika jaringan Anda menggunakan layanan DNS pihak ketiga, bukan Microsoft DNS. Anda harus mengatur entri DNS A secara manual untuk sistem FSx file Amazon Anda. Untuk sistem file Single-AZ 1, Anda perlu menambahkan satu entri DNS A; untuk sistem file Single-AZ 2 dan Multi-AZ, Anda perlu menambahkan dua entri DNS A. Gunakan prosedur berikut untuk mendapatkan alamat IP sistem file atau alamat untuk digunakan ketika secara manual menambahkan entri DNS A.

1. Di dalam https://console.aws.amazon.com/fsx/, pilih sistem file yang ingin Anda dapatkan alamat IP untuk menampilkan halaman detail sistem file.
2. Di tab Jaringan & keamanan lakukan salah satu hal berikut:

   - Untuk sistem file Single-AZ 1:
     - Di panel Subnet, pilih elastic network interface yang ditampilkan di bawah Network interface untuk membuka halaman Network Interfaces di Amazon. EC2
     - Alamat IP untuk sistem file Single-AZ 1 yang akan digunakan ditampilkan di kolom IPv4 IP pribadi Primer.
   - Untuk sistem file Single-AZ 2 atau Multi-AZ:
     - Di panel subnet Preferred, pilih elastic network interface yang ditampilkan di bawah Network interface untuk membuka halaman Network Interfaces di Amazon. EC2
     - Alamat IP untuk subnet pilihan untuk digunakan ditampilkan di kolom IPv4 IP pribadi Sekunder.
     - Di panel subnet Amazon FSx Standby, pilih elastic network interface yang ditampilkan di bawah Network interface untuk membuka halaman Network Interfaces di konsol Amazon. EC2
     - Alamat IP untuk subnet siaga yang akan digunakan ditampilkan di kolom IPv4 IP pribadi Sekunder.

Tidak dapat mengakses sistem file menggunakan alias DNS

Jika Anda tidak dapat mengakses sistem file menggunakan alias DNS, gunakan prosedur berikut untuk memecahkan masalah.

1. Pastikan bahwa alias terkait dengan sistem file dengan melakukan salah satu dari langkah-langkah berikut:

   a. Menggunakan FSx konsol Amazon — Pilih sistem file yang Anda coba akses. Pada halaman Detail sistem file, halaman Nama alias DNS ditampilkan pada tab Jaringan & keamanan.

   b. Menggunakan CLI atau API — Gunakan perintah `describe-file-system-aliases`CLI, atau operasi DescribeFileSystemAliasesAPI untuk mengambil alias yang saat ini terkait dengan sistem file.

2. Jika DNS alias tidak terdaftar, Anda harus mengaitkannya dengan sistem file. Untuk informasi selengkapnya, lihat Mengelola alias DNS pada sistem file yang ada.

3. Jika alias DNS terkait dengan sistem file, pastikan bahwa Anda juga telah mengkonfigurasi item yang diperlukan berikut:

   - Membuat nama utama layanan (SPNs) yang sesuai dengan alias DNS pada objek komputer Active Directory sistem FSx file Amazon Anda.

     Untuk informasi selengkapnya, lihat Konfigurasikan nama utama layanan (SPNs) untuk Kerberos.

   - Membuat catatan DNS CNAME untuk alias DNS yang menyelesaikan nama DNS default sistem file Amazon. FSx

     Untuk informasi selengkapnya, lihat Memperbarui atau membuat catatan DNS CNAME.

4. Jika Anda membuat catatan CNAME yang valid SPNs dan DNS, verifikasi bahwa DNS klien memiliki catatan DNS CNAME yang menyelesaikan ke sistem file yang benar.

   a. Jalankan `nslookup` untuk mengkonfirmasi bahwa catatan ada dan bahwa diubah ke nama DNS default sistem file.

   b. Jika DNS CNAME diubah ke sistem file lain, tunggu cache DNS klien me-refresh, dan kemudian periksa catatan CNAME lagi. Anda dapat mempercepat proses dengan pembilasan cache DNS klien menggunakan perintah berikut.

```
ipconfig /flushdns
```

5. Jika catatan CNAME DNS menyelesaikan DNS default sistem FSx file Amazon, dan klien masih tidak dapat mengakses sistem file, lihat Anda tidak dapat mengakses sistem file Anda langkah-langkah pemecahan masalah tambahan.

Tidak dapat mengakses sistem file menggunakan alamat IP

Jika Anda tidak dapat mengakses sistem file Anda menggunakan alamat IP, coba gunakan nama DNS atau alias DNS terkait sebagai gantinya.

Anda dapat menemukan nama DNS sistem file dan alias DNS terkait di FSx konsol Amazon dengan memilih Windows File Server, Jaringan & keamanan. Atau, Anda dapat menemukan mereka dalam respon Operasi API CreateFileSystem atau DescribeFileSystems. Untuk informasi selengkapnya tentang menggunakan alias DNS, lihat Mengelola alias DNS.

- Untuk sistem file Single-AZ yang bergabung dengan Direktori Aktif Microsoft AWS Terkelola, nama DNS terlihat seperti berikut ini.

```
fs-0123456789abcdef0.ad-domain.com
```

- Untuk semua sistem file Multi-AZ, dan sistem file Single-AZ yang bergabung dengan Active Directory yang dikelola sendiri, nama DNS terlihat seperti berikut ini.

```
amznfsxaa11bb22.ad-domain.com
```

Membuat sistem FSx file Amazon baru gagal

Ada beberapa kemungkinan penyebab ketika permintaan pembuatan sistem file gagal dilakukan, seperti yang dijelaskan di bagian berikut.

Topik

- Grup dan jaringan keamanan VPC yang salah konfigurasi ACLs
- Duplikat nama grup administrator sistem file
- Server DNS atau pengontrol domain tidak dapat dijangkau
- Kredensi akun layanan tidak valid

- Izin akun layanan tidak mencukupi
- Kapasitas akun layanan terlampaui
- Amazon tidak FSx dapat mengakses unit organisasi (OU)
- Akun layanan tidak dapat mengakses grup administrator
- Amazon FSx kehilangan konektivitas di domain
- Akun layanan tidak memiliki izin yang benar
- Karakter unicode yang digunakan dalam parameter pembuatan
- Mengalihkan jenis penyimpanan ke HDD saat memulihkan backup gagal dilakukan

Grup dan jaringan keamanan VPC yang salah konfigurasi ACLs

Pastikan grup dan jaringan keamanan VPC ACLs dikonfigurasi menggunakan konfigurasi grup keamanan yang disarankan. Untuk informasi selengkapnya, lihat Membuat grup keamanan.

Duplikat nama grup administrator sistem file

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

Amazon FSx tidak membuat sistem file karena ada beberapa grup administrator di domain dengan nama yang sama.

Jika Anda tidak menentukan nama grup, Amazon FSx akan mencoba menggunakan nilai default “Domain Admin” sebagai grup administrator. Permintaan akan gagal jika ada lebih dari satu grup menggunakan nama default “Domain Admin”.

Gunakan langkah-langkah berikut untuk menyelesaikan masalah.

1. Tinjau prasyarat untuk bergabung dengan sistem file Anda ke Active Directory yang dikelola sendiri.

2. Gunakan Alat Validasi Direktori FSx Aktif Amazon untuk memvalidasi konfigurasi Direktori Aktif yang dikelola sendiri sebelum membuat sistem file FSx untuk Windows File Server yang digabungkan ke Direktori Aktif yang dikelola sendiri.
3. Buat sistem file baru menggunakan AWS Management Console atau AWS CLI. Untuk informasi selengkapnya, lihat Bergabung dengan sistem FSx file Amazon ke domain Microsoft Active Directory yang dikelola sendiri.
4. Berikan nama untuk grup administrator sistem file yang unik di domain untuk Active Directory yang dikelola sendiri.

Server DNS atau pengontrol domain tidak dapat dijangkau

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
traffic from the file system to the domain controller.
```

Gunakan langkah-langkah berikut untuk memecahkan masalah dan menyelesaikan masalah.

1. Pastikan Anda mengikuti prasyarat untuk memiliki konektivitas jaringan dan perutean yang dibuat antara subnet tempat Anda membuat sistem FSx file Amazon, dan Active Directory yang dikelola sendiri. Untuk informasi selengkapnya, lihat Prasyarat.

   Gunakan alat Validasi Direktori FSx Aktif Amazon untuk menguji dan memverifikasi pengaturan jaringan ini.

   > **Note**
   >
   > Jika Anda memiliki beberapa situs Direktori Aktif yang ditentukan, pastikan bahwa subnet di VPC yang terkait dengan sistem file FSx Amazon Anda ditentukan di situs Direktori Aktif dan tidak ada konflik IP antara subnet di VPC Anda dan subnet di situs Anda yang

lain. Anda dapat melihat dan mengubah pengaturan ini menggunakan Situs Direktori Aktif dan snap-in MMC Layanan.

2. Verifikasi bahwa Anda mengonfigurasi grup keamanan VPC yang terkait dengan sistem FSx file Amazon Anda, bersama dengan jaringan VPC apa pun ACLs, untuk memungkinkan lalu lintas jaringan keluar di semua port.

   > **Note**
   >
   > Jika Anda ingin menerapkan pengurangan hak istimewa, Anda dapat mengizinkan lalu lintas keluar hanya untuk port tertentu yang diperlukan untuk komunikasi dengan pengontrol domain Direktori Aktif. Untuk informasi selengkapnya, lihat Dokumentasi Direktori Aktif Microsoft.

3. Pastikan bahwa nilai-nilai untuk Microsoft Windows file server atau sifat administratif jaringan tidak berisi karakter non-Latin-1. Sebagai contoh, pembuatan sistem file gagal jika Anda menggunakan `Domänen-Admins` sebagai nama grup administrator sistem file.
4. Pastikan bahwa server DNS domain dan pengontrol domain Direktori Aktif sudah aktif dan dapat menanggapi permintaan untuk domain yang disediakan.
5. Pastikan bahwa tingkat fungsional domain Direktori Aktif Anda adalah Windows Server 2008 R2 atau lebih tinggi.
6. Pastikan bahwa aturan firewall pada pengontrol domain Active Directory memungkinkan lalu lintas dari sistem FSx file Amazon Anda. Untuk informasi selengkapnya, lihat Dokumentasi Direktori Aktif Microsoft.

Kredensi akun layanan tidak valid

Membuat sistem file yang bergabung dengan Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

Gunakan langkah-langkah berikut untuk memecahkan masalah dan menyelesaikan masalah.

1. Pastikan bahwa Anda memasukkan hanya nama pengguna sebagai input untuk Nama pengguna akun layanan, seperti `ServiceAcct`, dalam konfigurasi Direktori Aktif yang dikelola sendiri.

   > **Important**
   >
   > JANGAN sertakan prefiks domain (`corp.com\ServiceAcct`) atau sufiks domain (`ServiceAcct@corp.com`) saat memasukkan Nama pengguna akun layanan. JANGAN gunakan nama terhormat (DN) saat memasukkan nama pengguna akun layanan (CN=ServiceAcct, OU = Contoh, DC = Corp, DC = COM).

2. Pastikan bahwa akun layanan yang Anda berikan ada di domain Direktori Aktif.
3. Pastikan bahwa Anda mendelegasikan izin yang diperlukan untuk akun layanan yang Anda berikan. Akun layanan harus mampu membuat dan menghapus objek komputer di OU di domain yang Anda gabungkan dengan sistem file. Untuk memiliki izin, Akun layanan juga setidaknya perlu untuk melakukan hal berikut:

   - Atur ulang kata sandi
   - Batasi akun dari membaca dan menulis data
   - Kemampuan tervalidasi untuk menulis ke nama host DNS
   - Kemampuan tervalidasi untuk menulis ke nama utama layanan

   Untuk mempelajari selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat Akun FSx layanan Amazon.

Izin akun layanan tidak mencukupi

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
```

```
permission to join the file system to the domain with the specified organizational
 unit.
```

Gunakan langkah-langkah berikut untuk memecahkan masalah dan menyelesaikan masalah.

- Pastikan bahwa Anda mendelegasikan izin yang diperlukan untuk akun layanan yang Anda berikan. Akun layanan harus mampu membuat dan menghapus objek komputer di OU di domain yang Anda gabungkan dengan sistem file. Untuk memiliki izin, Akun layanan juga setidaknya perlu untuk melakukan hal berikut:

  - Atur ulang kata sandi
  - Batasi akun dari membaca dan menulis data
  - Kemampuan tervalidasi untuk menulis ke nama host DNS
  - Kemampuan tervalidasi untuk menulis ke nama utama layanan

  Untuk mempelajari selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat Akun FSx layanan Amazon.

Kapasitas akun layanan terlampaui

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

Untuk mengatasi masalah, pastikan bahwa akun layanan yang Anda berikan telah mencapai jumlah maksimum komputer yang dapat digabungkan olehnya ke domain tersebut. Jika telah mencapai batas maksimum, buat akun layanan baru dengan izin yang benar. Gunakan akun layanan baru dan buat sistem file baru. Untuk informasi selengkapnya, lihat Akun FSx layanan Amazon.

Amazon tidak FSx dapat mengakses unit organisasi (OU)

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
This is because the organizational unit you specified either doesn't exist or isn't
 accessible
to the service account provided. To fix this problem, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

Gunakan langkah-langkah berikut untuk memecahkan masalah dan menyelesaikan masalah.

1. Pastikan bahwa OU yang Anda berikan di domain Direktori Aktif Anda.
2. Pastikan bahwa Anda telah mendelegasikan izin yang diperlukan untuk akun layanan yang Anda berikan. Akun layanan harus dapat membuat dan menghapus objek komputer di OU di domain yang Anda gabungkan dengan sistem file. Akun layanan juga harus memiliki, minimal, izin untuk melakukan hal berikut:

   - Atur ulang kata sandi
   - Batasi akun dari membaca dan menulis data
   - Kemampuan tervalidasi untuk menulis ke nama host DNS
   - Kemampuan tervalidasi untuk menulis ke nama utama layanan
   - Didelegasikan kontrol untuk membuat dan menghapus objek komputer
   - Kemampuan tervalidasi untuk membaca dan menulis Pembatasan Akun

   Untuk mempelajari selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat Akun FSx layanan Amazon.

Akun layanan tidak dapat mengakses grup administrator

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
```

```
system administrators group in the domain that is accessible to the service account
provided.
```

Gunakan langkah-langkah berikut untuk memecahkan masalah dan menyelesaikan masalah.

1. Pastikan bahwa Anda hanya menyediakan nama grup sebagai string untuk parameter grup administrator.

   > **Important**
   >
   > JANGAN menyertakan prefiks domain (`corp.com\FSxAdmins`) atau sufiks domain (`FSxAdmins@corp.com`) saat memberikan parameter nama grup.
   > JANGAN menggunakan Nama yang Dibedakan (DN) untuk grup. Contoh nama yang dibedakan adalah CN = FSx Admin, OU = Contoh, DC = Corp, DC = COM.

2. Pastikan bahwa grup administrator yang disediakan ada di domain Direktori Aktif yang sama dengan yang Anda ingin gabungkan dengan sistem file.
3. Jika Anda tidak memberikan parameter grup administrator, Amazon FSx mencoba menggunakan `Builtin Domain Admins` grup di domain Active Directory Anda. Jika nama grup ini telah diubah, atau jika Anda menggunakan grup lain untuk administrasi domain, Anda harus memberikan nama tersebut untuk grup tersebut.

Amazon FSx kehilangan konektivitas di domain

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

Saat membuat sistem file Anda, Amazon FSx dapat menjangkau server DNS dan pengontrol domain Active Directory Anda, dan berhasil bergabung dengan sistem file ke domain Active Directory Anda. Namun, saat menyelesaikan pembuatan sistem file, Amazon FSx kehilangan konektivitas atau keanggotaan di domain Anda. Gunakan langkah-langkah berikut untuk memecahkan masalah dan menyelesaikan masalah.

1. Pastikan konektivitas jaringan terus ada antara sistem FSx file Amazon Anda dan Direktori Aktif Anda. Dan, pastikan bahwa lalu lintas jaringan terus diizinkan di antara mereka dengan menggunakan aturan perutean, aturan grup keamanan VPC, ACLs jaringan VPC, dan aturan firewall pengontrol domain.
2. Pastikan objek komputer yang dibuat oleh Amazon FSx untuk sistem file Anda di domain Active Directory Anda masih aktif, dan tidak dihapus atau dimanipulasi.

Akun layanan tidak memiliki izin yang benar

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

Pastikan bahwa Anda telah mendelegasikan izin yang diperlukan untuk akun layanan yang Anda berikan. Gunakan langkah-langkah berikut untuk memecahkan masalah dan menyelesaikan masalah.

Akun layanan harus memiliki, minimal, izin berikut:

- Didelegasikan kontrol untuk membuat dan menghapus objek komputer di OU yang Anda gabungkan dengan sistem file
- Memiliki izin berikut di OU yang Anda gabungkan dengan sistem file:
  - Kemampuan untuk mengatur ulang kata sandi
  - Kemampuan untuk membatasi akun dari membaca dan menulis data
  - Kemampuan tervalidasi untuk menulis ke nama host DNS
  - Kemampuan tervalidasi untuk menulis ke nama utama layanan
  - Kemampuan (dapat didelegasikan) untuk membuat dan menghapus objek komputer
  - Kemampuan tervalidasi untuk membaca dan menulis Pembatasan Akun
  - Kemampuan untuk memodifikasi izin

Untuk mempelajari selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat Akun FSx layanan Amazon.

Karakter unicode yang digunakan dalam parameter pembuatan

Membuat sistem file yang bergabung dengan Direktori Aktif yang dikelola sendiri gagal dilakukan dengan pesan galat berikut:

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

Amazon FSx tidak mendukung karakter Unicode. Pastikan bahwa tidak ada parameter pembuatan yang memiliki karakter Unicode, seperti tanda aksen. Ini termasuk parameter yang dapat dibiarkan kosong di mana nilai default diisi secara otomatis. Pastikan nilai default yang sesuai di Direktori Aktif Anda juga tidak mengandung karakter Unicode.

Mengalihkan jenis penyimpanan ke HDD saat memulihkan backup gagal dilakukan

Membuat sistem file dari backup gagal dengan pesan galat berikut:

`Switching storage type to HDD while creating a file system from backup` *`backup_id`* `is not supported because a storage scaling activity was still under way on the source file system to increase storage capacity from less than 2000 GiB when the backup` *`backup_id`* `was taken, and the minimum storage capacity for HDD storage is 2000 GiB.`

Masalah ini terjadi saat memulihkan backup dan Anda telah mengubah jenis penyimpanan dari SSD ke HDD. Pemulihan dari backup gagal karena backup yang Anda pulihkan diambil sedangkan peningkatan kapasitas penyimpanan masih berlangsung pada sistem file semula. Kapasitas penyimpanan SSD sistem file sebelum peningkatan permintaan kurang dari 2000 GiB, yang merupakan kapasitas penyimpanan minimum yang diperlukan untuk membuat sistem file HDD.

Gunakan prosedur berikut untuk mengatasi permasalahan ini.

1. Tunggu permintaan peningkatan kapasitas penyimpanan hingga selesai dan sistem file setidaknya memiliki kapasitas penyimpanan SSD sebesar 2000 GiB. Untuk informasi selengkapnya, lihat Memantau peningkatan kapasitas penyimpanan.
2. Mengambil backup sistem file yang diprakarsai pengguna. Untuk informasi selengkapnya, lihat Bekerja dengan backup yang diinisiasi pengguna.
3. Pulihkan backup yang diprakarsai pengguna ke sistem file baru menggunakan penyimpanan HDD. Untuk informasi selengkapnya, lihat Memulihkan backup ke sistem file baru.

Sistem file dalam keadaan salah konfigurasi

Sistem file Server File Windows FSx untuk Windows dapat masuk ke status Salah Konfigurasi karena perubahan lingkungan Direktori Aktif Anda. Dalam keadaan ini, sistem file Anda saat ini tidak tersedia atau berisiko kehilangan ketersediaan, dan cadangan mungkin tidak berhasil.

Status salah konfigurasi menyertakan pesan kesalahan dan tindakan korektif yang disarankan yang dapat Anda akses menggunakan FSx konsol Amazon, API, atau. AWS CLI Setelah melakukan tindakan korektif, verifikasi bahwa status sistem file Anda akhirnya berubah menjadi `Available` — perhatikan bahwa perubahan ini dapat memakan waktu beberapa menit untuk diselesaikan.

Sistem file Anda dapat masuk ke status Salah Konfigurasi karena beberapa alasan, seperti berikut ini:

- Alamat IP DNS Server tidak lagi valid.
- Kredensyal akun layanan tidak lagi valid, atau tidak memiliki izin yang diperlukan.
- Pengontrol domain Active Directory tidak dapat dijangkau karena masalah konektivitas jaringan, seperti Grup Keamanan VPC yang tidak valid, ACL Jaringan VPC atau konfigurasi tabel perutean, atau pengaturan firewall pengontrol domain.

> **Important**
>
> Jangan pindahkan objek komputer yang FSx dibuat Amazon di OU setelah sistem file Anda dibuat. Dengan melakukannya, sistem file Anda akan mengalami kesalahan konfigurasi.

(Untuk daftar lengkap persyaratan Direktori Aktif, lihatPrasyarat. Anda juga dapat memvalidasi bahwa lingkungan Direktori Aktif dikonfigurasi dengan benar untuk memenuhi persyaratan ini dengan menggunakan alat Validasi Direktori FSx Aktif Amazon.)

Menyelesaikan beberapa masalah ini memerlukan pembaruan langsung satu atau beberapa parameter dalam konfigurasi Active Directory sistem file Anda, seperti mengubah alamat IP Server DNS, atau mengubah nama pengguna atau kata sandi akun layanan. Dalam kasus ini, tindakan korektif Anda akan melibatkan penggunaan FSx konsol Amazon, API, atau AWS CLI untuk memperbarui parameter konfigurasi yang diperlukan.

Masalah lain mungkin tidak memerlukan perubahan parameter konfigurasi Direktori Aktif, seperti mengubah pengaturan firewall pengontrol domain Anda atau Grup Keamanan VPC. Namun, dalam kasus ini, Anda perlu mengambil tindakan lebih lanjut sebelum sistem file dapat menjadi`Available`. Setelah memastikan lingkungan Direktori Aktif Anda dikonfigurasi dengan benar, pilih tombol Percobaan Pemulihan di sebelah status Salah Konfigurasi di FSx konsol Amazon, atau gunakan `StartMisconfiguredStateRecovery` perintah di FSx konsol Amazon, API, atau AWS CLI.

Topik

Sistem file yang salah konfigurasi: Amazon tidak FSx dapat menjangkau server DNS atau pengontrol domain untuk domain Anda.

Sistem file akan masuk ke `Misconfigured` keadaan ketika Amazon tidak FSx dapat berkomunikasi dengan pengontrol atau pengontrol domain Microsoft Active Directory Anda.

Untuk mengatasi keadaan ini, coba yang berikut ini:

1. Pastikan bahwa konfigurasi jaringan Anda mengizinkan lalu lintas dari sistem file ke pengendali domain.

2. Gunakan alat Validasi Direktori FSx Aktif Amazon untuk menguji dan memverifikasi pengaturan jaringan untuk Active Directory yang dikelola sendiri. Untuk informasi selengkapnya, lihat Menggunakan Microsoft Active Directory yang dikelola sendiri.
3. Tinjau konfigurasi Active Directory yang dikelola sendiri oleh sistem file di FSx konsol Amazon.
4. Untuk memperbarui konfigurasi Active Directory yang dikelola sendiri oleh sistem file, Anda dapat menggunakan FSx konsol Amazon.

   a. Pada panel navigasi, pilih Sistem file, dan pilih sistem file yang akan diperbarui; halaman Detail sistem file akan muncul.

   b. Pada halaman Detail sistem file, pilih Perbarui pada tab Jaringan dan keamanan.

   Anda juga dapat menggunakan `update-file-system` perintah Amazon FSx CLI atau operasi API. UpdateFileSystem

Sistem file yang salah dikonfigurasi: kredensial akun layanan tidak valid

Amazon tidak FSx dapat membuat koneksi dengan pengontrol atau pengontrol domain Microsoft Active Directory Anda. Hal ini karena kredensial akun layanan yang disediakan tidak valid. Untuk informasi selengkapnya, lihat Menggunakan Microsoft Active Directory yang dikelola sendiri.

Untuk mengatasi kesalahan konfigurasi, lakukan hal berikut:

1. Pastikan bahwa Anda menggunakan akun layanan yang benar, dan Anda menggunakan kredensial yang benar untuk akun tersebut.
2. Kemudian perbarui konfigurasi sistem file dengan akun layanan atau kredensyal akun yang benar menggunakan konsol Amazon FSx .

   a. Pada panel navigasi, pilih Sistem file, dan pilih sistem file yang salah dikonfigurasi untuk diperbarui.

   b. Pada halaman detail sistem file, pilih Perbarui di tab Jaringan dan keamanan.

   Anda juga dapat menggunakan operasi Amazon FSx API`update-file-system`. Untuk mempelajari selengkapnya, lihat Referensi FSx API Amazon. UpdateFileSystem

Sistem file yang salah dikonfigurasi: Akun layanan yang disediakan tidak memiliki izin untuk menggabungkan sistem file ke domain

Amazon tidak FSx dapat membuat koneksi ke pengontrol domain Microsoft Active Directory Anda. Hal ini karena akun layanan yang disediakan tidak memiliki izin untuk menggabungkan sistem file ke domain dengan OU tertentu.

Untuk mengatasi kesalahan konfigurasi, lakukan hal berikut:

1. Tambahkan izin yang diperlukan ke akun FSx layanan Amazon, atau buat akun layanan baru dengan izin yang diperlukan. Untuk informasi selengkapnya tentang langkah ini, lihat Akun FSx layanan Amazon.
2. Kemudian perbarui konfigurasi Direktori Aktif sistem file yang dikelola sendiri dengan kredensial akun layanan baru. Untuk memperbarui konfigurasi, Anda dapat menggunakan FSx konsol Amazon.

    a. Pada panel navigasi, pilih Sistem file, dan pilih sistem file yang akan diperbarui; halaman Detail sistem file akan muncul.

    b. Pada halaman Detail sistem file, pilih Perbarui pada tab Jaringan dan keamanan.

    Anda juga dapat menggunakan operasi Amazon FSx API`update-file-system`. Untuk mempelajari selengkapnya, lihat Referensi FSx API Amazon. UpdateFileSystem

Sistem file yang salah dikonfigurasi: Akun layanan tidak lagi dapat menggabungkan komputer ke domain

Amazon tidak FSx dapat membuat koneksi ke pengontrol domain Microsoft Active Directory Anda. Dalam hal ini, ini terjadi karena akun layanan yang disediakan telah mencapai jumlah maksimum komputer yang dapat bergabung ke domain.

Untuk mengatasi kesalahan konfigurasi, lakukan hal berikut:

1. Mengidentifikasi akun layanan lain atau membuat akun layanan baru yang dapat menggabungkan komputer baru ke domain.
2. Kemudian perbarui konfigurasi Active Directory yang dikelola sendiri oleh sistem file dengan kredensyal akun layanan baru menggunakan konsol Amazon. FSx

a. Pada panel navigasi, pilih Sistem file, dan pilih sistem file yang akan diperbarui; halaman Detail sistem file akan muncul.
b. Pada halaman Detail sistem file, pilih Perbarui pada tab Jaringan dan keamanan.

Anda juga dapat menggunakan operasi Amazon FSx API`update-file-system`. Untuk mempelajari selengkapnya, lihat Referensi FSx API Amazon. UpdateFileSystem

Sistem file yang salah dikonfigurasi: Akun layanan tidak memiliki akses ke OU

Amazon tidak FSx dapat membuat sambungan ke pengontrol domain Microsoft Active Directory karena akun layanan yang disediakan tidak memiliki akses ke OU yang ditentukan.

Untuk mengatasi kesalahan konfigurasi, lakukan hal berikut:

1. Mengidentifikasi akun layanan lain atau membuat akun layanan baru yang memiliki akses ke OU.
2. Kemudian perbarui konfigurasi Direktori Aktif yang dikelola sendiri dari sistem file dengan kredensial akun layanan baru.

   a. Pada panel navigasi, pilih Sistem file, dan pilih sistem file yang akan diperbarui; halaman Detail sistem file akan muncul.
   b. Pada halaman Detail sistem file, pilih Perbarui pada tab Jaringan dan keamanan.

   Anda juga dapat menggunakan operasi Amazon FSx API`update-file-system`. Untuk mempelajari selengkapnya, lihat Referensi FSx API Amazon. UpdateFileSystem

Anda tidak dapat mengkonfigurasi DFS-R pada sistem file Multi-AZ atau Single-AZ 2

Replikasi Sistem File yang Didistribusikan Microsoft (DFS-R) tidak support pada sistem file Multi-AZ dan Single-AZ 2.

Sistem file Multi-AZ dikonfigurasi untuk redundansi di beberapa zona akses native. Gunakan jenis deployment Multi-AZ untuk ketersediaan tinggi di beberapa Availability Zone. Untuk informasi selengkapnya, lihat Ketersediaan dan daya tahan: Sistem file Single-AZ dan Multi-AZ.

Pembaruan kapasitas penyimpanan atau throughput gagal dilakukan

Ada sejumlah potensi penyebab permintaan pembaruan kapasitas penyimpanan dan throughput sistem file gagal dilakukan, masing-masing dengan penyelesaiannya sendiri.

Peningkatan kapasitas penyimpanan gagal karena Amazon tidak FSx dapat mengakses sistem file AWS KMS key

Permintaan peningkatan kapasitas penyimpanan gagal karena Amazon FSx tidak dapat mengakses kunci KMS yang digunakan untuk mengenkripsi sistem file.

Anda perlu memastikan bahwa Amazon FSx memiliki akses ke kunci KMS yang digunakan untuk mengenkripsi sistem file untuk menjalankan tindakan administratif. Gunakan informasi berikut untuk menyelesaikan masalah akses kunci.

- Jika kunci KMS telah dihapus, sistem file dan cadangannya menggunakan kunci KMS yang dihapus tidak dapat dipulihkan. Untuk informasi selengkapnya, lihat Menghapus AWS KMS key s di Panduan AWS Key Management Service Pengembang.
- Jika kunci KMS dinonaktifkan, dan itu adalah kunci yang dikelola pelanggan, Anda harus mengaktifkannya kembali, dan kemudian mencoba lagi permintaan peningkatan kapasitas penyimpanan. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan kunci di Panduan Pengembang. AWS Key Management Service
- Jika kunci tidak valid karena penghapusan yang tertunda, Anda harus membatalkan penghapusan kunci saat masih dalam keadaan. `PendingDeletion` Anda dapat mencoba kembali permintaan setelah kunci KMS. `Enabled`
- Jika kunci tidak valid karena menunggu proses impor, Anda harus menunggu sampai impor selesai, dan kemudian coba lagi permintaan peningkatan penyimpanan.
- Jika batas pemberian kunci telah terlampaui, Anda harus meminta peningkatan jumlah pemberian untuk kunci. Untuk informasi selengkapnya, lihat Kuota sumber daya di Panduan AWS Key Management Service Pengembang. Ketika peningkatan kuota diberikan, coba lagi permintaan peningkatan penyimpanan.

Pembaruan kapasitas penyimpanan atau throughput gagal karena Direktori Aktif yang dikelola sendiri salah konfigurasi

Kapasitas penyimpanan atau permintaan pembaruan kapasitas throughput gagal karena sistem file Direktori Aktif yang dikelola sendiri berada dalam keadaan salah konfigurasi.

Untuk mengatasi keadaan salah konfigurasi tertentu, lihat Sistem file dalam keadaan salah konfigurasi.

Peningkatan kapasitas penyimpanan gagal karena kapasitas throughput tidak mencukupi

Permintaan peningkatan kapasitas penyimpanan gagal karena kapasitas throughput sistem file diatur ke 8 MBps.

Tingkatkan kapasitas throughput sistem file hingga minimal 16 MBps, lalu coba lagi permintaannya. Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput.

Pembaruan kapasitas throughput ke 8 gagal MBps

Permintaan untuk mengubah kapasitas throughput sistem file menjadi 8 MBps gagal.

Hal ini dapat terjadi ketika permintaan peningkatan kapasitas penyimpanan tertunda atau sedang berlangsung. Peningkatan kapasitas penyimpanan membutuhkan throughput minimum 16 MBps. Tunggu sampai permintaan peningkatan kapasitas penyimpanan telah selesai, dan kemudian coba lagi permintaan modifikasi kapasitas throughput.

Riwayat dokumen

- Versi API: 2018-03-01
- Pembaruan dokumentasi terbaru: 28 Mei 2025

Tabel berikut menjelaskan perubahan penting pada Panduan Pengguna Amazon FSx Windows. Untuk notifikasi tentang pembaruan dokumentasi, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Amazon FSx memperbarui kebijakan FSx FullAccess AWS terkelola Amazon	Kebijakan FSx FullAccess terkelola Amazon diperbarui untuk menambahkan`fsx:CreateAndAttachS3AccessPoint` ,`fsx:DescribeS3AccessPointAttachments` , `fsx:UpdateS3AccessPointAttachments`, dan `fsx:DetachAndDeleteS3AccessPoint` izin.	28 Mei 2025
Amazon FSx memperbarui kebijakan FSx ConsoleFullAccess AWS terkelola Amazon	Kebijakan FSx ConsoleFullAccess terkelola Amazon diperbarui untuk menambahkan`fsx:CreateAndAttachS3AccessPoint` ,`fsx:DescribeS3AccessPointAttachments` , `fsx:UpdateS3AccessPointAttachments`, dan `fsx:DetachAndDeleteS3AccessPoint` izin.	28 Mei 2025

Amazon FSx memperbarui kebijakan FSx ConsoleReadOnlyAccess AWS terkelola Amazon	Amazon FSx memperbarui FSx ConsoleReadOnlyAccess kebijakan Amazon untuk menambahkan `ec2:DescribeNetworkInterfaces` izin. Untuk informasi selengkapnya, lihat FSx ConsoleReadOnlyAccess kebijakan Amazon.	Februari 25, 2025
Support ditambahkan untuk titik akhir antarmuka VPC dual-stack untuk Amazon FSx	Anda sekarang dapat membuat titik akhir antarmuka VPC dual-stack untuk Amazon FSx dengan IPv6 alamat IP IPv4 dan nama DNS. Untuk informasi selengkapnya, lihat FSx untuk Windows File Server dan titik akhir VPC antarmuka.	Februari 7, 2025
Support ditambahkan untuk endpoint API dual-stack	API FSx layanan Amazon untuk membuat dan mengelola sistem file memiliki titik akhir dual-stack baru. Untuk informasi selengkapnya, lihat titik akhir API di Referensi Amazon FSx API.	Februari 7, 2025
Amazon FSx memperbarui kebijakan FSx ConsoleFullAccess AWS terkelola Amazon	Amazon FSx memperbarui FSx ConsoleFullAccess kebijakan Amazon untuk menambahkan `ec2:DescribeNetworkInterfaces` izin. Untuk informasi selengkapnya, lihat FSx ConsoleFullAccess kebijakan Amazon.	Februari 7, 2025

Versi terbaru dari alat Validasi Direktori Aktif Server File Windows untuk Windows FSx	Versi terbaru dari alat Validasi Direktori Aktif Server File Windows FSx untuk Windows tersedia. Untuk informasi selengkapnya, lihat Memvalidasi konfigurasi Direktori Aktif	6 November 2024
Support ditambahkan untuk level IOPS yang lebih tinggi pada sistem file dengan kapasitas throughput 4 dan lebih tinggi GBps	FSx untuk Windows File Server meningkatkan IOPS maksimum dari 130K menjadi 150K untuk sistem file dengan 4 GBps kapasitas throughput atau lebih tinggi, dari 175K menjadi 200K untuk sistem file dengan 6 GBps kapasitas throughput atau lebih tinggi, dari 260K hingga 300K untuk sistem file dengan 9 kapasitas throughput atau lebih tinggi, dan dari 350K hingga 400K untuk sistem file dengan 12 GBps kapasitas throughput atau lebih tinggi. GBps Untuk informasi selengkapnya, lihat FSx untuk kinerja Windows File Server.	Januari 17, 2024

Amazon FSx memperbarui kebijakan yang FSx ServiceRolePolicy AWS dikelola Amazon FSx FullAccess FSxConsoleFullAccess, Amazon FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon, dan Amazon	Amazon FSx memperbarui FSx ServiceRolePolicy kebijakan Amazon FSxFullAccess, Amazon FSxConsoleFullAccess, Amazon FSx ReadOnlyAccess FSxConsoleReadOnlyAccess, Amazon, dan Amazon untuk menambahkan `ec2:GetSecurityGroupsForVpc` izin. Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	Januari 9, 2024
Amazon FSx memperbarui kebijakan yang FSx ConsoleFullAccess AWS dikelola Amazon FSx FullAccess dan Amazon	Amazon FSx memperbarui FSx ConsoleFullAccess kebijakan Amazon FSx FullAccess dan Amazon untuk menambahkan `ManageCrossAccountDataReplication` tindakan. Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	20 Desember 2023
Amazon FSx memperbarui kebijakan yang FSx ConsoleFullAccess AWS dikelola Amazon FSx FullAccess dan Amazon	Amazon FSx memperbarui FSx ConsoleFullAccess kebijakan Amazon FSx FullAccess dan Amazon untuk menambahkan `fsx:CopySnapshotAndUpdateVolume` izin. Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	26 November 2023

Amazon FSx memperbarui kebijakan yang FSx ConsoleFullAccess AWS dikelola Amazon FSx FullAccess dan Amazon	Amazon FSx memperbarui FSx ConsoleFullAccess kebijakan Amazon FSx FullAccess dan Amazon untuk menambahkan `fsx:DescribeSharedVPCConfiguration` dan `fsx:UpdateSharedVPCConfiguration` izin. Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola.	14 November 2023
Support ditambahkan untuk memperbarui jenis penyimpanan sistem file	FSx untuk sistem file Windows File Server sekarang mendukung pembaruan dari jenis penyimpanan HDD ke jenis penyimpanan SSD. Untuk informasi selengkapnya, lihat Mengelola jenis penyimpanan.	9 Agustus 2023
Support ditambahkan untuk kapasitas throughput maksimum yang lebih tinggi	FSx untuk sistem file Windows File Server sekarang mendukung hingga 12 kapasitas GBps throughput. Untuk informasi selengkapnya, lihat FSx untuk kinerja Windows File Server.	9 Agustus 2023

Support ditambahkan untuk penyediaan SSD IOPS	FSx untuk sistem file Windows File Server sekarang mendukung penyediaan SSD IOPS secara independen dari kapasitas penyimpanan, hingga maksimum 350.000 IOPS. Untuk informasi selengkapnya, lihat Mengelola IOPS SSD.	9 Agustus 2023
Amazon FSx memperbarui kebijakan FSx ServiceRolePolicy AWS terkelola Amazon	Amazon FSx memperbarui `cloudwatch:PutMetricData` izin di Amazon FSxServiceRolePolicy. Untuk informasi selengkapnya, lihat Amazon FSx ServiceRolePolicy.	Juli 24, 2023
Amazon FSx memperbarui kebijakan FSx FullAccess AWS terkelola Amazon	Amazon FSx memperbarui FSx FullAccess kebijakan Amazon untuk menghapus `fsx:*` izin dan menambahkan `fsx` tindakan tertentu. Untuk informasi selengkapnya, lihat FSx FullAccess kebijakan Amazon.	13 Juli 2023
Amazon FSx memperbarui kebijakan FSx ConsoleFullAccess AWS terkelola Amazon	Amazon FSx memperbarui FSx ConsoleFullAccess kebijakan Amazon untuk menghapus `fsx:*` izin dan menambahkan `fsx` tindakan tertentu. Untuk informasi selengkapnya, lihat FSx ConsoleFullAccess kebijakan Amazon.	13 Juli 2023

Support ditambahkan untuk CloudWatch metrik baru untuk Amazon FSx untuk Windows File Server	FSx untuk Windows File Server sekarang menyediakan CloudWatch metrik tambahan yang memantau server file dan kinerja volume penyimpanan dan penggunaan kapasitas. Untuk informasi selengkapnya, lihat Metrik dan dimensi.	September 22, 2022
Support ditambahkan untuk peringatan kinerja sistem file	Amazon FSx sekarang memberikan peringatan di jendela Kinerja & pemantaua n ketika salah satu set CloudWatch metrik mendekati atau melewati ambang batas yang telah ditentukan untuk metrik ini. Setiap peringatan juga memberikan rekomenda si yang dapat ditindaklanjuti untuk meningkatkan kinerja sistem file. Untuk informasi selengkapnya, lihat Peringatan dan rekomendasi kinerja.	September 22, 2022

Support ditambahkan untuk pemantauan kinerja sistem file yang ditingkatkan	Dasbor pemantauan sistem file FSx konsol Amazon FSx untuk sistem file Windows File Server mencakup bagian Ringkasan, Penyimpanan, dan Kinerja baru. Bagian ini menampilkan grafik CloudWatch metrik baru yang memberi Anda pemantaua n kinerja yang ditingkatkan. Untuk informasi selengkap nya, lihat Metrik pemantauan dengan CloudWatch.	September 22, 2022
Support ditambahkan untuk AWS PrivateLink titik akhir VPC antarmuka.	Anda sekarang dapat menggunakan titik akhir VPC antarmuka untuk mengakses Amazon FSx API dari VPC Anda tanpa mengirim lalu lintas melalui internet. Untuk informasi selengkapnya, lihat Amazon FSx dan antarmuka VPC endpoint.	5 April 2022

Support ditambahkan untuk Amazon Kendra	Anda sekarang dapat menggunakan sistem file Windows File Server Anda FSx sebagai sumber data untuk Amazon Kendra, memungkinkan Anda untuk mengindeks dan mencari informasi yang terkandun g dalam dokumen yang disimpan di sistem file Anda. Untuk informasi selengkapnya, lihat Menggunakan FSx untuk Windows File Server dengan Amazon Kendra.	Maret 26, 2022
Support ditambahkan untuk audit akses file	Anda sekarang dapat mengaktifkan audit akses pengguna akhir pada file, folder, dan fitur berbagi file. Anda dapat memilih untuk mengirim log peristiwa audit ke Amazon CloudWatch Logs atau layanan Amazon Data Firehose. Untuk informasi selengkapnya, lihat Mengaudit akses file.	8 Juni 2021

Support ditambahkan untuk menyalin backup	Anda sekarang dapat menggunakan Amazon FSx untuk menyalin cadangan dalam AWS akun yang sama ke akun lain Wilayah AWS (Salinan lintas wilayah) atau dalam yang sama Wilayah AWS (Salinan dalam wilayah). Untuk informasi selengkapnya, lihat Menyalin cadangan.	12 April 2021
Secara otomatis meningkatkan kapasitas penyimpanan sistem file	Gunakan AWS CloudFormation templat AWS yang dapat disesuaikan yang dikembangkan untuk secara otomatis meningkatkan kapasitas penyimpanan sistem file Anda saat kapasitasnya mencapai ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Meningkatkan kapasitas penyimpanan secara dinamis.	17 Februari 2021

Support ditambahkan untuk akses klien menggunakan alamat IP non-pribadi	Anda dapat mengakses FSx sistem file Windows File Server dengan klien lokal menggunakan alamat IP non-pribadi. Untuk informasi lebih lanjut, lihat Lingkungan yang di-support. Anda dapat bergabung FSx untuk sistem file Windows File Server ke Microsoft Active Directory yang dikelola sendiri dengan server DNS dan pengontrol domain AD yang menggunak an alamat IP non-pribadi. Untuk informasi selengkap nya, lihat Menggunakan Amazon FSx dengan Direktori Aktif Microsoft yang Dikelola Sendiri.	17 Desember 2020
Support ditambahkan untuk menggunakan alias DNS	Anda sekarang dapat mengaitkan alias DNS dengan sistem file Windows File Server Anda yang dapat Anda gunakan untuk mengakses data pada sistem file Anda. FSx Untuk informasi selengkapnya, lihat Mengelola alias DNS dan Panduan 5: Menggunakan alias DNS untuk mengakses sistem file Anda.	9 November 2020

Support ditambahkan untuk Amazon Elastic Container Service	Anda sekarang dapat menggunakan FSx untuk Windows File Server dengan Amazon ECS. Untuk informasi lebih lanjut, lihat Klien yang Di-support.	9 November 2020
Amazon FSx kini terintegrasi dengan AWS Backup	Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan dan memulihkan sistem FSx file Anda selain menggunakan FSx backup Amazon asli. Untuk informasi selengkap nya, lihat Menggunakan AWS Backup dengan Amazon FSx.	9 November 2020
Support ditambahkan untuk penskalaan kapasitas throughput	Anda sekarang dapat memodifikasi kapasitas throughput untuk sistem file Windows File Server yang ada FSx saat persyaratan throughput Anda berkemban g. Untuk informasi selengkap nya, lihat Mengelola Kapasitas Throughput.	1 Juni 2020
Support ditambahkan untuk penskalaan kapasitas penyimpanan	Anda sekarang dapat meningkatkan kapasitas penyimpanan untuk sistem file Windows File Server yang ada FSx saat kebutuhan penyimpanan Anda berkembang. Untuk informasi selengkapnya, lihat Mengelola Kapasitas Penyimpanan.	1 Juni 2020

Support ditambahkan untuk penyimpanan hard disk drive (HDD)	Penyimpanan HDD memberi Anda fleksibilitas harga dan kinerja saat menggunakan FSx untuk Windows File Server. Untuk informasi selengkapnya, lihat Mengoptimalkan Biaya dengan Amazon FSx.	26 Maret 2020
Support ditambahkan untuk transfer file menggunakan AWS DataSync	Anda sekarang dapat menggunakan AWS DataSync untuk mentransfer file ke dan dari FSx untuk Windows File Server Anda. Untuk informasi selengkapnya, lihat Memigrasi File ke Amazon FSx untuk Menggunakan AWS DataSync Server File Windows.	4 Februari 2020
FSx untuk Windows File Server merilis dukungan untuk tugas administrasi sistem file Windows tambahan	Anda sekarang dapat mengelola dan mengelola berbagi file, deduplikasi data, kuota penyimpanan, dan enkripsi dalam perjalana n untuk berbagi file Anda menggunakan Amazon FSx CLI untuk manajemen jarak jauh. PowerShell Untuk informasi selengkapnya, lihat Mengelola sistem file.	20 November 2019

FSx untuk Windows File Server merilis dukungan Multi-AZ asli	Anda dapat menggunakan penyebaran Multi-AZ FSx untuk Windows File Server agar lebih mudah membuat sistem file dengan ketersediaan tinggi yang menjangkau beberapa Availability Zone ()AZs. Untuk informasi selengkapnya, lihat Ketersediaan dan Daya Tahan: Sistem File Single-AZ dan Multi-AZ.	20 November 2019
FSx untuk Windows File Server merilis dukungan untuk mengelola sesi pengguna dan membuka file	Anda sekarang dapat menggunakan alat Folder Bersama asli Microsoft Windows untuk mengelola sesi pengguna dan membuka file pada sistem file Windows File Server Anda FSx . Untuk informasi selengkapnya, lihat Mengelola Sesi Pengguna dan File Terbuka.	17 Oktober 2019

Amazon FSx merilis dukungan untuk salinan bayangan Microsoft Windows	Anda sekarang dapat mengkonfigurasi salinan bayangan Windows pada sistem file Windows File Server Anda FSx . Salinan bayangan memungkinkan pengguna Anda untuk dengan mudah membatalkan perubahan file dan membandingkan versi file dengan memulihkan file ke versi sebelumnya. Untuk informasi selengkapnya, lihat Bekerja dengan Salinan Shadow.	31 Juli 2019
Amazon FSx merilis dukungan Microsoft Active Directory bersama	Anda sekarang dapat bergabung FSx untuk sistem file Windows File Server ke AWS Managed Microsoft AD direktori yang berada di VPC yang berbeda atau Akun AWS berbeda dari sistem file. Untuk informasi selengkapnya, lihat Support Active Directory.	25 Juni 2019
Amazon FSx merilis dukungan Microsoft Active Directory yang disempurnakan	Sekarang Anda dapat bergabung FSx untuk sistem file Windows File Server ke domain Microsoft Active Directory yang dikelola sendiri, baik lokal maupun di cloud. Untuk informasi selengkapnya, lihat Support Active Directory.	24 Juni 2019

Amazon FSx mematuhi sertifikasi SOC	Amazon FSx telah dinilai untuk mematuhi sertifikasi SOC. Untuk informasi selengkapnya, lihat Perlindungan Keamanan dan Data.	16 Mei 2019
Menambahkan catatan klarifikasi mengenai AWS Direct Connect, VPN, dan dukungan koneksi peering VPC antar wilayah	Sistem FSx file Amazon yang dibuat setelah 22 Februari 2019 dapat diakses menggunakan AWS Direct Connect, VPN, dan peering VPC antar wilayah. Untuk informasi selengkapnya, lihat Metode Akses yang Di-support.	25 Februari 2019
AWS Direct Connect, VPN, dan dukungan koneksi peering VPC antar-wilayah ditambahkan	Anda sekarang dapat mengakses sistem file Amazon FSx untuk Windows File Server dari sumber daya lokal dan dari sumber daya di Akun AWS VPC Amazon yang berbeda atau. Untuk informasi selengkapnya, lihat Metode Akses yang Di-support.	22 Februari 2019

Amazon FSx sekarang tersedia secara umum	Amazon FSx untuk Windows File Server menyediakan server file Microsoft Windows yang dikelola sepenuhnya, didukung oleh sistem file Windows yang sepenuhnya asli. Amazon FSx untuk Windows File Server menyediakan fitur, kinerja, dan kompatibilitas untuk dengan mudah mengangkat dan mengalihkan aplikasi perusahaan ke AWS.	28 November, 2018

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